

Transforming Joint Air and Space Power

THE  
JOURNAL  
OF THE JAPCC



6

**Sweden Strengthens NATO's Presence in Europe**

The Swedish Air Force Commander's View on Joining NATO

13

**The Turkish Air Force**

Boosting Defence Capabilities within NATO:  
Perspectives from the Turkish Air Chief

28

**Enhancing NATO's Strategic Edge**

A Human-Centric Approach  
to Multi-Domain Operations





## STATE OF THE ART MARKSMAN

The Skyranger 30 and Skyranger 35 from Rheinmetall Air Defence in Zurich are the mobile all-in-one solutions against current and future airborne threats.

### **Move**

The Skyranger turret on any proven and highly mobile armoured vehicle, guarantees protection in all situations, whether it is on or off roads.

### **Sense**

The Skyranger commander monitors the airspace autonomously with its own sensor suite and/or via a higher echelon sensor network. The Skyranger reliably detects, classifies and acquires even small flying objects while on the move or in stationary deployment.

### **Defend**

The revolver guns in their respective calibre (30 or 35 mm), combined with the airburst ammunition deliver impressive performance optimised to engage airborne threats such as drones and cruise missiles with unmatched precision. Customer-specific guided missiles in the Skyranger 30 variation additionally extend the spectrum of engagements and range.

[www.rheinmetall.com](http://www.rheinmetall.com)

**TAKING RESPONSIBILITY** IN A CHANGING WORLD

 **RHEINMETALL**

# Editorial

**A**fter an exhilarating three years in Kalkar, my tenure as the JAPCC Assistant Director and Managing Editor of this Journal will end in September 2024. I am immensely grateful to my editorial team, under the leadership of the Chief of Staff, for their dedication and hard work in ensuring the success of our Journal. Their efforts have made my role seamless, and I truly appreciate their contributions. I also extend my thanks to all the contributing Nations for providing their exceptional Subject Matter Experts, who have enriched the relevance of the JAPCC.

Editing the Journal has been one of the most rewarding tasks in my entire portfolio. The numerous contributions from across the Alliance and beyond have been thought-provoking and innovative, but also educational and simply enjoyable to read. I extend my heartfelt gratitude to all of you – readers and authors alike – who have played a role in making this Journal a valuable asset in JAPCC's transformational toolbox.

We kick off this issue with a captivating article by Major General Jonas Wikman, Commander of the Swedish Air Force, who discusses Sweden's recent accession into NATO and its implications for the air domain. Following this, General Ziya Cemal Kadioğlu, Commander of the Turkish Air Force, shares his perspectives on current efforts and strategic advancements within his service.

Next, we explore the cybersecurity risks brought about by the proliferation of small satellites, followed by the latest advancements and methodologies for human performance in Multi-Domain Operations. Continuing our theme of transformational capabilities, we conclude our three-part

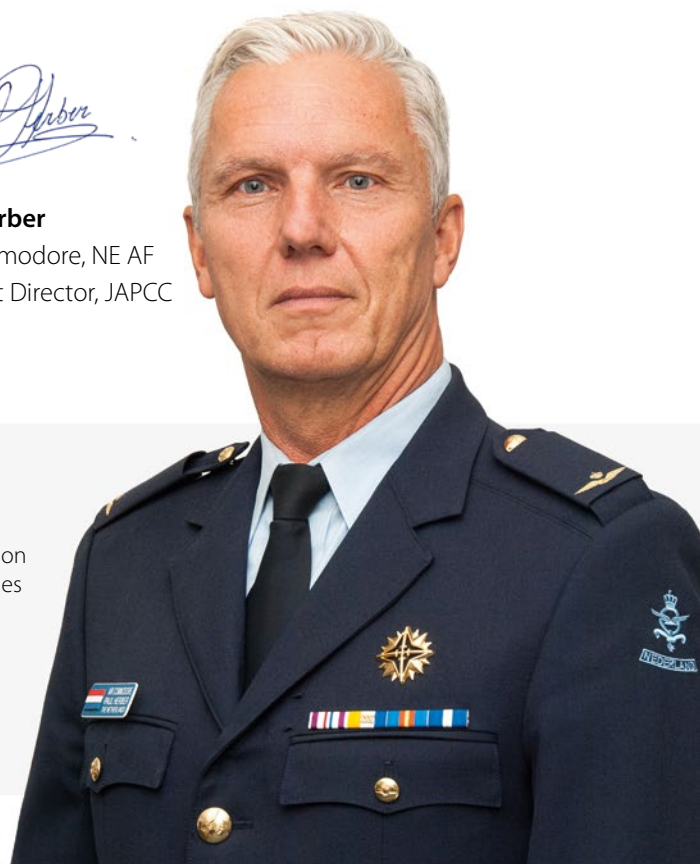
series on the military applications of quantum technology. Next, we examine the concept of hosted payloads in space, proposing this as an additional layer of resilience and deterrence.

Within our Viewpoints section, we delve into defence acquisition principles in the new security and technology environment with an intriguing article on 'Bending the Hufnagel'. This is followed by an exploration of the evolving technological and policy challenges for deterrence. Then we discuss Multi-Domain Operations in NATO, focusing on aspects of trust and technology in the US's Combined Joint All Domain Command and Control concept. Finally, we present fresh perspectives on measures of effectiveness in non-lethal targeting.

Thank you for your valuable feedback, which has greatly contributed to our ongoing efforts to transform Joint Air and Space Power. We invite you to explore our website at [www.japcc.org](http://www.japcc.org), connect with us on LinkedIn, or reach out to us via email at [contact@japcc.org](mailto:contact@japcc.org).

Finally, let me introduce the new JAPCC Assistant Director, Colonel Vito Cracas of the Italian Air Force and wish him the best in this great and challenging job. I know he'll continue the JAPCC's proud tradition of delivering independent thought and analysis to promote and improve NATO Air Power!

**Paul Herber**  
Air Commodore, NE AF  
Assistant Director, JAPCC



The Journal of the JAPCC welcomes unsolicited manuscripts. Please email submissions to: [contact@japcc.org](mailto: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](http://www.japcc.org/journals)

Follow us on Social Media





69



52



77

# Table of Contents

## Leadership Perspective

**06** Sweden Strengthens NATO's Presence in Europe  
*The Swedish Air Force Commander's View on Joining NATO*

**13** The Turkish Air Force  
*Boosting Defence Capabilities within NATO: Perspectives from the Turkish Air Chief*

## Transformation and Capabilities

**20** Small Satellites with Large Exposure  
*How Does New Space Fare in Cyberspace?*

**28** Enhancing NATO's Strategic Edge  
*A Human-Centric Approach to Multi-Domain Operations*

**36** Quantum Technologies for Air and Space (Part 3 of 3)  
*Quantum for ISR and PNT: Use Cases and Timelines*

**44** Hosted Satellite Payloads  
*NATO's Strategic Pathway to Space Resilience*

## Viewpoints

**52** Bending the 'Hufnagel'  
*Defence Acquisition Principles for the New Security and Technology Environment*

**61** The Evolving Context for Deterrence  
*Technology and Policy Challenges*

**69** Technology and Trust  
*Interoperability for NATO's Multi-Domain Operations and US Combined Joint All Domain Command and Control*

## Out of the Box

**77** Non-Lethal Measures of Effectiveness in Targeting



28



44

## Inside the JAPCC

86

### The Joint Air and Space Power Think Tank Forum

*Adapting to the Evolving Landscape of Modern Warfare*

#### Spotlight on Success

*JAPCC Showcases its Achievements at the 2024 NATO COE Marketplace*

#### 2024 SC/SRC Meetings with Sponsoring Nations

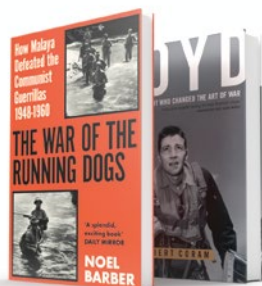
*Realigning JAPCC Priorities through Collaborative Efforts*

## Book Reviews

90

### 'The War of the Running Dogs – Malaya 1948–1960'

'Boyd – The Fighter Pilot Who Changed the Art of War'



## Imprint

### Transforming Joint Air & Space Power:

The Journal of the Joint Air Power Competence Centre (JAPCC)

#### Director

General James B. Hecker

#### Executive Director

Lieutenant General Thorsten Poschwatta

#### Assistant Director

Air Commodore Paul Herber

#### Editor

Colonel Matthew E. Hanson

#### Assistant Editors

Major Tamás Oszlár, Captain Lucas J. Stensberg

#### Production and Advertising Manager

Mr Simon J. Ingram

#### Editorial Review Team

Colonel Markus Müller, Colonel Maurizio De Angelis, Colonel Tyler Niebuhr, Colonel Kevin Anderson, Commander Aaron Shiffer, 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](http://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.

#### Copyrights







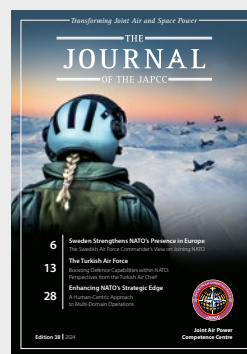
Front Cover |  © Jesper Sundström/Swedish Air Force

Table of Contents | Ad 28:  © K\_E\_N/Shutterstock.com; Ad 44:  © Andrei Armiagov/Shutterstock.com; Ad 52:  © Hamara/Shutterstock.com; Ad 69:  © Gorodenkoff/Shutterstock.com; Ad 77:  © Jets/Background: © Mike Mareen/Shutterstock.com, Network Pattern: © Irvin 2809 – stockadobe.com


**Cover Photo:** A Swedish pilot stands watchful as Saab JAS 39 Gripen jets soar in a perfect formation against the breathtaking backdrop of Sweden's picturesque landscape. This captivating montage encapsulates Sweden's recent integration into NATO, showcasing its advanced air capabilities and steadfast dedication to the Alliance. This momentous occasion signifies a pivotal point in history as Sweden enhances NATO's influence in the Nordic region, demonstrating the preparedness and unity of the Swedish Air Force along with its unwavering commitment to bolstering collective security.



# Sweden Strengthens NATO's Presence in Europe

*The Swedish Air Force Commander's View on Joining NATO*

By Major General Jonas Wikman, Commander of the Swedish Air Force



“*The great strength of an alliance and air power stems from mutual trust and the shared belief that synergies arise when one seeks, without prestige, ways to enhance others’ strengths and compensate for each other’s weaknesses.*”

*Welcome to NATO. Although the process took a little longer than planned, it really was a rapid change from the status quo. How did you use the time to prepare for accession into NATO, and what are your priorities as the new Chief of the Air Force?*

Thank you! We have worked hard to be as prepared as possible. These past 18 months have truly been something extraordinary both for the Air Force and for me as Air Chief. First, I want to take this opportunity to thank everyone for their support. This support has been significant for us and has certainly demonstrated the strength of having allies.

The initial focus for our integration team was to establish and optimize connectivity. More than twenty years of active partnership, participation in numerous exercises, and fruitful bilateral collaborations have contributed to interoperable tactics, techniques, and procedures. We aim for day-zero connectivity to achieve day-zero readiness.

To prioritize and balance the overall workload in the Air Force, we have focused on four lines of effort: current operations, capability development, support to Ukraine, and accession into NATO. The Air Staff and units have collaborated to create synergies between these lines of effort. One notable example is our participation in multilateral combat readiness training alongside our NATO Allies. This multinational approach not only enhances our preparedness but also deepens our understanding of NATO’s procedures and requirements.

The Swedish support for Ukraine has been carefully coordinated with our own capability development. For example, the procurement of AEW&C aircraft S 106 GlobalEye has not only enhanced our own capabilities, but has also allowed us to supply Ukraine with two ASC 890 AEW&C aircraft.

*It’s only been three months since your ratification as a NATO member, but what is your initial impression and what constitutes the most significant changes for Swedish Air Force as a NATO member?*

The great strength of an alliance and air power stems from mutual trust and the shared belief that synergies arise when one seeks, without prestige, ways to enhance others’ strengths and compensate for each other’s weaknesses. I perceive that this attitude prospers within NATO, and it is something I greatly appreciate. We got off to a very good start!

One thing became clear to us early in the process: we needed to adjust our overall concept. Sweden is transitioning from a national doctrine based on a strong defensive capability to absorb an attack and follow up with a counter-offensive. We are now entering an international deterrence and defence context. This marks a significant change in our security policy.

As a member of NATO, it is imperative that we reassess our defensive strategies and adopt a more proactive approach as part of our collective defence concept. We can no longer rely solely on a reactive, bullet-for-bullet approach.

The Swedish Joint Staff is developing a new defence concept based on three core principles: protection, concentration, and effects. These founding principles translate well into the tactical level and our new operational concept for the Air Force.

In the Air Force, our primary goal is to uphold our national excellence as a valued allied partner in support of the joint concept. Our legacy capabilities with operational relevance for the future will be adapted into an allied context. Our capability development will focus on both national and Alliance needs to reach the requirements and assigned capability targets. With the integration into NATO IAMD, our air base concept must be even more resilient. Robust air bases enable extensive deployment of forces for combined air operations to address the military challenges in the north, both from Swedish main operating bases and dispersed airbases.

*Please describe the strengths of the Swedish Air Force and what capabilities you bring to NATO.*


The Swedish Air Force is a modern, well-trained, and adaptable military organization. Our previous policy of non-alignment has shaped our capabilities today,

as we had to rely solely on our own resources and expertise. This led us to develop a diverse set of capabilities that are unmatched by many countries of similar size. However, this self-reliance has also posed challenges for us; as a small nation, we have not been able to invest in specialized capabilities, such as air-to-air refuelling platforms or strategic UAVs. In this regard, joining NATO offers us an exceptional opportunity to address these limitations. By collaborating with other nations and pooling resources, we can combine our existing strengths with those of our new allies.

We embody a warfighting culture, characterized by a can-do spirit that thrives on overcoming challenges. Our Air Force culture is influenced by the asymmetry inherent in our previous policy of non-alignment. Similar to Finland, Sweden was compelled to adapt with doctrinal, conceptual, and technological flexibility in order to meet the existential threat nearby. The innovative solutions we devised were truly groundbreaking, as they were forged under the intense pressure of a complex and demanding operational environment.

Now we all share a challenging operational environment where our bases are no longer the safe havens they used to be. NATO needs to be more agile and become more unpredictable to effectively counter our adversaries. Sweden has a long history of conducting air operations from dispersed bases; in effect we have practiced Agile Combat Employment since 1960. This extensive experience provides valuable insights that can be leveraged in developing future



 © Jesper Sundström/Swedish Air Force



concepts to improve mobility and protection, both of which are essential for NATO's collective defence.

Another key aspect is that our units use conscripts as extensively as possible for a wide range of skilled tasks. This approach allows us to transform young men and women into skilled, multi-capable airmen in a very short period of time. We reinstated conscription in 2017 after a period of dormancy, and the results have been highly successful. After a few months of training, a team consisting of five conscripts and one supervising officer stationed at a remote road base can efficiently execute a tactical turn-around on a Gripen aircraft for air-to-air missions in just 15 minutes.

Our expertise lies in air operations in the High North where darkness, snow, and cold often impact our missions. Rest assured that we are committed to do everything necessary to become as proficient as possible in 360° operations across NATO's entire area of interest. Strong alliances are built on trust and loyalty, and our new Allies can count on the Swedish Air Force.

*As you mentioned earlier, one prioritized capability is air defence. How are you adapting your forces to be a part of NATO's IAMD?*

IAMD, with both its offensive and defensive components, forms the foundation of the Swedish Air Force's future operating concept. With our NATO membership, a shift towards a more offensive posture will be possible, making our air defence more well-rounded.

It starts with connectivity, whether between NATO Allies, other countries, or within our own Armed Forces. I will not be satisfied until we can seamlessly transmit data between any platform in any domain, creating a unified kill-web. We aim to support cross-domain targeting by integrating space-based sensors with surface-based shooters, fostering a multi-domain and multi-national approach. Sweden has the necessary systems that makes this possible. However, the focus must be on coordinating and connecting these systems to form a cohesive network, rather than allowing them to remain isolated.

*With the complex and evolving security landscape, there is growing interest in enhanced regional co-operation. Could you elaborate on how the Swedish Air Force is contributing to the development of the Nordic air power concept, and what benefits do you foresee from this collaboration for regional security in the High North? Please explain how Nordic Defence Cooperation (NORDEFCO) bolsters NATO rather than providing competition?*

I want to emphasize that the Nordic Air Power Concept is in no way an alternative to or a competitor of NATO. We are committed to contribute to NATO's collective defence in the most effective and responsive way possible. The concept gives us the opportunity to operate together before 'day one', and ensure our capabilities are fully integrated within NATO and can be deployed in any direction as needed.



*Technical personnel from the 11<sup>th</sup> Maintenance Company prepare JAS 39s of the Skaraborg Wing for their return flight back to Sâtenäs from Luleå after Exercise Nordic Response.*

The Nordic countries share a common understanding of the military challenges in our region. From both political and military perspectives, there is great consensus on how we can and should address future conflicts in the Nordic region. Geographical conditions, similar strategic cultures, and comparable economic conditions create a natural basis for a common Nordic defence concept.

The Nordic Air Power Concept is in the initial implementation phase, and the Nordic air chiefs have delegated extensive authority to our respective planners. It is crucial that we work expeditiously to keep pace with the current security situation.

NATO membership has removed the invisible barriers that our previous non-alignment and national borders created, allowing our air forces to fully utilize their strategic potential and enhance our contribution to deterrence.

National operational plans and NATO remain the foundation for Nordic joint air operations. The Nordic air forces will achieve the ability to plan and conduct joint air operations as one force, with day-zero readiness. A key component is the establishment of capabilities for distributed command and control.

Nordic cooperation will create synergies in future multi-domain operations. Denmark, Norway, and soon Finland flying low-observable F-35s and deep precision strike capability will combine with Swedish Gripen aircraft featuring state-of-the-art Electronic Warfare (EW) systems, long-range anti-surface missiles, and outstanding availability from dispersed airbases. Our new AEW&C aircraft, the S 106 GlobalEye, serves as the C2 hub that enables multi-domain SA for cross-domain operations and targeting. We have just finalized our Nordic seamless air defence network for radar data exchange. This allows us to share real-time data and it significantly enhances our SA and early warning.

The NORDEFSCO also eases the implementation of new strategic initiatives for defence material procurement. Possible areas of cooperation include tactical airlift, air-to-air refueling aircraft, AEW&C, and advanced

unmanned ISR platforms. These collaborations allow each country to access resources and capabilities that would have been financially out of reach if pursued individually.

### *How is the Swedish Air Force adapting to the rapid changes in the operational and technological landscape?*

Adaptation and innovation are indeed essential for us. We are actively engaged in developing next-generation aircraft, sensors, airbase concepts, and enhancing our space capabilities. However, our pace is too slow. We must reclaim the drive that once marked our air force: the desire to evolve through the power of innovation. Years of missed investments have affected our ability to develop and acquire new technologies. During years of budget cuts and savings, innovation was not rewarded, leading to a stagnation that we must overcome. We must improve our ability to develop new capabilities. This is a matter of great importance to me, and we have several initiatives in the works to stimulate innovation and accelerate development. This will be essential in preparing for the challenges of the future operational environment. We cannot afford to rely on projects that take 15 years to move from conception to capability.

### *Speaking of future projects, could you share insights into any upcoming initiatives in Sweden?*

Our focus is not only on acquiring new aircraft and helicopters, but also on upgrading our existing fleet, such as enhancements in sensors, EW, and weapons technology. We are acquiring new active and passive sensors to replace the ground-based early-warning network with a new sensor grid.

The space and cyber domains are indeed becoming increasingly significant. We are in the process of establishing a more robust cyber defence framework to protect our systems and sensitive information. In terms of space, we are establishing a recognized space picture and exploring satellite technology, aiming to launch our first satellite before the end of 2029.



M Fighter Jets: © Jesper Sundström/Swedish Air Force; Sky: © 1xpert – stock.adobe.com; Flare: © jangnhut – stock.adobe.com

*Swedish Air Force JAS 39s on the flightline at Luleå Air Base, home of the Norrbotten Wing, ready for Exercise Nordic Response 2024.*

Due to the general importance of combat air capabilities, combined with the required resources and long time-scales, Sweden has launched a national concept programme (SWAP) for assessing future solutions for combat air capabilities. The programme will create knowledge necessary to support an informed decision on how to ensure long-term access to combat air capabilities into the 2060s and beyond. While it is too early to discuss specifics about the core platform, current trends point us in a clear direction: Whether we opt to develop or acquire, you will recognize ‘the Swedish DNA’ in our next fighter system. International cooperation will be a necessary part of any future solution, regardless of nominal supply option.

*It will be interesting to follow Sweden’s progress integrating into NATO. Finally, how do the current developments in Ukraine and in the Middle East affect your concept and capability development?*

I follow the Ukrainian armed forces’ fight against Russian aggression with deep admiration. The Ukrainian

military’s ability to conduct both defensive and offensive operations, while simultaneously innovating and adapting, truly astounds me. Our military support to Ukraine is a central part of Swedish defence policy and probably the most important investment we can make in our future security. It is imperative that our support remains robust and sustained over the course of several years.

We are continuously refining our TTPs and developing our CONOPS based on what we see on the battlefield in Ukraine. Our readiness and progress in various aspects, such as implementing our airbase concept and tailoring our Gripen operating concept. Agile employment to our dispersed bases serves to mitigate attacks by ballistic and cruise missiles.

We are enhancing our capabilities in Electronic Attack and Deep Precision Strike to shift our focus from Defensive Counter-Air to include Offensive Counter-Air. However, there is still more work to be done. Our capability to counter attacks that combine both

sophisticated high-end weapon systems and basic, low-cost weapons requires improvement. We must field a range of defensive capabilities, balancing cost, capability, and quantity against diverse threats such as those demonstrated in Ukraine.

Assuming that future wars will be the same as this one is hazardous. One conclusion is clear and obvious to us: the operational environment changes rapidly, demanding constant tactical adaptation and ongoing development throughout a conflict. Innovation and adaptability are core requirements for our future warfighting concept.

Finally, the current situation in the Middle East is a cause for concern, and we are diligently monitoring its developments. One valuable takeaway from recent events is the impressive performance of our western air defence systems. The defensive capabilities demonstrated by Israel and its allies have been nothing short of remarkable. They have effectively handled a

combination of high-end and low-end threats through allied connectivity and effective targeting and sorting. This success indicates that control of the air remains both relevant and feasible. By ensuring our air defence systems are readily available, persistent, multi-domain, and integrated, we can effectively protect against a wide range of threats.

### *Do you have any final remarks about joining NATO?*

In conclusion, let me re-state how proud I am of the men and women of the Swedish Air Force during this period of rapid change in our mission. I am confident our new allies will appreciate their professionalism and dedication as we our nations continue to learn from one another. Sweden is proud to be NATO's newest member, and we are committed to the goal of peace through cooperation and credible deterrence. It is a fitting celebration to join this historic Alliance on the occasion of its 75<sup>th</sup> anniversary. Thank you all for the warm welcome to the NATO family. ●

---

#### ABOUT THE AUTHOR

---



© Louise Levin/Swedish Air Force

### Major General Jonas Wikman

Commander of the Swedish Air Force

Major General Jonas Wikman graduated from the Air Force Flying Training School in 1993 and began his career as a light attack pilot and flight instructor. He transitioned to flying the J-35 Draken and later the JAS 39 Gripen. Throughout his career as a fighter pilot, General Wikman contributed to the development of the man-machine interface for aircrew. He also gained experience in aviation medicine, eventually serving as Head of the Armed Forces Aeromedical Centre. After completing the advanced command course at the Swedish Defence University in 2009, Jonas Wikman served in the Plans and Finance Department of the Defence Staff. In 2012, he became Commanding Officer of the Flight Test Centre in Linköping.

Two years later, he was appointed Chief of Plans in the Joint Force Generation Command. In 2016, Jonas Wikman became the Senior Air Advisor to the NATO Resolute Support Mission in Kabul, Afghanistan. He was subsequently promoted to Brigadier General and appointed Chief of the Joint Materiel and Support Directorate, as well as Assistant Chief of the Joint Force Generation Command. In 2021, he was promoted to Major General and appointed Deputy Chief of Joint Operations where he gained experience during the evacuation operation from Afghanistan and the events surrounding the Russian full-scale invasion of Ukraine. He held this position until assuming his current command in December 2022.

# The Turkish Air Force

## *Boosting Defence Capabilities within NATO: Perspectives from the Turkish Air Chief*

By General Ziya Cemal Kadiođlu, Commander of the Turkish Air Force

‘Türkiye plays a crucial role in maintaining regional stability through its efforts to deter security threats using its military capabilities.’

*What are the current air and space capability developments in the Turkish Air Force?*

Before I get into the details of the capability development roadmap, I would like to summarize the Turkish Air Force (TÜ AF) concept mindset with some examples. The TÜ AF has initiated modernization and R&D projects with a roadmap through 2050 to enhance its operational effectiveness and acquire advanced capabilities, leveraging cutting-edge systems and platforms. Our ambitious project roadmap focuses on the development of aircraft systems, such as the fifth generation KAAN low visible, multi-role fighter aircraft, trainers such as HÜRKUŞ and HÜRJET aircraft and GÖKBEY helicopter, and Unmanned Aerial Vehicle (UAV) systems such as ANKA, AKINCI, AKSUNGUR, BAYRAKTAR TB3, and KIZILELMA. When it comes to space capabilities, our priority is to enhance our existing space-based ISR capability, and our space projects are initiated accordingly. Furthermore, our air and missile defence concept is being bolstered by HİSAR and SİPER air defence missile systems, as augmented by next-generation Early Warning Radar systems.

A forthcoming procurement initiative is set to replace the T-38M, which is expected to be completely phased out of service by the mid-2030s, with a modern



General Ziya Cemal Kadiođlu, © Turkish Air Force; Turkish flag in background: © Tarik Haiga/Unsplash



*One of Türkiye's milestone projects is developing a fifth-generation fighter aircraft. KAAN successfully completed its maiden flight on 21 February 2024, in Ankara.*



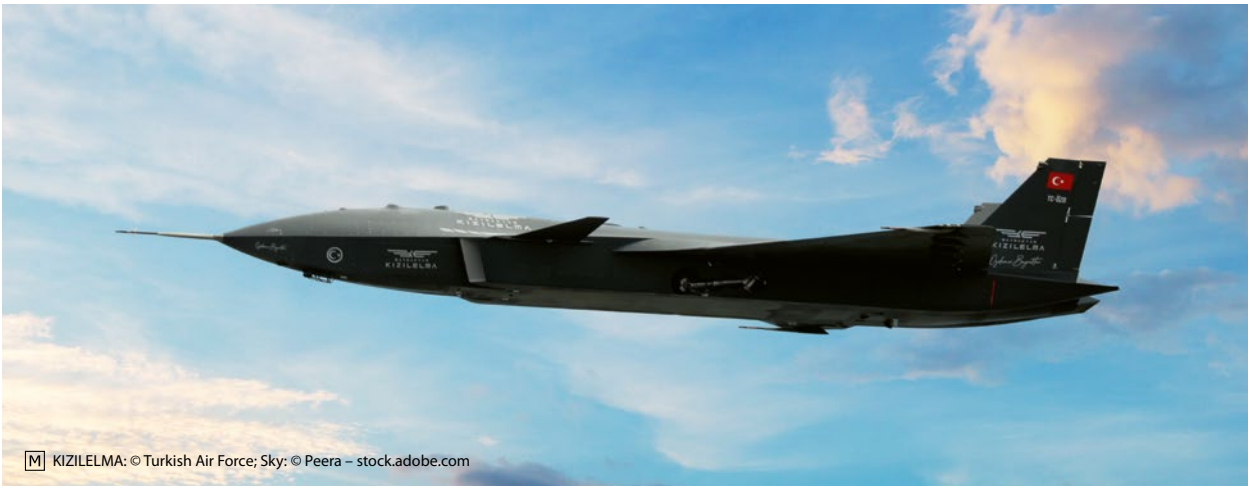
*Air Force Commander General Ziya Cemal KADIOĞLU visited the Turkish Aerospace Industries (TAI) facilities in Ankara on 22 May 2024. During his visit, he had the opportunity to take his first flight in Türkiye's first domestically produced manned jet engine aircraft, the HÜRJET, which had its maiden flight on 25 April 2023.*

trainer aircraft. Specifically, the HÜRJET project seeks to fulfil the requirements for jet training and aerobatic capabilities, thereby ensuring continuous training of pilots and aerobatic team members.

Since 2018, the TÜ AF has been operationally utilizing UAV systems designed and developed with national capabilities to meet reconnaissance and surveillance needs. The procurement of high-altitude UAV platforms, including AKINCI and AKSUNGUR, has enabled the TÜ AF to expand its capacity in close air

support, air-to-ground attack, and electronic warfare missions. These platforms have remarkably enhanced ammunition and payload-carrying capacities. Currently, the development of next-generation stealth UAV systems, including ANKA-3 and KIZILELMA is still ongoing.

In alignment with the fundamental principles of peaceful and defensive utilization of space, and consistent with international best practices, we have identified key areas for capability development. These



*The Bayraktar KIZILELMA Combat Unmanned Aircraft System is planned to be a force multiplier for the Turkish Air Force with its low visibility capability and capacity to conduct air-air combat. On 14 December 2022, KIZILELMA made its first flight.*

areas include force development, space support, and space control. In order to protect our national space assets against threats and hazards, we have recently established our own Space Command under the Turkish Air Force. The space project roadmap consists of space-based Electro-Optical (EO) and Synthetic Aperture Radar (SAR), electronic support, regional Positioning, Navigation, and Timing (PNT), and early warning satellite systems. We are aware of the fact that space domain awareness is the key to space warfare, and we are planning to have our own space situational awareness capability.

#### *What are the current challenges the TÜ AF is facing?*

As other NATO nations, we face common global challenges, including health crises, climate change, and social issues that necessitate a multidisciplinary approach that encompasses both security and economic considerations. Furthermore, we are witnessing a profound shift towards an information and technology-driven society, precipitated by the cumulative effects of globalization and digitization, which demands a comprehensive understanding of the interconnected nature of these developments.

Furthermore, we carefully consider these factors and incorporate lessons learned into training protocols to

mitigate the impact of climate change on operational capability. Our Search and Rescue units are actively engaged in responding to natural disasters, which necessitates continuous updates to our operational approach. Moreover, our humanitarian aid mission effectiveness has also been enhanced through this adaptive strategy.

The individual and societal benefits associated with these factors are integrated into training programs to ensure that operational capacity is not compromised in environments affected by climate change and health issues. Our units continually refine their operational protocols to adapt to increasing natural disasters such as floods and earthquakes. This has been particularly evident in the wake of recent earthquake disasters that have significantly impacted our country, yielding valuable lessons learned and the development of new projects.

It is imperative to establish a military force structure comprising a judiciously allocated number of personnel with high mobility and firepower, capable of rendering both direct and indirect support to international operations. This force should be equipped with weapon systems that are commensurate with the technological advancements of the present era, enabling effective and efficient execution of its mandate.

A personnel structure integrated with its corporate culture and trained in accordance with current developments is a valuable asset that cannot be replicated or replaced by competitors. The first element of our success in the 21<sup>st</sup> century, where our understanding of security and our mission types are diversified and uncertain, is a very well-equipped and psychologically resilient workforce. In light of the evolving needs of the modern age, the importance of modern weapons systems is becoming increasingly apparent. The ability to operate, use, and manage these systems effectively, and make the right decisions in complex battlefield conditions, is becoming a crucial skill for personnel. In addition, the role of commanders in directing and managing these systems turns is increasingly significant. The personnel structure in the 21<sup>st</sup> century should be more flexible, agile, and professional.

The proliferation of weapons systems to terrorist groups has created new challenges, as they can now employ unconventional tactics with devastating effects. This development underscores the need for militaries to adopt asymmetric strategies and enhance command and control relationships to effectively counter these unconventional threats.

The increasing globalization of the satellite and aerospace industry has resulted in a scenario where various countries with established space programs can now manufacture key subsystems, ground systems, and components. This development has led to a reliance on a limited number of suppliers, thereby increasing the risk of supply chain disruptions and potential project delays. Consequently, it is essential to develop alternative logistics strategies for the space and aerospace sectors to mitigate these risks and ensure the timely delivery of critical products and services.

Investing in the space domain has been hindered by the scarcity of trained professionals in this field, as well as the significant resource requirements arising from the incorporation of cutting-edge technologies into the systems, subsystems, and components utilized.

*How would you assess the global and regional situation around Türkiye, and the air and space contributions of the TÜ AF to ongoing NATO operations and missions?*

Located in the southeastern wing of NATO, Türkiye faces a unique set of security challenges due to its proximity to a complex regional environment marked by interstate competition and terrorism. Despite these challenges, Türkiye plays a crucial role in maintaining regional stability through its efforts to deter security threats using its military capabilities. The global security environment is closely monitored, and transformative studies are conducted to enable the TÜ AF to respond effectively to emerging challenges in a timely manner.

NATO actively promotes international peace and security, remaining vigilant and engaged in global affairs. The TÜ AF is recognized by NATO as a vital contributor to the





Alliance's operational capability. Through collaborative efforts with NATO members, the TÜ AF is committed to supporting Alliance operations and missions, with all units adhering to NATO's rigorous training and operational standards. The TÜ AF organizational structure is harmonized with the NATO Defence Planning Process, ensuring cooperation and coordination with other stakeholders.

We place significant emphasis on supporting the NATO Warfighting Capstone Concept (NWCC) initiative undertaken by NATO Allied Command Transformation, specifically adhering to the Warfare Development Agenda (WDA). Based on the lessons derived from these efforts,

we prioritize enhancing our transformation pace and optimizing the combat readiness of our troops through a rigorous and standardized certification process.

Upon the 72<sup>nd</sup> anniversary of Türkiye's accession into NATO, we remain committed to upholding NATO's values and core mission, just as we always have. In line with the principles of fair burden sharing, the TÜ AF has been actively engaged in various NATO endeavours, including contributions to the NATO New Force Model and Allied Reaction Force. TÜ AF personnel have been deployed to support NATO Mission Iraq (NMI) and Kosovo Forces (KFOR), while also participating in NATO exercises and peacekeeping operations through Enhanced Air Policing, Airborne Early Warning, and Air-to-Air Refuelling missions. Additionally, as an alternate Joint Force Air Component Command (TÜ JFACC), the TÜ AF aims to assume increased responsibility within the Alliance in the near future.

The TÜ AF has been actively supporting NATO space activities since 2012. We are fully engaged in the NATO space domain implementation plan, and we display this effort by sending our space SMEs to space-related NATO exercises, contributing to space doctrine development efforts, and filling our billets within the NATO Command Structure/NATO Force Structure (NCS/NFS) space C2 structure. We provide high-resolution space-based E/O imagery to fulfil NATO joint ISR, Find, Fix, Track, Target, Engage, Exploit and Assess (F2T2E2A), and focused collection activity requests. And finally, we are one of the 15 nations that established the NATO Space Centre of Excellence in Toulouse, France. Once the Turkish Space Command reaches its full operational capability, it will contribute to other space operational functional areas besides space-based ISR.

*What are your insights on the future of NATO's joint air and space power capabilities, and what roles do you envision the Turkish Air Force fulfilling?*

The advent of advanced technologies has not only brought about numerous benefits; it also poses significant security concerns for NATO. The proliferation of hypersonic missiles, coupled with the emergence of cyber and asymmetric threats, presents a formidable challenge to both neighbouring countries and the

*The Turkish Air Force AEW&C aircraft (E-7T) and the Turkish Stars Aerobatic Team are stationed at the 3<sup>rd</sup> Main Jet Base Command (Konya) of the Turkish Air Force.*



M © Turkish Air Force

*The ANKA-III High Altitude Long Endurance (HALE) Unmanned Combat Aircraft is designed to operate at an altitude of 40,000 feet, achieve a speed of Mach 0.7, and sustain flight for up to 10 hours. This cutting-edge aircraft completed its inaugural flight on 28 December 2023.*

Alliance. To effectively mitigate these threats, NATO must undergo a rapid adaptation process across all domains and proactively prepare for future security risks in order to safeguard the territory and personnel of the Alliance.

To effectively counter and deter potential threats, NATO needs to prioritize the attainment of information superiority, which can be achieved by gaining access to critical information before adversaries and leveraging this advantage to inform decision-making. Developing a robust Joint Air Command and Control (JAC2)

structure of the future is crucial in this regard, necessitating integration of innovative technologies such as Artificial Intelligence (AI), cloud computing, and big data analytics to expedite and enhance the decision-making process.

Adopting cloud technology is expected to facilitate a paradigm shift from a single, monolithic platform to a system of systems architecture, ultimately enabling the realization of a Multi-Domain/Joint All-Domain environment. This transformation will likely lead to an accelerated operational tempo and decision-making



M © Turkish Air Force

*The Turkish Air Force successfully completed the NATO Enhanced Air Policing (eAP) mission using four F-16 aircraft at Borcea (Fetești) Base in Romania from 1 December 2023 to 31 March 2024.*

---

**[...]** *‘TÜ AF plays a crucial role within NATO and its regional context, being dedicated to upholding its responsibilities.’*

---

processes, as AI will be integrated to support critical decision points. Moreover, it is anticipated that a unified information architecture will be established, providing a single, comprehensive information set for all decision-makers, thereby ensuring information superiority and a unified operational picture across all domains promoting decision superiority.

The TÜ AF plays a crucial role within NATO and its regional context, being dedicated to upholding its responsibilities. To maintain its status as a formidable and deterrent force, the TÜ AF prioritizes the development of a robust and sustainable air and space power infrastructure, recognizing the imperative for continued adaptability and competitiveness in an evolving security landscape.

Through participation in global missions and joint exercises, our military has been actively engaging in efforts to enhance interoperability with NATO forces, prioritizing collaboration in the domains of air and space power. As we envision the Joint Air and Space Force of the future, we recognize ourselves as a crucial component, poised to leverage our capabilities to foster enhanced cooperation and adapt to an evolving operational landscape.

The TÜ AF has maintained its efficacy and deterrent presence in its region, adaptively incorporating new technologies to enhance its capabilities. Over the next decade, the TÜ AF’s expertise in joint operations will continue to have a significant impact, particularly in the development of cutting-edge air defence, command and control systems, UAVs, radar systems, and combat aircraft projects. Moreover, the implementation of advanced Ballistic Missile Defense (BMD) and Integrated Air and Missile Defence (IAMD) systems will reinforce regional air defence capabilities, solidifying the TÜ AF’s role as a vital member within NATO. ●

---

**ABOUT THE AUTHOR**

---

**General Ziya Cemal Kadioğlu**

Commander of the Turkish Air Force



General Ziya Cemal Kadioğlu joined the Turkish Air Force in 1978 and graduated from the TÜ AF Academy in 1982. Until 1995, he served as a wingman and instructor jet pilot at Malatya and Eskisehir. After graduating from Air War College in 1997, he performed several duties in 1<sup>st</sup> Air Force Command HQ/Eskisehir, TÜ AF Academy/Istanbul, 1<sup>st</sup> Main Jet Base/Eskisehir, and NCO College Regiment/Izmir. Promoting to Brigadier General in 2007, he served as the 11<sup>th</sup> Air Transportation Base Commander and TÜ AF Intelligence-Planning Management Director in Ankara. In 2011, he was promoted to Major General and served as Air

Force Intelligence Department Head/Ankara, then the Air Force Technical Schools Commander/Izmir. Following promotion to Lieutenant General in 2015, he served as the Deputy of Combatant Air Force and CAOCs Commander/Diyarbakir, Chief of Evaluation and Inspection Department/Ankara and Air Force Training Commander/Izmir. He was promoted to General in 2022. Following his promotion, he was appointed as the Combatant Air Force Commander. With a wide spectrum of expertise and 4,800 flight hours, General KADIOĞLU has been the Turkish Air Force Commander since August 2023.

# Small Satellites with Large Exposure

## *How Does New Space Fare in Cyberspace?*

By Captain Luke Stensberg, US Space Force, JAPCC

### **The Advent of Small Satellites**

In recent years, both public and private actors have embraced innovations in the space industry that have allowed for a democratization of space, known colloquially as *new space*. New space consists of various advancements that improve cost efficiency and accelerate development cycles, opening the door for new actors to access space. One prominent new space trend is small satellites, characterized by many, individually lesser-valued satellites that comprise a scalable and meshed constellation, typically in Low-Earth Orbit (LEO). Together they reduce latency due to their proximity to Earth and can offer robust coverage when adequately scaled.

The emergence of small satellites represents a significant departure from the traditional space operations conducted by large governmental organizations. Historically, these organizations would deploy exquisite capabilities in Geostationary Orbit (GEO), which was financially and technologically inaccessible to smaller players. Nowadays, new actors are emerging who can quickly and affordably procure or develop small satellites that leverage standardized and miniaturized Commercial Off the Shelf (COTS) components, piggyback on other launches, and even Command and Control (C2) missions with web-accessible ground infrastructure.<sup>1</sup> These advancements lower the need for full vertical integration, significantly cutting development barriers and overhead.

Besides development speed and cost savings, small satellite LEO architectures inherently offer operational resilience through their proliferation. For example, an adversary cannot easily deny space capabilities kinetically when many more satellites share the load in delivering the mission's Data, Products, and Services





(DPS). Destroying one or even several small satellites would, at most, degrade said DPS. Beyond this, scaling up kinetic strikes to destroy the preponderance of these small satellites – enough to significantly degrade or fully deny the capability – is not as practical and could risk an ever-escalating positive feedback loop of debris yielding indiscriminate collateral damage. This could potentially reach the point of the Kessler Effect, in which LEO becomes hazardous for all space actors, friend and foe alike.<sup>2</sup> Surely, proliferated constellations tilt the cost-benefit analysis of kinetic-minded aggressors enough to think twice about taking on proliferated small satellite constellations in this manner. Consequently, a top US space official recently claimed that satellites are more likely to be targeted through non-kinetic means, specifically through the cyber domain.<sup>3</sup>

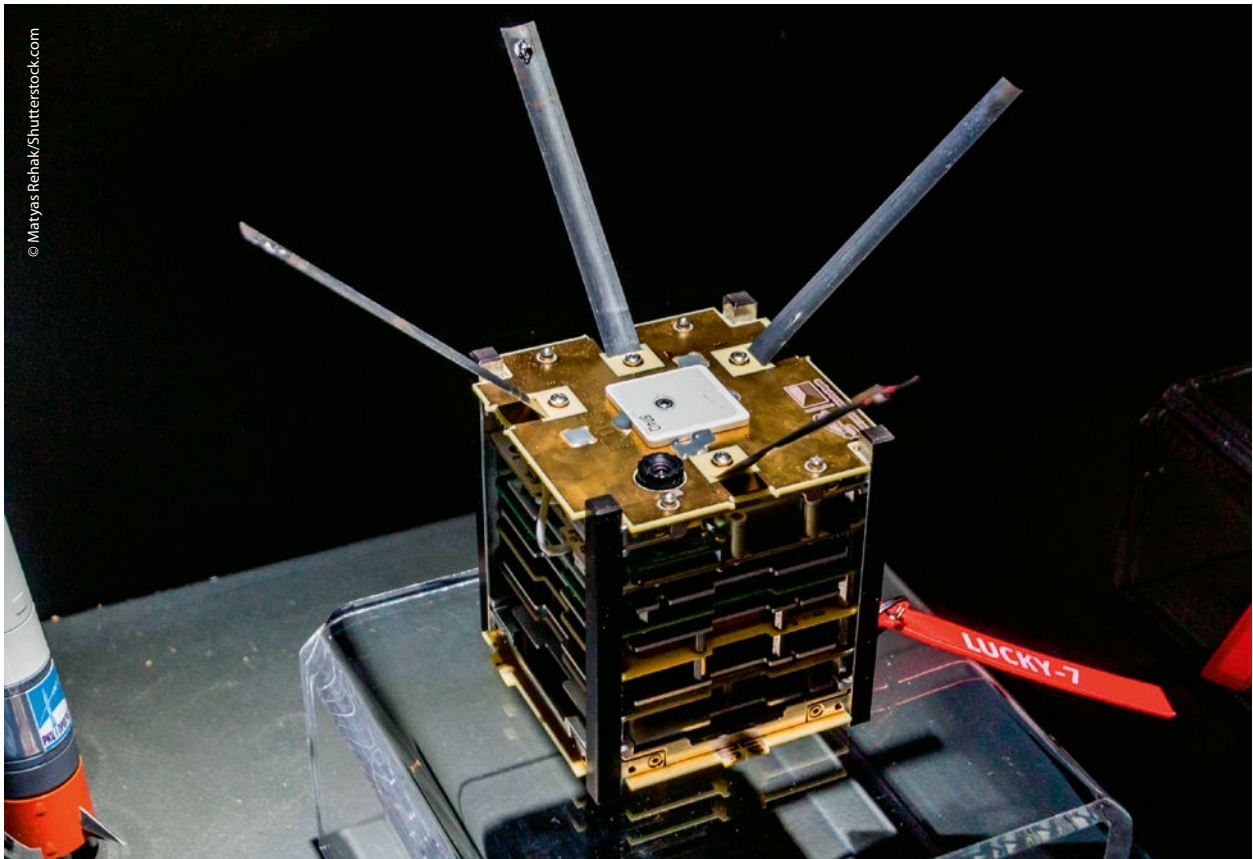
---

**[...]** *'As the space domain becomes more intertwined with the cyber domain to lower costs and increase convenience, the benefits may come with the additional risks inherent to cyberspace.'*

---

### **The Risk of Small Satellites in Cyberspace**

Small satellite designs focus on affordability, simplicity, and standardization to promote scalability. This trend has even paved the way for the CubeSat concept. CubeSats are a subset of nanosatellites based on one or more 10x10x10 cm units (1U) that often utilize widely available and standardized components. These can be stand-alone or modular since multiple units, for example, three 1Us, may form a larger 3U CubeSat. Despite relative simplicity in design, small satellites can scale in numbers to produce constellations that can provide key DPS to NATO warfighters such as C2, ISR, and more. However, cybersecurity experts are warning that this ease of development, scalability, and operations may encourage potential design shortcuts that bring cybersecurity trade-offs.<sup>4</sup> Interconnectivity and standardization can diminish the obscurity of space systems, which once deterred malicious cyber actors from targeting such historically foreign systems.



*A one unit (1U) CubeSat typically weighs less than 2 kg and is relatively cheap, thanks to its reliance on COTS components.*

These shifts in design are analogous to when industry began enabling remote access for Industrial Control Systems (ICS) to control water, energy, manufacturing, and logistical processes. While remote management improved ICSs' operational efficiency, it is evident many ICS systems were hastily networked, often neglecting cybersecurity. Recently, a cybersecurity firm reported that their ICS honeypots – decoy networks designed to mimic real networks to lure attackers – detected an average of 813 unique attacks daily. This is an alarming indicator because there is no current patch or remediation for 34% of ICS cybersecurity vulnerabilities in 2023, up from 13% in 2022.<sup>5</sup> At the strategic level, vulnerabilities in critical national infrastructure now pose geopolitical risk, as evidenced by the Five Eyes nations recently condemning China for targeting US infrastructure with malicious cyber activity.<sup>6</sup>

Therefore, the broader space community, both public and private, must balance their pace of innovation with

cybersecurity to avoid ending up as vulnerable in cyberspace as terrestrial ICSs are. Implementing cybersecurity as an afterthought is less effective and more expensive reactively than if done proactively. Meanwhile, as the space industry is rapidly growing at 9% per annum with projections to reach \$1.8 trillion by 2035, this target-rich environment will surely attract malicious cyber actors.<sup>7</sup> If NATO nations decide to increase their reliance on small satellites, they need to understand how one cyber-attack could massively impact operations across multiple domains.

### **Security (Challenges) From the Ground Up**

NATO defines space as possessing four segments: ground, user, link, and space.<sup>8</sup> All segments are crucial, so if a cyber actor can deny, degrade, disrupt, or destroy any of them, the entire delivery of space DPS

is impacted. This expands the attack surfaces compared to the mission-relevant terrain of typical terrestrial networks. The following sections examine some new space concepts as they relate to each space segment, along with potential vulnerabilities if left unchecked. This article will only sparingly address the user segment since it is more agnostic to the type of space architecture utilized within this cybersecurity context, be it old or 'new'. For example, Russia's 2022 AcidRain cyber-attack on over 10,000 European Via-Sat modems was user segment-focused, making the types of ViaSat ground stations and satellites irrelevant to the attack.<sup>9</sup>

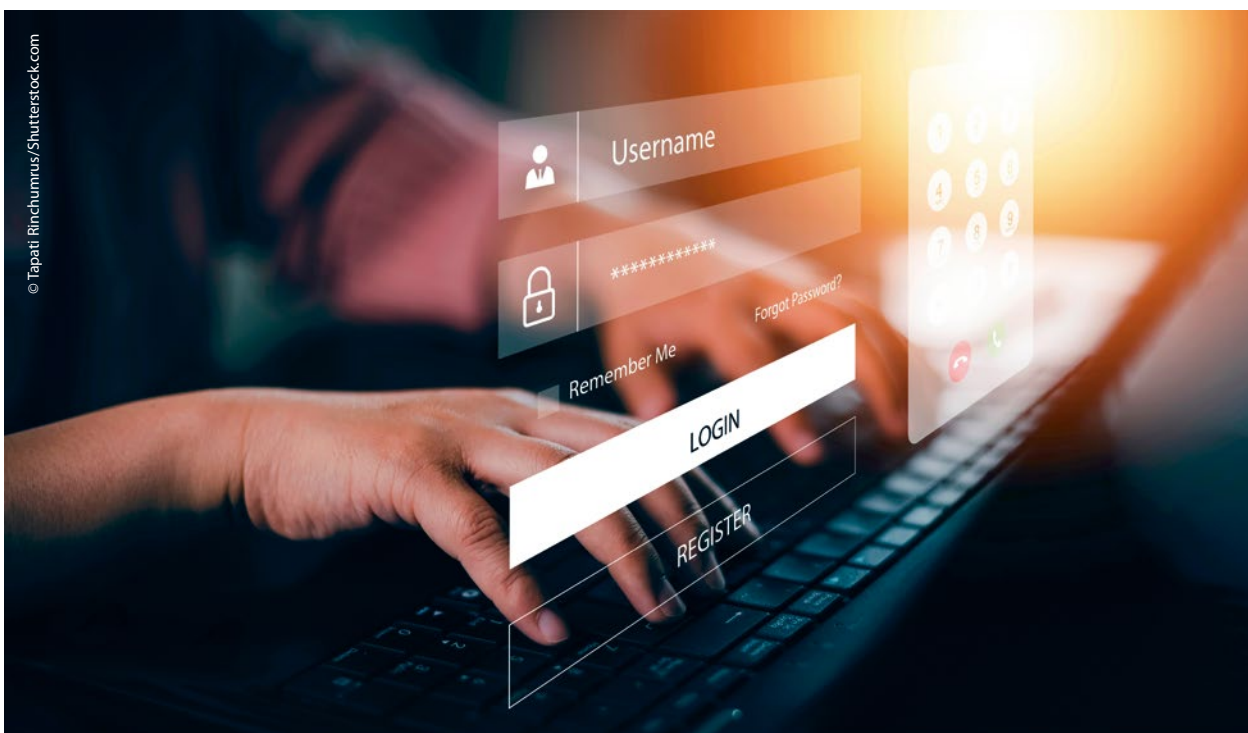
## The Ground and User Segments

Ground stations are required for tracking, C2, and data transmission to and from satellites, so naturally they pose as ripe targets to impact space operations. Any uplinked commands or downlinked tracking and telemetry data will flow with implicit trust between the ground station and satellite due to the (hopefully) encrypted link segment. Therefore, to impact

the spacecraft, malicious cyber actors may look to leverage the ground station as a pathway.

Designing and building a network of ground stations for LEO spacecraft is very expensive. Unlike GEO satellites, which remain relatively stationary from the perspective of a ground station, LEO satellites may move in and out of view in less than 15 minutes due to their high velocity and lower altitudes. Therefore, a LEO constellation may require numerous ground stations scattered globally.<sup>10</sup> This has historically meant unsurmountable up-front infrastructure costs for smaller actors. To respond, large cloud service providers like Amazon Web Services and Microsoft Azure now offer leased access to their own worldwide network of ground station antennae along with cloud computing and web-accessible storage services.

This business model is called Ground Station as a Service (GSaaS), and it allows smaller actors to circumvent substantial initial investments required to build a network of ground stations. Satellite operators pay small usage fees to access a cloud environment that can relay space commands and data via the various



*Technology has advanced to allow for efficient remote access to operational control systems, now including satellites.*



© PX Media – stock.adobe.com

*Data Centres host Ground Station as a Service (GSaaS) command and control services.*

GSaaS antennae to communicate with the satellites. Besides C2, these cloud services can also push the user segments to the cloud by, for example, allowing customers direct access to the satellite imagery.

GSaaS migrates access to satellites from air-gapped, in-house networks to the cloud, expanding the attack surface due to the inability to completely isolate vulnerable assets. While the cloud environment can be very secure, some cloud customers falsely assume that they can outsource all their cybersecurity responsibilities to the cloud providers. In fact, experts estimate that 99% of cloud security failures will be the customer's fault by 2025.<sup>11</sup> Therefore cloud exploitations have already begun as a leading cybersecurity firm published in its 2023 annual report stating that cloud environment intrusions increased 75% over 2022.<sup>12</sup> The most dedicated malicious cyber actors could even theoretically pay to legitimately gain access to GSaaS services, only to conduct their own reconnaissance by probing for vulnerabilities. As the space domain becomes more intertwined with the cyber domain to lower costs and increase convenience, the benefits may come with the additional risks inherent to cyberspace.

## The Link Segment

The link segment is the electromagnetic connection between the ground and user segments to the satellite(s), and satellites to one another. A key development in small satellite communications is the shift from analogue transceivers to digital Software-Defined Radios (SDRs). SDRs are radios in which physical functions normally conducted by hardware are instead executed by software. While affordable and convenient, some commercially available SDRs used by small satellites may have configurable code that has been exploited in realistic lab settings.

In one study, a team of Air Force Institute of Technology researchers simulated a ground station linked to a small satellite with commonly used hardware, open-source software, and an SDR. They were able to glean valid commands from the lab's ground station to prepare their own identically formatted commands. However, they transmitted commands with malevolent adjustments to spoof the satellite's positioning data used to orient itself relative to the sun.<sup>13</sup> Despite the commands originating from an unknown source, the SDR still accepted the attacker's commands



to adjust the satellite attitude improperly. Hypothetically, the malicious commands would have conducted a manoeuvre that could risk damaging solar cells and optical sensors, and would deplete limited propellant. Additionally, other researchers have also highlighted that certain SDR configurations are susceptible to buffer overflow cyber-attacks.<sup>14</sup> This type of attack has disruptive effects analogous to electromagnetic jamming, although with far more subtlety because it does not generate high levels of power that could be geolocated.

---

**[...] *‘There are difficult dilemmas for small satellite designers when prioritizing resources onboard a confined small satellite bus with competing demands. Still, engineers should not overlook the potential total loss of mission due to a cyber-attack.’***

---

Encryption is a computationally intensive process that offers security and is commonplace in terrestrial networks. However, encryption becomes more challenging as satellites get smaller. A recent presentation showcased risks due to weak encryption in the CubeSat Space Protocol, affecting command validation and acceptance.<sup>15</sup> For resource-limited small satellites, lightweight encryption and hashing algorithms like ASCON may be more suitable. Established in 2023 as the National Institute of Standards and Technology’s standard for lightweight cryptography, ASCON is likely a more secure family of algorithms.<sup>16</sup>

There are difficult dilemmas for small satellite designers when prioritizing resources onboard a confined small satellite bus with competing demands. Still, engineers should not overlook the potential total loss of mission due to a cyber-attack. As small satellites in LEO begin to leverage automation to relay commands to one another, any chink in the link segment’s armour can lead to spiralling effects. These vulnerabilities underscore the risk of bolting COTS products together without cybersecurity as a central design requirement.

## The Space Segment

Lastly, the space segment is the orbital component of the space architecture. As satellite development becomes cheaper and faster, small satellites’ use of COTS products and open-source software has effectively made them IoT devices in orbit. Because smaller space operators do not have the resources to institute their own proprietary methods for C2 and data handling, some are leveraging common operating systems and programming languages onboard their satellites (e.g. Linux, Java, and C/C++). This convenience comes with risk because malicious cyber actors are also very familiar with these languages.

If a compromised ground segment sends malicious commands, the satellite may rely on its inherent trust relationship and execute the commands, assuming they are authenticated if properly formatted. Therefore, some experts have called for spacecraft designers to follow suit with terrestrial networks and institute zero trust bases within and between the four segments of space, even onboard the spacecraft themselves. One way to do this is by having intrusion detection software to detect and flag anomalous commands or malicious behaviours.<sup>17</sup> To glean which malicious behaviours may threaten one’s space networks, the Space Information and Sharing Analysis Center is an organization that collaborates on space network vulnerabilities and associated adversarial TTPs. Similarly, the United States Cyber Command’s ‘Under Adversity’ program has shown precedents for how government agencies can share cyber threat reporting at adequate classification levels with industry.

Additionally, if these small satellites continue to use COTS components and open-source software from communal repositories, cybersecurity professionals should be aware of their origins. Supply chain interdiction remains a robust avenue for malicious cyber actors to gain unauthorized access. The US Defense Intelligence Agency has reported that one unit in the Chinese People’s Liberation Army has even carried out cyber espionage specifically against European and American space supply chains since at least 2007 in an effort to jump ahead of competition.<sup>18</sup> Furthermore, penetration testers recently demonstrated the



*Many terrestrial networks rely on interconnected system of satellites with automated connections to efficiently transmit data, products, and services.*

impacts of supply chain injection when they installed malware to carry out a cyber-attack on a live, European Space Agency OPTSAT in orbit. The testers showcased several critical stages of an attack, including privilege escalation, persistent access, and lateral movement from the satellite's bus to the remote sensing payload. They manipulated the images taken by the nanosatellite's camera before being down-linked back to Earth. Although not demonstrated, they claim to have also been able to drain the satellite's batteries, tamper with its GPS coordinates, and shut down services.<sup>19</sup> In an operational environment, what would happen if an adversary replayed outdated imagery to mask ground activity?

Finally, even if cybersecurity is designed into systems before launch, the job is not over. Starlink has 'resisted all hacking and jamming attempts' partly because of its bounty program, which pays anybody who can find and report vulnerabilities, enabling swift patching.<sup>20</sup> This proactive mentality is similarly seen at the US Space Force's annual Hack-a-Sat, and a recent effort

to create a virtualized test range to assess an Estonian CubeSat's cybersecurity posture.<sup>21</sup>

## Conclusion

Although it may appear daunting, it is important to note that all these new space capabilities can be secure if the space community does not procrastinate or neglect the proper cybersecurity steps. Securing the four segments does not necessarily require novel cybersecurity techniques, but rather by enforcing high standards already in place for our most sensitive military networks. Pending established cybersecurity standards for space, mission owners can apply existing standards used by lightweight cryptography, IoT, and national security networks. As new space rapidly employs shared software, COTS products, small satellites, GSaaS, and other future developments, space mission owners need to prioritize cybersecurity with greater urgency throughout all the space segments. Failure to do so could compromise NATO operations.

Implementing proactive measures such as continuous vulnerability assessments, penetration testing, zero trust, and fostering collaboration between government and private sectors will greatly reduce risk so that new space innovations remain resilient against evolving cyber threats. ●

1. 'Miniature Satellites with Massive Benefits', NASA Space Station Integration Office, July 2022. <https://www.nasa.gov/missions/station/miniature-satellites-with-massive-benefits/> (accessed 17 June 2024).
2. Swan, McKayla, 'Anti-satellite Tests: A Risk to the Security and Sustainability of Outer Space', Liberty University Journal of Statesmanship & Public Policy Vol. 3 Iss. 1, Article 4 p. 6 (2022). <https://digitalcommons.liberty.edu/jspp/vol3/iss1/4> (accessed 17 June 2024).
3. Erwin, Sandra, 'DoD space agency: Cyber attacks, not missiles, are the most worrisome threat to satellites', Space News, April 2021. <https://spacenews.com/dod-space-agency-cyber-attacks-not-missiles-are-the-most-worrisome-threat-to-satellites/> (accessed 17 June 2024).
4. Kaczmarek, Sylvester, 'Cybersecurity for Space Assets: Focusing on SmallSats and CubeSats', Sylvester Kaczmarek. <https://sylvesterkaczmarek.com/blog/cybersecurity-for-space-assets-focusing-on-smallsats-and-cubesats> (accessed 17 June 2024).
5. 'Industrial Control Systems Vulnerabilities Soar: Over One-Third Unpatched in 2023', The Hacker News, August 2023. <https://thehackernews.com/2023/08/industrial-control-systems.html> (accessed 17 June 2024).
6. Siddiqui, Zeba and Bing, Christopher, 'Chinese hackers spying on US critical infrastructure, Western intelligence says', Reuters, May 2023. <https://www.reuters.com/technology/microsoft-says-china-backed-hacker-targeted-critical-us-infrastructure-2023-05-24/> (accessed 17 June 2024).
7. Torkington, Simon, 'These 6 countries are using space technology to build their digital capabilities. Here's how', World Economic Forum, April 2024. <https://www.reuters.com/technology/microsoft-says-china-backed-hacker-targeted-critical-us-infrastructure-2023-05-24/> (accessed 17 June 2024).
8. 'NATO Space Handbook', 2021.

9. Page, Carly, 'ViaSat Cyberattack Blamed on Russian Wiper Malware', Tech Crunch, March 2022. <https://techcrunch.com/2022/03/31/viasat-cyberattack-russian-wiper/?guccounter=1> (accessed 17 June 2024).
10. Evan Meyrick, Aaron Pickard, Tobias Rahloff et al, 'Ground Station as a Service: A Space Cybersecurity Analysis', 72<sup>nd</sup> International Astronautical Congress, October 2021. <https://www.researchgate.net/publication/356378842> (accessed 17 June 2024).
11. Panetta, Kasey, 'Is the Cloud Secure?', Gartner, October 2019. <https://www.gartner.com/smarterwithgartner/is-the-cloud-secure> (accessed 17 June 2024).
12. '2023 Global Threat Report', CrowdStrike, 2023. <https://www.crowdstrike.com/resources/reports/global-threat-report-executive-summary-2023/> (accessed 20 August 2023).
13. B. Lin, W. Henry, R. Dill, 'Defending Small Satellites from Malicious Cybersecurity Threats', 17<sup>th</sup> International Conference on Cyber Warfare and Security, March 2022. <https://papers.academic-conferences.org/index.php/icwss/article/view/60> (accessed 18 June 2024).
14. S. D. Hitefield, M. Fowler, T. Charles Clancy, 'Exploiting Buffer Overflow Vulnerabilities in Software Defined Radios', IEEE, 2018. <https://ieeexplore.ieee.org/abstract/document/8726592/> (accessed 18 June 2024).
15. M. Manulis, 'Security challenges for satellite constellations and communications', [online video], 2021, <https://www.youtube.com/watch?v=caz8-LeBs9Q&t=629s> (accessed 18 June 2024).
16. F. Schiffer and T. Rostek, 'Improved security for the IoT: NIST selects Ascon as international standard for lightweight cryptography', Infineon, February 2023. <https://www.infineon.com/cms/en/about-infineon/press/market-news/2023/INFSS202302-064.html> (accessed 18 June 2024).
17. D. Werner, 'Small Satellites, Big Weakness', Aerospace America, September 2019. <https://aerospaceamerica.aiaa.org/features/small-satellites-big-weakness/> (accessed 18 June 2024).
18. '2022 Challenges to Security in Space', Defense Intelligence Agency, March 2022. [https://www.dia.mil/Portals/110/Documents/News/Military\\_Power\\_Publications/Challenges\\_Security\\_Space\\_2022.pdf](https://www.dia.mil/Portals/110/Documents/News/Military_Power_Publications/Challenges_Security_Space_2022.pdf) (accessed 18 June 2024).
19. B. Bailey and B. Roeher, 'Hacking an On-Orbit Satellite: An Analysis of the CYSAT 2023 Demo', Medium, May 2023. <https://medium.com/the-aerospace-corporation/hacking-an-on-orbit-satellite-an-analysis-of-the-cysat-2023-demo-ae241e5b8ee5> (accessed 18 June 2024).
20. M. Kan, 'SpaceX Invites Security Researchers to Hack Starlink', PCMag, August 2022. <https://www.pcmag.com/news/spacex-invites-security-researchers-to-hack-starlink> (accessed 18 June 2024).
21. 'University of Tartu and CybExer Technologies plan to connect ESTCube-2 satellite into a unique cyber security system', Cybexer Technologies, March 2022. <https://cybexer.com/news/estcube-2-satellite-into-a-unique-cyber-security-system/> (accessed 18 June 2024).

---

#### ABOUT THE AUTHOR

---

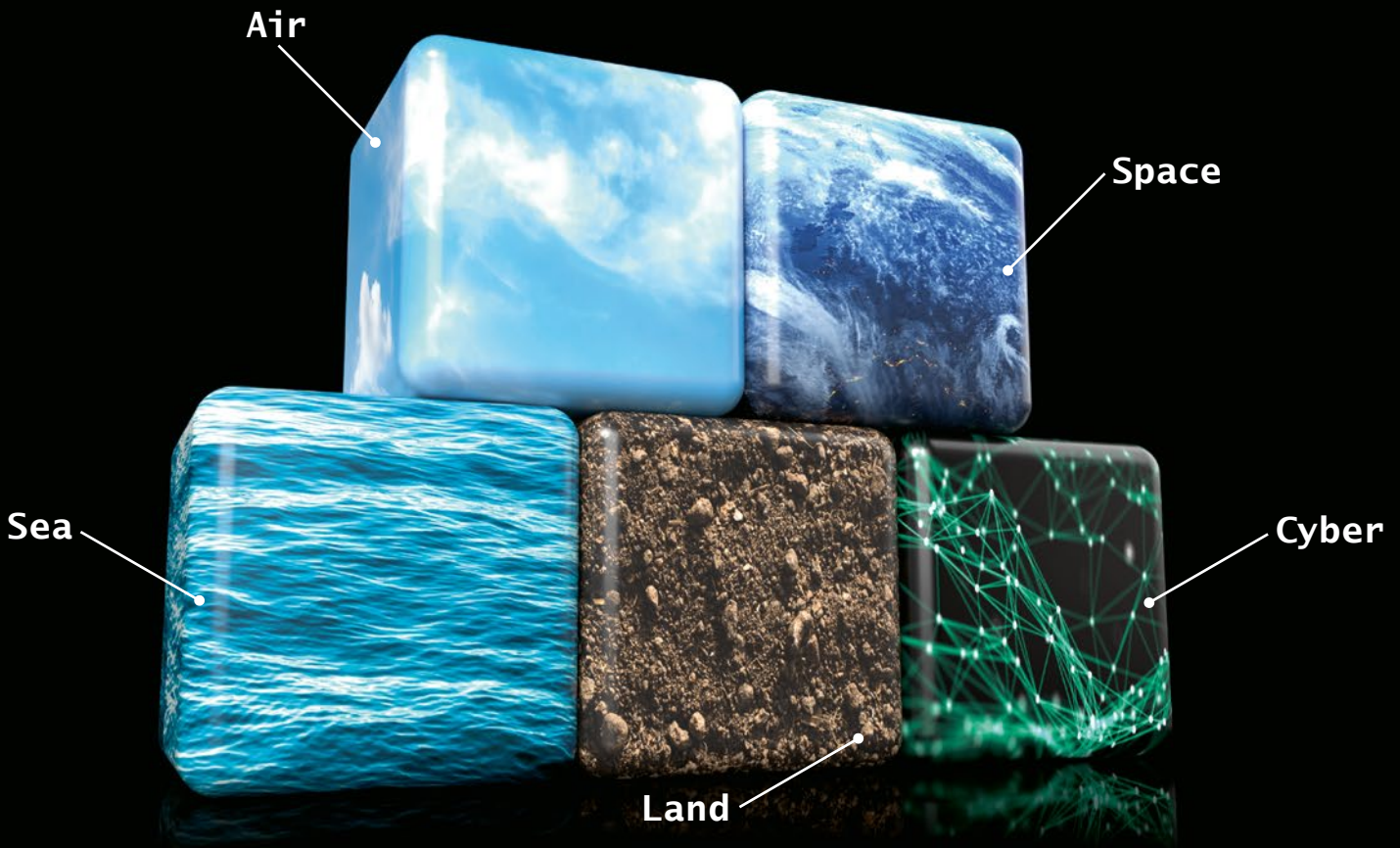


**Captain Luke Stensberg**

US Space Force, JAPCC

Captain Stensberg is a subject matter expert in space and cyber integration, leading the way in the JAPCC's C5ISR & Space branch to enhance the Alliance's comprehension of these critical domains. Before this role, he served in a Space Force talent management function, and prior to that, as a Cyberspace Operations Planner at the 16<sup>th</sup> Air Force's Headquarters. There, he aligned strategies with US Cyber Command and, notably, the newly stood-up US

Space Command. Other previous assignments include Flight Commander of Tactical Communications for the 485<sup>th</sup> Intelligence Squadron, managing C4ISR capabilities for 29 nations and over 900 intelligence analysts. He also provided Integrated Project Management support to the 694<sup>th</sup> ISR Group in Osan, Republic of Korea. Captain Stensberg was commissioned as a Cyberspace Operations Officer in 2016 from the United States Air Force Academy.



3D Objects: © Adobe; Sea: © Tomasz Zajda – stock.adobe.com; Land: © 994yellow – stock.adobe.com; Cyber: © Dmitry – stock.adobe.com; Air: © lovelyday12 – stock.adobe.com; Space: © Shutter2U – stock.adobe.com;

# Enhancing NATO's Strategic Edge

## *A Human-Centric Approach to Multi-Domain Operations*

By Colonel Tyler Niebuhr, US Air Force, JAPCC

### **The Need for Action**

The war in Ukraine and conflict in Israel present a potential catalyst for wider regional hostilities. Technology has given terrorist organizations increased capabilities, and the pervasive use of information warfare allows for widespread emotional manipulation with geopolitical consequences. In today's interconnected and emotionally charged society, terrorism continues to pose a grave threat to NATO members' security. The current state of global affairs, which includes Russia's aggression towards Ukraine, its developing relationship with China, and the ongoing turbulence in the Middle East, presents complex

security challenges for NATO. We must recognize that deterrence and defence are not mere slogans but a shared responsibility that requires our constant adaptation to emerging forms of warfare in today's multi-domain operating environment. The wide range of security concerns amidst the ever-evolving character of conflict in the 21<sup>st</sup> century calls for our diligent attention and strategic thinking.

Thankfully, NATO has taken steps towards addressing these pressing threats by bolstering its political unity, expanding its membership, and developing a comprehensive military strategy to organize and coordinate warfare development.<sup>1</sup>

As the Alliance moves forward, it must prioritize the importance of actual human performance in Multi-Domain Operations (MDO); otherwise, it will miss the mark in its quest towards transformation and potentially fall prey to the false hope that technology will solve all our problems. Although technological advancements are absolutely necessary to maintain the advantage over revanchist challengers, technology is irrelevant without the right people, processes, and training. In today's fast-paced, technologically advanced world, personnel face the challenge of using sophisticated technology to synchronize various effects across multiple domains to outmanoeuvre adversaries in pursuit of calculated objectives.

As technology continues to advance at an exponential rate, it becomes increasingly crucial to remember the human factor. Every technological advancement and increased capability should be designed to enhance the performance of the human actor. By adopting a mindset that prioritizes enhancing and optimizing human performance, the Alliance can establish a focused approach towards policy alignment, multi-domain doctrine creation, and synchronized Tactics, Techniques and Procedures (TTPs). A performance-focused mindset can serve as the foundation for technological and weapon system developments, increasing combined capabilities, and ensuring superior execution. A force with a strong emphasis on performance enhances deterrence through its credibility – by maintaining a highly competent defensive force. Prioritizing performance offers significant strategic advantages and upholds the collective security interests of member nations. Each individual's contribution is crucial in preserving the integrity and unity of the Alliance through a performance-oriented strategy.

## Strategic Guidance

NATO leadership recognizes the need to optimize the full potential of integrated mission execution to harmonize its instruments of power. In February 2021, the NATO Defence Ministers endorsed the NATO Warfighting Capstone Concept (NWCC), a 'North Star' for warfare development through 2040. It identified that the

Alliance's future warfighting strategies must consider a multi-region, multi-dimensional, and multi-domain operating environment. The NWCC identified five Warfare Development Imperatives (WDIs) and six critical enablers as a means for the Alliance to organize and synchronize national development efforts. Subsequently, the NATO Military Committee (MC) tasked Allied Command Transformation (ACT) to further operationalize the concepts in the NWCC and, with Allied Command Operations (ACO), develop the Alliance's initial concept for MDO.

In April 2022, ACT delivered the Warfare Development Agenda (WDA), a 20-year plan through which ACT manages the planning and implementation of the NWCC and links it closely with the NATO Defence Planning Process (NDPP). The following year, the MC approved an official NATO definition for MDO and released the Alliance's Concept for MDO.

Developing guiding concepts demands monumental thought power, yet their value remains unrealized without implementation. Pathways to progress require action. J. D. Rockefeller, the world's first self-made billionaire, emphasized, 'I know that there is no result without action, and there is nothing in the world that is obtained just from thinking. As long as people are alive, they must consider taking action.'<sup>2</sup> This philosophy of action seamlessly aligns with key military principles such as *initiative*, *offensive spirit*, and *freedom of action*.<sup>3</sup>

ACT actively pursues a path towards an MDO-enabled Alliance. They are focused on codifying MDO concepts and updating Allied Joint Publications. Together with ACO, ACT is conducting training events and exercises, such as Steadfast Jupiter and Steadfast Duel, focused on data fusion and the targeting process, and Steadfast Defender series to exercise multi-domain capabilities. ACT seeks to identify capability requirements and build processes to provide a more accurate assessment of the environment and assist political-military decision-making. To further develop plans of action, ACT developed Lines of Delivery (LODs) with associated working groups and team leads to establish a process towards achieving the Warfare Development Imperatives.



*Military technology is a critical enabler and will continue to evolve, but war and peace are ultimately human endeavours. The JAPCC vision for MDO seeks to optimize the human role, supported by technology, structure, and practice.*

In response to the call for action, the Joint Air Power Competence Centre (JAPCC) has taken on the crucial task of spearheading MDO development as its umbrella project. With a team of subject matter experts, JAPCC is committed to leveraging its expertise and thought power to support ACT and ACO in developing an MDO-capable force. Multi-domain operations place unprecedented demands on our forces to sense, make sense, and act at a rate that will defeat those who would challenge NATO. Optimizing human performance should be the central theme to maximize combined performance throughout the Alliance in a multi-domain fashion.

## Human Performance

Within the context of this article, human performance is defined as an individual's tangible and quantifiable output, as well as accomplishments in completing tasks or reaching goals. It is different from human capital, which encompasses an individual's combined knowledge, skills, abilities, and potential that can contribute to their productivity.<sup>4</sup> Human capital focuses on the potential and growth of individuals, including

their education, training, expertise, and experience. In contrast, human performance focuses on the concrete outcomes and achievements that individuals produce in their work or activities. It is a measure of actual results rather than potential capabilities.

Investing in human capital sets a foundation of training with the hope of future success, but it must be done thoughtfully with both the desired system and the individual in mind. Human-Centred Design (HCD) puts people at the forefront of systems, policies, procedures, and technology, recognizing their unique needs and abilities.<sup>5</sup> Implementing an HCD approach to NATO development would ensure that the capabilities of MDO are custom-built to align perfectly with people's natural abilities, resulting in enhanced performance. Emphasizing usability and effectiveness, HCD would intend to reduce the cognitive load on individuals and improve decision-making processes, ensuring optimal human performance even in complex environments. Integrating HCD principles into MDO development would target and maximize human factors to elevate the overall performance of forces within the Alliance. It is akin to a finely crafted instrument designed specifically for the musician who will play it with ease and precision.



*The NATO Airborne Early Warning & Control Force is one example of a multinational unit at the tactical level that trains and operates together to protect NATO nations' airspace.*

The shift towards a human-centric mindset complements top-down strategies in developing an MDO-enabled Alliance. By taking a bottom-up approach, the JAPCC identifies opportunities to prioritize efforts in education and training, the use of technology, and evaluating mission-focused scenarios to identify gaps across the Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities, and Interoperability (DOTMLPFI) framework. This synergistic approach combines performance requirements with strategic guidance to propel us towards action.

## Education and Training

For NATO to effectively implement its MDO concept, education and training must be improved at all levels within the Alliance. This means addressing member nations' varying capabilities and readiness, and developing a cohesive strategy for sharing information, promoting continuous learning, and bridging knowledge gaps.

While the Alliance's MDO concept is well-known at the strategic level, its application and understanding

diminish at the operational and tactical levels. This disparity hinders the successful implementation of MDO strategies, highlighting the importance of a comprehensive approach to education and training. Bridging this gap between echelons cultivates a force that operates seamlessly across multiple domains and enables a holistic approach to military operations.

To achieve this goal, ACT must take on an active role in disseminating knowledge about MDO through targeted information campaigns. NATO Centres of Excellence (COEs) can support ACT's efforts in this area. As one of NATO's COEs, the JAPCC actively plays a role in increasing the Alliance's understanding of MDO and has provided educational briefings at key events such as Ramstein Ambition, command and control seminars, NATO's Tactical Leadership Programme (TLP), and national air conferences. These efforts promote a comprehensive understanding of MDO principles at various levels within the NATO structure.

Although each nation is responsible for providing well-trained forces for NATO's needs, there are disparities amongst member nations in terms of capabilities and development. A collaborative training approach



*Live exercises are a platform for validating proposed solutions and identifying unforeseen challenges.*

addresses these discrepancies to ensure a unified development of MDO within the Alliance. As an example, national air warfare centres, NATO COEs, and ACT can all play a role in creating and implementing a cohesive development program for Joint Air and Space Power. National air warfare centres offer expertise and current knowledge of national developmental levels, which can contribute to tailored training programs. NATO COEs bring subject-matter knowledge, and their organizations have internal structures to support NATO education and training. ACT can coordinate these efforts as a driver of NATO transformation to ensure a unified development plan that aligns with Alliance standards. An example of incorporating this opportunity should be regularly scheduled working seminars to align and coordinate Alliance efforts towards high-priority requirements. This collaboration should target force developmental differences and improve overall human performance for MDO readiness.

A centralized knowledge hub specifically dedicated to MDO is needed to support this collaborative endeavour. Creating an online hub for MDO would serve as a central resource for publishing guidance and facilitating communication about new or emerging concepts, ideas, and thoughts related to MDO. This

hub should be accessible for all NATO personnel, promoting continuous learning and adaptation to the ever-evolving nature of multi-domain warfare.

By implementing regular collaborative training and education measures, NATO can take additional steps towards cultivating a knowledgeable and skilled force capable of meeting the challenges of modern warfare while considering the varying levels of development within the Alliance.

### **Technology: Human-Centred Design**

At its core, HCD is a reminder of our responsibility to foster a complimentary relationship of humans supported by technology. It goes beyond simply creating advanced systems; it requires us to consider how these systems will interact with our inherent abilities and limitations as human beings. By prioritizing the individuals' needs and experiences, we can ensure that technology serves as a tool for enhancing our lives, rather than controlling them.

As NATO continues to prioritize the digital transformation of its forces, it must consider a human-centric approach. While advanced technology can certainly



enhance capabilities, a highly skilled and adaptable force is essential for effectively utilize it. Relying solely on technology may lead to underutilization or misapplication in complex operational environments. Moreover, adversaries are constantly adapting and developing countermeasures, making it imperative that personnel can quickly adjust tactics and strategies. Therefore, investing in HCD must remain a top priority to ensure the success of NATO's digital transformation and overall mission.

Technology should act as an enabler, specifically designed to support the user rather than dictating operational procedures. It is not uncommon to find disparity between how engineers design systems and how users need to operate them. The mismatch between engineer-centric design and user-centric operation often results in a usability gap, leading to decreased productivity and increased errors. Delays in real-time execution due to such usability gaps could result in unacceptable risk-to-mission and risk-to-forces. An HCD ap-

proach would incorporate user feedback and iteratively refine the interface to align closely with the end users' mental models and operational needs.

NATO's current focus on the Alliance's digital transformation is a top-down approach that aligns technology with MDO objectives. However, a complementary bottom-up approach is essential to ensure that technology is inherently user-centric. HCD principles must guide the development of technological solutions to maximize user performance. This dual strategy recognizes the need for integration by design across all nations within the Alliance, fostering a cohesive technological ecosystem.

## Human Performance Through Experiential Scenarios

Activities such as mission-focused scenarios, wargames, and exercises provide a bottom-up approach that complements top-down MDO strategies. This method allows for a thorough analysis of the combined performance of forces and identifies any deficiencies across





*To truly achieve a multi-domain solution, it is imperative to include the right representatives from all services and entities with a shared mindset focused on domains and effects rather than service or component.*

DOTMLPFI. By utilizing models like AIRCOM's inaugural Weapons and Tactics Conference (WEPTAC), a structured framework can be applied to address and resolve these gaps systematically.

WEPTAC, as an illustrative model, involved tactical operators developing plans for specific tactical challenges and subsequently identifying necessary changes in policies, procedures, and procurements to maximize combined performance and achieve objectives while minimizing risks. This process helps prioritize efforts to resolve gaps within the DOTMLPFI framework, resulting in a more efficient approach to improving performance. The mission-focused scenarios served as a conceptual testing ground, revealing areas for improvement within operations.

Following the thorough planning phase held at WEPTAC, AIRCOM's next crucial step is to execute the plan, or portions of the plan through comprehensive live exercises. An action phase provides valuable opportunities for operators to test and refine their operational approach in a controlled environment. Live exercises act as a platform for validating proposed solutions and identifying unforeseen challenges that may arise in the real-world applications of the plan. The insights gained during this performance phase are integral in shaping the feedback loop for continuous improvement. These lessons learned are then integrated into subsequent WEPTAC sessions, contributing to

refining tactics, strategies, and DOTMLPFI elements. Through this iterative process, the force's approach to mission-focused scenarios evolves and adapts, remaining agile in the face of emerging challenges and advancements in technology and tactics.

The first and most vital recommendation from WEPTAC is to address the air-focused planning for a missionized scenario involving multiple NATO components. To truly achieve a multi-domain solution, it is imperative to include the right representatives from all services and entities involved in providing effects. Such a collaborative effort harnesses the collective expertise of diverse entities, resulting in a more multi-domain, comprehensive, and effective planning process.

Furthermore, to enhance the exercise phase, it is highly recommended to incorporate a virtual component. Not all effects and tactics may be available in live exercises, making the virtual realm an invaluable tool to test a wider range of capabilities. This also adds an element of secrecy, safeguarding sensitive tactics and developments from outside observation.

However, including a virtual component highlights a critical discrepancy within NATO: the lack of integrated virtual training amongst its members and services. To rectify this issue, urgent investment must be made to acquire standardized and integrated virtual training platforms. A cohesive and interoperable approach to

virtual training exercises specifically supports optimizing human performance and ensuring readiness and effectiveness across all levels of the alliance.

Ultimately, incorporating mission-focused scenarios, exemplified by models like WEPTAC, offers a robust methodology for identifying and addressing DOTMLPFI gaps in an MDO-enabled force. This bottom-up approach complements overarching MDO strategies, providing a dynamic and adaptive framework for enhancing the combined performance of NATO forces in the complex and evolving multi-domain battlespace.

## Conclusion

The challenges faced by NATO in our current era are multifaceted and intricate. To address these challenges with resolute action, a comprehensive approach that places human performance at its core is crucial. As MDO becomes increasingly important, shifting towards a human-centric mindset is imperative for optimizing Alliance capabilities.

Furthermore, the success of NATO's endeavours hinges on integrating both top-down strategies and bottom-up approaches. This necessitates a synergistic fusion of education and training, incorporating human-centred design principles in technological advancements, and performance improvement through mission-oriented scenarios. By highlighting the significance of human performance in these critical areas, NATO can fortify its readiness and effectiveness, ensuring adaptive responses to the evolving complexities of modern warfare. Ultimately, the human element remains central in shaping the alliance's response to the interconnected and ever-changing security landscape of the 21<sup>st</sup> century. ●

1. Bergmann, M., Toygür, I., & Svendsen, O. (2023). *A Continent Forged in Crisis, Assessing Europe One Year into the War*. Center For Strategic & International Studies.
2. Rockefeller, John Davison. 2023. *The 38 Letters from J. D. Rockefeller to his son*. OS.
3. NATO. 2019. NATO Standard AJP-3, Allied Joint Doctrine for the Conduct of Operations, Edition C Version 1. NATO Standardization Office (NSO), p. 1-10–1-11.
4. Dictionary.com. *Human Capital*. Accessed 7 July, 2024. <https://www.dictionary.com/browse/human%20capital>.
5. The International Civil Aviation Organization (ICAO). n.d. *Human-Centered Design*. Accessed 21 December, 2023. <https://www.icao.int/safety/OPS/OPS-Normal/Pages/HCD.aspx>.

---

### ABOUT THE AUTHOR

---

#### Colonel Tyler Niebuhr

US Air Force, JAPCC



Colonel Niebuhr entered the Air Force in 2001 as a distinguished graduate from the Air Force Reserve Officer Training Corps.

After his commission, he attended Euro-NATO Joint Jet Pilot Training and completed the F-16 Basic Operational Training Course as a distinguished graduate in 2004. Colonel Niebuhr has worked in various flying assignments at the squadron, group, and wing level, including operational experience in NOBLE EAGLE, ODESSEY DAWN,

ENDURING FREEDOM, RESOLUTE SUPPORT and FREEDOM'S SENTINEL, which included two deployments to Afghanistan. He has over 3,300 flight hours and 190 combat sorties in the F-16.

Colonel Niebuhr's educational background includes a Bachelor of Science in Applied Physics, a dual Masters of Human Relations and International Relations from the University of Oklahoma, and a Master of Strategic Studies from Air War College, Maxwell AFB.



# Quantum Technologies for Air and Space (Part 3 of 3)

## *Quantum for ISR and PNT: Use Cases and Timelines*

By Dr Michal Krelina, Czech Technical University in Prague

By Lieutenant Colonel Denis Dubravcik, CZ Air Force, JAPCC

### **Introduction**

This is the third and final piece in a series on air, space, and cyber applications of Quantum Technology (QT).

The objective of the series is to disentangle the science of QT to inform strategic leaders and defence planners of realistic expectations for QT.

In the previous part, we explored quantum transducers and clocks, and introduced the promising benefits of quantum-enhanced radars. In this paper we will elaborate on quantum imaging systems for Intelligence, Surveillance, and Reconnaissance (ISR), introduce QT-enabled sensors such as gravimeters and magnetometers, and explain their benefits for Positioning, Navigation, and Timing (PNT) applications.



Since the publication of the inaugural article in the series in February 2023, which established the theoretical basis for our subsequent comprehensive discussions of their applications, QT has gained greater recognition in NATO circles. As Technology Readiness Levels (TRL) rise and advancements in quantum-powered devices progress, NATO introduced its Quantum Technology Strategy in January 2024.<sup>1</sup> This vision considers the potential of QT to offer disruptive capabilities that, if exploited by our adversaries, could reduce the Alliance's ability to deter and defend. In concert with other Emerging and Disruptive Technologies (EDT) such as autonomy, Artificial Intelligence (AI), and big data, QT may also constitute strategic advantage for the Alliance.

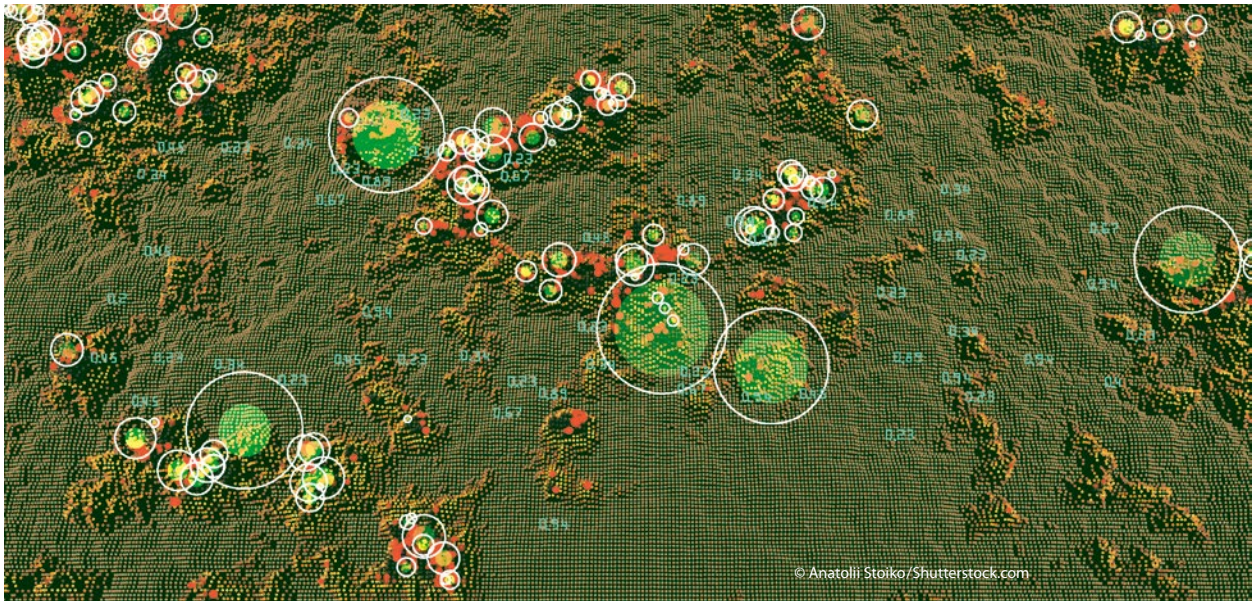
The complexity of quantum technologies is not merely reflected in the recently introduced strategy. NATO's key enabler of capability identification, the NATO Defence Planning Process (NDPP), is at the initial stage informed by Strategic Foresight Analysis (SFA). This

strategic document establishes the prognosis for the future Alliance operating and security environment and identifies that the convergence of EDTs, particularly QT and AI, will not only transform world society but will change the character of the future warfare.

## Intelligence, Surveillance, and Reconnaissance

### Quantum Imaging Systems

**Introduction:** Quantum imaging leverages the unique properties of quantum mechanics to transcend the capabilities of traditional imaging technologies. Its remarkable applications include seeing through obstacles, enhanced imaging in adverse weather conditions, and capturing images from around corners or in three dimensions. Central to quantum imaging is the use of single or entangled photons. When photons are entangled, the state of one is intrinsically linked to



*A visual depiction of Earth's gravitational field reveals an intricate and nuanced map, rather than a uniform field. Precise measurements by quantum gravimetry could enable accurate navigation without external support, such as GPS, and an entirely new method of intelligence gathering and target development.*

the other, regardless of distance. Manipulating one photon reveals information about its partner, allowing us to capture information beyond the reach of conventional photons. This advanced imaging process involves intricate quantum optics and relies on highly sensitive detection equipment.

**Advantage:** The foremost advantage of quantum imaging, which commonly uses entangled photon pairs, is its superior resolution and sensitivity compared to classical methods. Excelling in low-light environments, it can penetrate mediums like fog, smoke, or certain solids, which would usually hinder traditional optical imaging. Quantum systems are adept at detecting single photons and precisely measuring their attributes, enabling detailed imaging in challenging conditions where standard cameras are ineffective.

Quantum ghost imaging is a technique that uses pairs of entangled photons to create images. One photon interacts with the object and is detected by a simple sensor, while its entangled partner is captured by a camera. The image is formed by linking the detections, even though the camera never directly sees the object. This method is more resistant to environmental interference

and can produce clear images in difficult conditions, using various types of light for greater flexibility.

Another application, Quantum Light Detection and Ranging (LIDAR), offers unmatched capabilities compared to traditional LIDAR. Commercially available quantum LIDAR systems, like quantum gas LIDAR with a range of approximately 200 meters, exemplify this advancement.<sup>2</sup> Other breakthroughs are three-dimensional quantum cameras with hundreds of meters of range, or non-line-of-sight imaging, capable of visualizing objects around corners over distances up to 1.43 km.<sup>3,4</sup>

**Applications:** In military contexts, quantum imaging presents a multitude of significant advantages. Its ability to see through obscurants such as smoke or foliage has obvious advantages for ISR and aviation operations. This capability ensures the delivery of clear imagery in situations where conventional systems might be ineffective. For instance, quantum imaging could prove invaluable for helicopter pilots landing in environments obscured by dust, fog, or smoke, and for long-range surveillance and target identification under challenging weather conditions.<sup>5</sup>

In the space domain, quantum LIDAR is particularly useful for observing space debris and other space assets such as satellites, enhancing situational awareness and safety in space operations.<sup>6,7</sup>

An additional intriguing defence application is to use non-linear optical materials to convert longer infrared light into near-visible light.<sup>8</sup> This conversion allows detection with conventional, cost-effective, high-performance silicon-based cameras, which is particularly relevant for applications like night vision.

**Time Expectations:** Quantum imaging is among the more mature quantum technologies, with a few commercial products already available, such as quantum LIDAR for gas leak detection. The development of military-grade quantum imaging systems is progressing, focusing on enhancing robustness and real-world applicability. Overcoming challenges in miniaturization and improving photon production rate and detection efficiency will be key to integrating these advanced systems into military operations in more than five years.

## Quantum Magnetometry

**Introduction:** Quantum magnetometry utilizes quantum principles and systems to measure magnetic fields with exceptional precision, surpassing classical magnetometers. Central to quantum magnetometry are the quantum properties of particles, such as spin states, which are highly sensitive to magnetic fields. This technology finds applications in various fields, from medical imaging like MRI, to geophysical exploration, and archaeological surveys.

For magnetic sensing, various approaches can be used, such as Superconducting Quantum Interference Devices (SQUIDs), Nitrogen Vacancy (NV) centres in diamonds, and Optically Pumped Magnetometers (OPMs). These technologies exploit quantum interference in superconducting loops, the sensitivity of electron spins, or changes in light polarization to detect magnetic fields.

**Advantage:** Quantum magnetometers outperform classical magnetometers in sensitivity, accuracy, spatial resolution, and range. SQUIDs can measure fields

as low as a few femtoteslas. NV centres, operating at room temperature, provide high spatial resolution and can detect fields in the nanotesla range. OPMs balance sensitivity and practicality, often reaching femtotesla sensitivities. In comparison, classical magnetometers like fluxgate magnetometers typically have sensitivities in the range of 1 to 10 picoteslas and spatial resolutions from millimetres to centimetres. NV centres and OPMs can achieve nanoscale spatial resolution and do not require cryogenic cooling, making them ideal for compact applications, such as advanced brain function measurements in magnetoencephalography (MEG).<sup>9</sup>

**Applications:** In military applications, quantum magnetometers' sensitivity and precision are invaluable. Quantum magnetometers can help with extending of situational awareness, enabling visualizing, tracking, and classifying of objects that are underground.<sup>10</sup> They can detect submarines' subtle magnetic signatures from airborne platforms at distances of several kilometers, significantly farther than classical magnetometers.<sup>11</sup> This capability extends to detecting camouflaged weapons and military systems or standoff weapon detection<sup>12</sup> and to mine detection.<sup>13</sup>

Other significant applications include non-destructive corrosion detection in aircraft and microelectronic assurance in evaluating the integrity of integrated circuits, for example, sensing hardware trojans in microchips that are critical for military systems across all domains.<sup>14</sup> Quantum magnetometers are also expected to be used for space surveillance and weather measurement.

**Time Expectations:** The field of quantum magnetometry is rapidly evolving. While SQUIDs offer unmatched sensitivity, their requirement for cryogenic temperatures and the need for reduced Size, Weight, and Power (SWaP) limit some applications. NV centres and OPMs, being more adaptable for field deployment, are closer to broader deployment. For example, a portable NV-based magnetometer has already been demonstrated.<sup>15</sup> In the coming years, we can expect to see more advanced and miniaturized versions of these technologies being integrated into military systems, enhancing capabilities in surveillance, navigation, and reconnaissance.

## Quantum Gravimetry

**Introduction:** Quantum gravimetry uses quantum principles to achieve highly precise measurements of gravitational fields. The key technology here is cold-atom interferometry, where ultra-cold atoms are used as highly accurate sensors. In a typical quantum gravimeter, a cloud of these atoms is released, and their fall is measured with laser pulses. The wave-like nature of the atoms creates an interference pattern, allowing for extremely precise measurements of gravitational acceleration. Additionally, new technologies in this field, such as superconducting devices and sensors using entangled atoms, are expanding the possibilities of quantum gravimetry.

These advanced quantum instruments are not limited to a single application, their potential spans across geophysical exploration, navigation, and even the detection of subterranean structures or resources. In geophysics, for instance, they offer detailed insights into natural subsurface structures, assisting in the exploration of minerals or hydrocarbons.

**Advantage:** Quantum gravimeters have a distinct edge over classical gravimeters in terms of sensitivity and precision. For example, cold atom gravimeters have achieved sensitivities within tens of micro-gals, surpassing classical gravimeters which typically measure gravitational acceleration with an accuracy of hundreds of micro-gals. This heightened sensitivity allows quantum gravimeters to detect minute changes in gravitational fields, which classical instruments might miss. Furthermore, quantum gravimeters are less susceptible to environmental noise, enabling absolute measurements of gravitational acceleration and gradiometry. Quantum gradiometers can detect variations over smaller spatial scales, making them very useful for applications like detecting under-

ground cavities or monitoring geological changes. Additionally, quantum gravimeters are known for their long-term stability and low drift rate, reinforcing their reliability.

**Applications:** The exceptional sensitivity and accuracy of quantum gravimetry and gradiometry have significant implications for military applications. They can be instrumental in detailed subterranean mapping, aiding military operations in uncovering underground bunkers, tunnels, or concealed facilities, particularly in regions where direct surveillance is impractical. In naval contexts, quantum gravimeters enhance the detection of submerged entities like submarines, with their sensitivity aiding identification of large underwater metallic objects. Beyond these, quantum gravimetry can bolster geophysical ISR efforts. They can detect minute changes in the gravitational field, potentially revealing the presence of heavy military equipment or landscape modifications due to enemy activities. Absolute quantum gravimetry has already been tested from airborne platforms.<sup>16</sup>

**Time Expectations:** Quantum gravimetry is a rapidly evolving field. Currently, cold atom gravimeters are predominantly experimental and in the prototype phase, with a recent significant advancement being the successful demonstration of trapped neutral atoms in a compact device placed on a drone, paving the way for future integration of gravimetry sensing capabilities.<sup>17</sup> Within the next 3 to 8 years, we can anticipate the emergence of practical, deployable quantum gravimeters for scientific and industrial purposes. Their incorporation into military technology to enhance mapping, navigation, and surveillance capabilities is likely to soon follow. The speed at which these technologies are adopted into military applications hinges on ongoing advancements in miniaturization, robustness, and operational versatility in various environments.



## Positioning, Navigation and Timing (PNT)

### Gravity and Magnetic-Aided Navigation

**Introduction and Applications:** Quantum sensors are revolutionizing gravity and magnetic-aided navigation (map-matching), offering robust alternatives to GPS, especially in environments where GPS signals are unavailable. Magnetic-anomaly aided navigation, for instance, leverages detailed maps of Earth's magnetic field, which exhibits geographically unique and immutable patterns, for precise location estimation, crucial in areas like underwater navigation. Similarly, gravity-aided navigation employs quantum technology to accurately measure Earth's gravitational field, providing precise geolocation information. These quantum technologies, as detailed in the ISR section, have potential in areas where conventional navigation systems fall short.

**Time Expectation:** The deployment of gravity and magnetic-aided navigation systems is contingent on the availability of comprehensive gravity and magnetic field maps of Earth, because these navigation systems will be most impactful when sufficiently detailed anomaly maps are available. A recent breakthrough involves SandboxAQ's AQNav, a near-commercial quantum magnetometry-aided navigation solution that the USAF successfully tested on various aircraft to demonstrate its potential for real-time, unjammable navigation.<sup>18</sup>

### Quantum Inertial Navigation

**Introduction:** Quantum inertial navigation, employing principles akin to those in quantum gravimetry, represents a significant advancement in navigation technology. This method uses quantum accelerometers and gyroscopes, harnessing the behavior of super-cooled atoms or ions. These systems precisely measure the quantum properties of particles, including their wave functions and responses to movement, allowing for accurate determination of position and orientation. In comparison, mechanical or optical inertial navigation systems drift over time, typically up to one nautical mile per hour. Quantum inertial navigation systems are expected to reduce this drift just a few meters per hour.

**Applications:** The potential applications of quantum inertial navigation, particularly in miniaturized forms suitable for airborne systems like aircraft or missiles, are vast. This technology is independent of external signals like GPS or sensors such as radar or infrared guiding, and is not vulnerable to electronic warfare countermeasures. Furthermore, it shows promise as a primary navigation system in future space exploration and presence.

**Time Expectations:** Quantum inertial navigation components are currently undergoing testing in relevant environments, including aboard ships and aircraft. An intermediate step might involve hybrid systems combining quantum and classical sensors, offering incremental yet significant advantages.<sup>19</sup> Overall, the timeline for fully operational quantum inertial navigation systems parallels that of quantum gravimetry, with similar developmental milestones and challenges anticipated.

## Discussion

The quantum technologies discussed, along with their applications and use cases, represent a selection of the most promising research and development for military use in the near-to-medium term. Notably, many of these technologies are undergoing testing in relevant environments. Concurrently, there have been significant strides in supporting technologies, such as laser and vacuum chamber miniaturization and advances in integrated photonics, which can contribute to reductions in SWaP, potentially lowering overall cost.

AI is another important supporting technology, as it plays a significant role in analyzing and interpreting data from quantum sensing systems. For example, the AQNav system utilizes AI to precisely compare local measurements with global magnetic field maps, enabling accurate location estimation. AI algorithms enhance the signal-to-noise ratio, filtering out environmental and mechanical noise, and ensuring precise and reliable data interpretation. This integration of AI with quantum sensing technologies not only improves accuracy but also accelerates the processing of complex data, making these systems more efficient and effective for various applications.

NATO has increasingly focused on supporting military-oriented quantum technology through various initiatives. For instance, quantum-related activities now make up a significant portion of Research Task Groups (RTGs), where specific scientific research and technology development challenges are addressed. Additionally, NATO's Defence Innovation Accelerator for the North Atlantic (DIANA) and the NATO Innovation Fund provide significant support to startups and SMEs. These programs aim to integrate innovative ideas into NATO's strategic framework, promoting the development of dual-use technologies that benefit both military and civilian sectors.

Furthermore, it is important to recognize that many leading defence contractors are actively involved in quantum technology research, with a particular emphasis on quantum sensing. Their development efforts are likely more advanced, especially regarding testing in relevant environments, compared to academic research. This involvement by major defence entities indicates a robust and growing interest in leveraging quantum technologies for enhanced military capabilities. NATO's DIANA accelerators play a crucial role here by also supporting small startups, ensuring that innovative solutions from smaller enterprises can be developed and integrated, thereby transforming defence capabilities in the coming years.

## Conclusions and Key Takeaways

The exploration of quantum technologies in this paper underscores their growing role and huge potential in the military domain, particularly in air and space operations. The advancements in quantum sensing and metrology, quantum communication, and quantum computing can offer a significant paradigm shift, offering capabilities far beyond the scope of current technologies. With quantum sensors already showing high levels of technological readiness, their application in diverse and challenging military environments appears close. These advancements are not just theoretical; practical demonstrations in real-world scenarios aboard ships, aircraft, and drones highlight the transition of these technologies from laboratory settings to operational fields.

---

**[...]** *'Quantum imaging...and its remarkable applications include seeing through obstacles, enhanced imaging in adverse weather conditions, and capturing images from around corners or in three dimensions.'*

---

The following paragraphs present the principal recommendations from the QT article series:

- Sound understanding of QT is crucial for the defence planners and senior leaders to establish informed requirement, resourcing, and programmatic decisions. Their expert perspective is pivotal in interaction with industry and science to clearly define the defence technology demands.
- In order to foster the Quantum-Ready Alliance Strategy, nations should seek to accelerate innovations and development in the QT field and focus on those that are most impactful in augmenting NATO capabilities. Furthermore, given the dual-use nature of QT, their strategic potential can only be fully utilized through a deeper collaboration between Allies and their technology and science organizations.
- Converging EDTs will likely have an unprecedented impact on society in the coming 20 years, but will also change the character of warfare and the quality of military capabilities. QT and AI together constitute a potential capability to support NATO's future warfighting concept, which will require an increased level of autonomy, automated decision-supporting tools, and high-fidelity sensors.

As QT technologies continue to evolve and mature, they are likely to redefine the landscape of defence technology, including the air and space domains, in the near future. NATO may leverage the potential of QT and transform it into a strategic advantage to ensure that it fulfils its core tasks of collective defence and deterrence. ●

1. 'Summary of NATO's Quantum Technologies Strategy', NATO, [https://www.nato.int/cps/en/natohq/official\\_texts\\_221777.htm](https://www.nato.int/cps/en/natohq/official_texts_221777.htm) (accessed 12 August 2024).
2. 'QLM – WHAT IS QUANTUM GAS LIDAR?', <https://www.qlmtec.com/technology>, (accessed 12 August 2024).
3. QuantIC, 'QuantIC – Sensing and Imaging for Defence and Security', accessed 12 December 2023, <https://www.quantiac.ac.uk/technologies/defenceandsecurity/#imagingwithundetectdphotons,single-fibreendoscope,non-lineofsightimaging,wavelengthtransformationcamera,underwaterimaging,realtime3dimaging> (accessed 12 August 2024).

4. Cheng Wu et al., 'Non-Line-of-Sight Imaging over 1.43 Km', *Proceedings of the National Academy of Sciences* 118, no. 10 (9 March 2021): e2024468118, <https://doi.org/10.1073/pnas.2024468118> (accessed 12 August 2024).
5. Philip Inglesant, Marina Jirotko, and Mark Hartswood, 'Responsible Innovation in Quantum Technologies Applied to Defence and National Security', 2018, <https://nqit.ox.ac.uk/sites/www.nqit.ox.ac.uk/files/2018-11/Responsible%20Innovation%20in%20Quantum%20Technologies%20Applied%20to%20Defence%20and%20National%20Security%20PDFNov18.pdf> (accessed 12 August 2024).
6. QuantIC, 'QuantIC – Sensing and Imaging for Defence and Security'.
7. Darin C Koblick and Steven Wilkinson, 'Space-Based Spooky Radar Orbit Determination Benefits at Earth-Moon Lagrange Points', 2020.
8. QuantIC, 'QuantIC – Sensing and Imaging for Defence and Security'.
9. Orang Alem et al., 'An Integrated Full-Head OPM-MEG System Based on 128 Zero-Field Sensors', *Frontiers in Neuroscience* 17 (14 June 2023), <https://doi.org/10.3389/fnins.2023.1190310>.
10. Anna Ahveninen, 'Quantum Diamond Magnetic Field Sensors for Improved Situational Awareness', *Research*, 8 June 2023, <https://research.unimelb.edu.au/strengths/updates/news/quantum-diamond-magnetic-field-sensors-for-improved-situational-awareness>.
11. Rajesh Uppal, 'Militaries Thrust on Quantum Sensors Including Quantum Magnetometers for Submarine Detection and Navigation in GPS Denied Environments', International Defense Security & Technology Inc., 12 June 2021, <https://dstch.com/geopolitics/militaries-employing-quantum-sensors-including-quantum-magnetometers-for-submarine-detection-and-navigation-in-gps-denied-environments/>.
12. Michal Krelina, 'Quantum Technology for Military Applications', *EPI Quantum Technology* 8, no. 1 (December 2021): 1–53, <https://doi.org/10.1140/epjqt/s40507-021-00113-y>.
13. Lee-Sun Yoo et al., 'Application of a Drone Magnetometer System to Military Mine Detection in the Demilitarized Zone', *Sensors* 21, no. 9 (January 2021): 3175, <https://doi.org/10.3390/s21093175>.
14. Denise Schiavone, 'Using Flaws to Find Flaws: Quantum Sensing for Microelectronics Security', 9 November 2023, <https://www.mitre.org/news-insights/impact-story/using-flaws-find-flaws-quantum-sensing-microelectronics-security>.
15. Ahveninen, 'Quantum Diamond Magnetic Field Sensors for Improved Situational Awareness'.
16. Y. Bidel et al., 'Airborne Absolute Gravimetry With a Quantum Sensor, Comparison With Classical Technologies', *Journal of Geophysical Research: Solid Earth* 128, no. 4 (2023): e2022JB025921, <https://doi.org/10.1029/2022JB025921>.
17. Matt Swayne, 'Aquark Technologies Demonstrates Airborne Cold Atom System on a Small Drone', *The Quantum Insider*, 25 October 2023, <https://thequantuminsider.com/2023/10/25/aquark-technologies-demonstrates-airborne-cold-atom-system-on-a-small-drone/>.
18. SandboxAQ, 'AQNav', 16 July 2024, <https://www.sandboxaq.com/solutions/aqnav>.
19. Caroline Rees, 'First Hybrid & Multidimensional Quantum Inertial Sensor Developed', *Unmanned Systems Technology* (blog), 22 November 2022, <https://www.unmannedsystemstechnology.com/2022/11/first-hybrid-multidimensional-quantum-inertial-sensor-developed/>.

---

#### ABOUT THE AUTHORS

---



### Lieutenant Colonel Denis Dubravcik

CZ Air Force, JAPCC

Lieutenant Colonel Denis Dubravcik was enlisted in the Czech Air Force in 1996. He graduated from the Brno Military Academy with a BSc in Military Rocket and Aircraft Systems and an MSc in Mechanical Engineering. He is a graduate of the Squadron Officers School at Maxwell Airbase, US. He served, among other functions, as a weapons instructor and commander of the 212<sup>th</sup> Tactical Squadron at Air Force Base Čáslav, the Czech Republic. He is a pilot and instructor on the L-159 ALCA aircraft with more than 1,500 flight hours. He is currently serving in the Assessment, Coordination, and Engagement Branch of the JAPCC as the Plans, Concepts, Development, and Vision Staff Officer.



### Dr Michal Krelina

Czech Technical University in Prague

Dr Michal Krelina is a research scientist at the Czech Technical University in Prague, the Czech Republic. His original background is in high-energy theoretical particle and nuclear physics. Michal is a consultant, analyst, and strategist in quantum technology, emphasizing security and defence applications. His quantum technology research focuses on mapping quantum technology military applications, exploring quantum technology roles in future conflicts, quantum technology risk and threat assessment, and consulting for different departments of NATO, EUSPA (European Union Agency for the Space Programme) and various defence and law enforcement organizations. He has a PhD in experimental nuclear physics.



# Hosted Satellite Payloads

## *NATO's Strategic Pathway to Space Resilience*

By Lieutenant Colonel Arda Ayan, TÜ Air Force, JAPCC

By Major Brian Ladd, US Space Force, JAPCC

### Introduction

Acting alone in the space arena is difficult and may not always be the best strategy for nations. Space is a costly domain to operate in, and requires significant investments in research, development, and operational resources. Additionally, the vast expanse of space presents numerous opportunities for international collaboration and joint defence, especially within alliances like NATO.

Through cooperative efforts in space, NATO member countries can combine their resources, knowledge, and capabilities to strengthen their collective defence posture. Space collaboration encompasses a range of activities, including satellite communications, early warning systems, navigation, and ISR.

NATO member states can enhance their presence in the space domain through *hosted payloads*. The term hosted payloads refers to using available capacity on satellites by allies, partner nations, or companies to accommodate additional transponders, instruments, or other equipment.<sup>1</sup> Hosted payloads provide additional resources, resilience, and contingency capabilities, enhancing the robustness of NATO's space assets by diversifying NATO members' space-based capabilities.

This article provides a concise overview of hosted payloads, the benefits and drawbacks associated with this concept, the role they play in enhancing resilience and deterrence, and offers recommendations for NATO countries to pursue collaborative space initiatives.



## The Evolution of Hosted Payloads

A satellite bus, also known as a spacecraft bus or satellite platform, constitutes the fundamental and standardized structural framework for a satellite. It encompasses and supports the critical systems and subsystems required for the satellite's operational functionality. Concurrently, the payload, customized to fulfil the satellite's precise mission objectives, is integrated onto the bus.

Hosted payloads, also referred as *satellite-as-a-service*, *hitchhiking*, or *piggybacking*, are becoming more appealing for space missions. The idea is to share the spacecraft bus platform with other payloads and still achieve mission success.<sup>2</sup> This timely solution clearly supports the concept of collaboration and collective defence in space. Such an approach enables multiple NATO nations or entities to distribute the costs and advantages associated with space missions, capitalizing on pre-existing infrastructure and reducing overall cost.

## Examples of Hosted Payloads

The following examples illustrate the diverse approaches to the concept of hosted payloads and highlight the different strategies adopted by various stakeholders.

**US-Norway:** The US and Norway have a partnership in which Enhanced Polar Systems-Recapitalization (EPS-R) Flight One and Flight Two payloads are scheduled to launch in 2024 onboard two Arctic Satellite Broadband Mission (ASBM) space vehicles on a dual launch from Vandenberg Space Force Base, California. EPS-R is an Extremely High Frequency (EHF) MILSATCOM system designed to extend EPS services into the early/mid-2030s. Its mission serves to provide 24/7 protected satellite communications for US polar forces operating in the Arctic region. This marks a historic collaboration between Norway and the US Department of Defense (DoD) on a hosted payload where the US is entrusting a Norwegian bus to support strategic missions.<sup>3</sup>

**Government/Commercial:** Government and commercial partnerships for hosted payload initiatives are becoming increasingly popular. Notable examples include:

- Skynet 5, a United Kingdom (UK) government/commercial enterprise communications satellite that also provides bandwidth for critical NATO missions involving ISR.<sup>4</sup>
- The collaboration between Intelsat and the Australian Ministry of Defence (MoD), which launched 22 telecommunications satellites to extend internet routing into space.<sup>5</sup>



*Two of the EPS-R satellites built through the cooperation of the US and Norway go through testing at the Northrop Grumman facility prior to their launch on 15 August 2024.*

- The US, which is in the early stages of coordinating with multiple commercial companies to deliver Link-16 tactical datalink communications through space-to-ground connections from Low Earth Orbit (LEO) to a series of terrestrial receivers. Link-16 from space has the potential to increase the reach and redundancy of tactical communications and would be a key enabler of multi-domain operations.<sup>6</sup>

**Commercial/Commercial:** This partnership model is primarily focused on enhancing access to civilian markets. One prominent example is the collaboration between Intelsat and OneWeb. By integrating payloads onto their commercial satellites, Intelsat and OneWeb can offer high-speed internet access to regions that lack robust infrastructure, bringing broadband internet services to underserved and remote civilian areas.<sup>7</sup>

**Government/Government:** US governmental agencies such as NASA and the National Oceanic and Atmospheric Administration (NOAA) are using hosted payloads to support a variety of environmentally-focused scientific missions. These missions include

the Tropospheric Emissions: Monitoring of Pollution (TEMPO), Commercial Weather Satellite Program (CWSP), Geostationary Extended Observations (GeoXO) Program, and Clouds and the Earth’s Radiant Energy System (CERES).<sup>8</sup>

## Benefits and Considerations

Within the paradigm of NATO’s collective defence, hosted payloads offer manifold advantages. Through collaborating on satellite launch and management projects, NATO member states can reduce the financial burdens of creating and maintaining customized space assets. Through resource pooling and cost-sharing, all NATO nations can actively engage in space missions and leverage space-based capabilities at reduced cost. Hosting payloads on satellites operated by more space-capable NATO members affords new members of the NATO space community the opportunity to access space without the up-front cost of developing, managing, and maintaining their own launch infrastructure or satellite systems.



© Lockheed Martin

*The GeoXO constellation has NOAA payloads hosted on NASA satellites which contribute weather, ocean, and climate observations to NOAA forecasts and predictions.*

From a Research and Development (R&D) perspective, the significance of hosted payloads cannot be understated. Hosted payloads offer substantial benefits for advancing technology, conducting experiments, and testing new concepts in space exploration and satellite operations. Researchers can prototype, deploy experimental instruments or systems on existing satellites, assess their performance in space, gather data, and iterate on designs more efficiently than traditional satellite development cycles. Engaging in R&D activities in space entails inherent risks, including potential hardware failures or operational challenges. By hosting payloads on proven satellites, researchers can mitigate some of these risks by leveraging the reliability and infrastructure of the host platform. This enables more reliable validation of recent technologies and concepts in a real-world space environment.

Hosted payload providers frequently offer flexible options to accommodate payloads in varying orbits. Non-spacefaring countries can collaborate with these providers to tailor their hosted payloads for specific

### Orbital Rocket Launch Costs per Launch in USD

Sounding Rockets	1 million
New Shepard	5 million
Electron	7.5 million
Falcon 9	67 million
Delta IV Heavy	350 million
SLS	4.1 billion
Soyuz-2	35–80 million
Long March	30–81 million
PSLV	21–31 million
GSLV	47 million
Ariane 5	178 million

**Table 1:** *The immutable laws of physics impose a substantial cost for securing passage rights to space, with expenditures ranging from millions to billions of dollars per launch.<sup>9</sup>*



orbital requirements, thereby gaining access to a variety of orbital configurations. This creates a notable opportunity to reach Geostationary Orbit (GEO) and Highly Elliptical Orbit (HEO) which are more challenging to reach than LEO.

Hosted payloads play a critical role in enabling capabilities across various space functional areas, supporting a wide range of civilian and military applications by including:

- Instruments such as GPS receivers or atomic clocks which are critical for providing accurate PNT information.
- Transponders, antennas, or other communication equipment that enhance satellite communication capabilities.
- Sensors and instruments for collecting weather and oceanographic data from space and monitoring space weather phenomena such as solar flares, geomagnetic storms, and radiation levels.

- Sensors and instruments that enhance space situational awareness by tracking and monitoring objects in space, including satellites, debris, and potential threats.
- Imaging sensors, Signal Intelligence (SIGINT) receivers, and other ISR equipment.

While there are many opportunities for technology exchange within NATO from a hosted payload perspective, limitations and barriers can impact sharing knowledge and expertise.

When the satellite bus operator and the payload operator differ, the payload operator is beholden to the actions of the bus. If the bus needs to manoeuvre or an issue occurs, coordination between the two parties is essential, but mission impacts may be unavoidable. When two or more commercial companies co-develop a satellite, there is a high potential for technology exchange barriers which could result in



interoperability issues. Additionally, hosted payloads must be compatible with the satellite bus and other systems on the spacecraft. Technical compatibility issues can limit the ability of NATO members to host a variety of payloads from multiple sources, which may require significant engineering resources. Addressing these limitations requires a coordinated approach, with member countries working together to overcome technical, resource, and policy-related challenges.

## A Pathway to Resilience

The International Telecommunication Union (ITU) governs the allocation and use of radio frequency spectrum for satellite communications. In compliance with ITU regulations, hosted payloads offer a valuable and effective way to reserve specific frequency band slots for SATCOM missions. The ITU manages the limited amount of spectrum available

in the GEO belt. If a nation has claimed a portion of the frequency spectrum but is unable to use it, they risk losing it. By using hosted payloads, NATO nations can coordinate their GEO missions to ensure that ITU frequency allocations are managed and not lost. Operators can maximize spectrum utilization, guarantee regulatory compliance, and deploy SATCOM missions in an economical and scalable way through hosted payloads. Diversifying NATO nations' space capabilities through hosted payloads enhances resilience, reduces vulnerability, and strengthens the overall security posture of space operations.

## The Role of Hosted Payloads in Deterrence

Through several mechanisms, hosted payloads in the space domain support NATO's deterrence efforts. Hosted payloads improve terrestrial and space situational awareness cost-effectively. Ballistic missile launches



*The International Telecommunication Union manages frequency allocations and geostationary orbit locations for the space commons.*

and other hostile actions in orbit are examples of adversary activities that these payloads could be fitted with sensors and instruments to detect and identify. By demonstrating the Alliance's ability to promptly detect and respond to potential threats, NATO can enhance its deterrence posture.

Hosted payloads strengthen NATO's deterrent posture further by fostering better member-state coordination and communication. By using hosted communication payloads to improve the organization's communication channels, NATO member states can make decisions more quickly and securely during a crisis or possible threat. This improved communication infrastructure strengthens NATO's commitment to deterring aggression in space, bolstering the Alliance's collective defence capabilities.

The risks to space systems include any threats that can impact the system's control, reliability, bandwidth availability, security, flexibility, or affordability. Considering the variety of intentional threats (Directed Energy Weapons (DEW), electronic, cyber, or kinetic attacks) highlights the importance of deterrence in the space domain. At the 2021 Brussels Summit, NATO recognized that attacks to, from, or within space present a clear challenge to the security of the Alliance and could lead to the invocation of Article 5 of the North Atlantic Treaty. In this case, when a satellite with a hosted payload is targeted, it potentially impacts multiple NATO members. By integrating hosted payloads with strategic objectives and enhancing operational flexibility, NATO can better deter potential threats by ensuring continuous and reliable access to critical space assets.

## Recommendations

When NATO declared space an operational domain in December 2019, it demonstrated the Alliance's understanding of the critical role that space-based capabilities play in modern warfare and security operations. This declaration not only acknowledges NATO's reliance on space assets for communication, navigation, intelligence gathering, and early warning systems, but it also reaffirms the Alliance's commitment to deterrence and defence against space threats.

NATO should encourage member nations to have a desired space roadmap that identifies how they best believe space should be used and developed for their defence.

Regardless of their current level of space capability, NATO nations pursuing space capabilities would benefit from investing in hosted payload projects because it would strengthen the spirit of the Alliance and improve collective security. By participating in hosted payload projects, NATO countries can pool their resources and expertise to develop and deploy space-based capabilities more efficiently and effectively. These collaborative efforts foster a sense of solidarity and cooperation among member states, strengthening the Alliance's bonds and encouraging unity in addressing shared security challenges.

---

**[...] 'Diversifying NATO nations' space capabilities through hosted payloads enhances resilience, reduces vulnerability, and strengthens the overall security posture of space operations.'**

---

The commercial sector leads in various aspects of R&D concerning satellite bus and payload development. However, ambiguity exists within space law regarding the recognition of commercial satellites as legitimate targets, mainly when a commercial satellite hosts a military payload. To overcome this complexity, NATO nations should diversify the notion of hosted payloads to include both commercial and governmental entities. By embracing a diversified approach, NATO countries can benefit from the expertise and resources of the commercial sector while ensuring the integrity of military payloads and expediting the resolution of legal uncertainties they may entail.

## Conclusion

Hosted payload projects allow NATO nations to leverage existing satellite infrastructure while sharing the costs of launching and operating payloads, making space more accessible and affordable for all members. This inclusive approach ensures that even nations with

limited space capabilities can contribute meaningfully to collective security efforts while reaping the benefits of space-based assets.

Recognizing the strategic importance of space operations on the battlefield potential adversaries have made a concerted effort to undermine or limit space assets' advantages for NATO nations. Implementing hosted payloads allows the Alliance to pursue two overarching objectives simultaneously. First, NATO can diversify resources across all functional areas of space operations and improve resilience. Second, by implementing a collective defence approach, the Alliance can deter potential hostile actions against its space assets, promoting the integrity and effectiveness of NATO's space-based operations. ●

1. Category: Hosted Payloads, Office of Space Commerce. <https://www.space.commerce.gov/category/government-business/hosted-payloads/> (accessed 2 July 2024).
2. State-of-the-Art of Small Spacecraft Technology, Chapter 2.2.1 Hosted Payloads. <https://www.nasa.gov/smallsat-institute/sst-soa/platforms/#2.2.1> (accessed 3 June 2024).
3. Recapitalization Flight One Payload Thermal Vacuum Test, Space Systems Command Media Release, 3 August 2023 (accessed 7 June 2024).
4. Guidance SKYNET 6, UK MOD, 21 November 2023. <https://www.gov.uk/guidance/sky-net-6#about-sky-net-5> (accessed 10 July 2024).
5. Product Hosted Payloads, INTELSAT. <https://www.intelsat.com/space/products/hosted-payloads/> (accessed 27 June 2024).
6. Space Development Agency Successfully Completes Space to Ground Transmission from Link 16 Tactical Data Network, SDA, 28 November 2023. <https://www.sda.mil/space-development-agency-successfully-completes-space-to-ground-transmission-from-link-16-tactical-data-network/> (accessed 7 June 2024).
7. Intelsat signs \$ 500 m deal with Eutelsat for OneWeb connectivity, Dan Swinhoe, 25 March 2024. <https://www.datacenterdynamics.com/en/news/intelsat-signs-500m-deal-with-eutelsat-for-oneweb-connectivity/> (accessed 27 June 2024).
8. Tropospheric Emissions: Monitoring of Pollution, NASA. <https://eosps.nasa.gov/missions/tropospheric-emissions-monitoring-pollution-emi-1> (accessed 2 July 2024).
9. How Much Does It Cost To Launch A Rocket? [By Type & Size], Ria Urban, 16 August 2023. <https://spaceimpulse.com/2023/08/16/how-much-does-it-cost-to-launch-a-rocket/> (accessed 3 June 2024).

---

#### ABOUT THE AUTHORS

---



#### Major Brian Ladd

US Space Force, JAPCC

Major Brian Ladd graduated from Bowling Green State University in 2005 with a Bachelor's degree in History and received his commission by AFROTC. His first tour was at the 4<sup>th</sup> Space Operations Squadron at Schriever AFB in Colorado Springs, CO, where he was a Satellite Operator of the MILSTAR communications system. His other operational tour was as the Liaison Officer at RAF Fylingdales Strategic Missile Warning Radar. He has completed many Space Staff assignments at Joint Base Pearl Harbor-Hickam, Vandenberg AFB, and Offutt AFB. He transitioned to the US Space Force in October 2020. Since June 2021 he serves as the Chief of Cyber and Space Readiness at the JAPCC.



#### Lieutenant Colonel Arda Ayan

TÜ Air Force, JAPCC

Lieutenant Colonel Arda Ayan graduated from the Turkish Air Force Academy in 2005 with a Bachelor's degree in Computer Engineering. Following his Master's degree in Space Sciences in 2014, he took on the duties of Satellite Control Officer and Satellite Operators' Supervisor, respectively, in the military Earth observation satellite command and control centre in Türkiye in charge of Göktürk-1 and Göktürk-2 remote sensing satellites. Between August 2021–August 2024, he was assigned as Space SME at the JAPCC. He serves as the Reconnaissance Satellite Battalion Commander since August 2024 under the Turkish Space Command.

# Bending the ‘Hufnagel’

## *Defence Acquisition Principles for the New Security and Technology Environment*

By Kristin Waage, Sascha Krell, Christoph Mueller, Dr. Dirk Zimper, and the Honourable Alan Shaffer

### Introduction

In 1925, General of the Infantry Hans von Seeckt, then Chief of the Army Command, published a memorandum called the ‘Hufnagelerlass’ condemning the increasing bureaucratization within the Army Command. In the memorandum, von Seeckt sarcastically exaggerated the bureaucratic effort involved in introducing a new horseshoe nail as symbol for very simple business processes in the Reichswehr. In conclusion, he called on responsible commanders to cooperate in reducing the bureaucracy.

Almost one hundred years later, the outcome of military acquisition programs still ranges from major failings, such as the US Zumwalt Class Destroyer with a cost overrun of more than 80% and two decades of program delay,<sup>1</sup> to great successes such as the rapid fielding of Germany’s tracked howitzer into a war zone while requiring the Ukrainians to develop a domestic fire control system within a couple of weeks. Experiences from rapid deployment of systems to

ongoing operations within NATO countries also demonstrate how quick acquisitions are possible ‘when needs are greatest’<sup>2</sup>

In sum, few would disagree that the processes for procuring military systems within NATO countries must be improved. Acquisitions are delayed and often exceed budgets. In some cases, they do not even yield the expected performance. But what precisely should be done? For years, there has been ample evidence for, and attention to, the problems in defence acquisition practices across NATO countries.<sup>3</sup> National defence acquisition systems have been perceived to be ‘broken’ for decades.<sup>4</sup> Yet despite countless inquiries and repeated improvement efforts, most countries remain stuck in old practices or struggle with alternative approaches, showing only a few promising examples.<sup>5</sup>

At the same time, the need for NATO countries to improve their acquisition practices has become particularly urgent considering two developments. The first

*National defence procurement systems have been considered ‘broken’ for decades. Yet despite countless studies and repeated efforts to improve, most countries remain stuck in old practices or struggle with alternative approaches.*



is the current security environment, including the ongoing war between Russia and Ukraine, and increased tensions in the Indo-Pacific and Middle East. The second is the increasing importance of commercially-driven Emerging and Disruptive Technologies (EDTs) to military-technological superiority. These developments put pressure on the range of capabilities NATO countries must possess to deter and handle threats in the 21<sup>st</sup> century, and urge the Allies to innovate, acquire, and field leading-edge military technological systems faster, better, and cheaper than geopolitical rivals.<sup>6</sup>

This is the first in a series of three articles intending to reflect on the current state of military acquisition programs and provide a concise set of questions to senior managers with decades of combined experience in military programs. It provides a summary of research on the current state of defence acquisitions and derives hypotheses that will be further explored in the subsequent articles.

### A Common Dilemma – The State of Defence Acquisitions

Generally, defence acquisitions are perceived as a trade-off between the three outcome parameters: performance, cost, and schedule. These trade-offs are always in tension and are known as the ‘iron triangle’<sup>7</sup>:

‘you can have it fast, good, or cheap – pick two.’<sup>8</sup> However, existing research and experience give ample evidence, that defence organizations often struggle to get even two.

Many studies examine challenges in cost management in defence acquisitions. *Table 1* on page 54 shows illustrative statistics on cost overruns in defence acquisition projects. The statistics show how many procurement projects – and particularly major acquisitions – are not completed within budget. The ability to accurately assess costs varies between acquisitions, and novel and/or highly technologically complex materiel make it particularly difficult to calculate costs.<sup>9</sup> Furthermore, life-cycle costs tend to be underestimated by government as well as vendor, either due to a lack of data or systematic incentives to underestimate, or both.<sup>10</sup>

Irrespective of cost overruns, scholars also document how the unit costs of technologically advanced defence materiel have increased between generations of weapon systems.<sup>11</sup> This puts pressure on defence acquisition budgets. Ultimately, such technology-driven inflation dynamics result in making cutting-edge, technologically advanced military systems less affordable for states.<sup>12</sup> The increasing costs of defence materiel and prioritization of quality over quantity risk creating a ‘technology gap’ within NATO between the most technologically advanced nations and other nations in





Study	Country	Findings
17. RüRep <sup>13</sup>	GE	Major procurement programmes record an average cost overrun of about 20%.
Gray <sup>14</sup>	UK	Program costs increase 40% on average or about £ 300 million.
DE&S <sup>15</sup>	UK	While improving since the 2009 Gray report, 27% of the largest defence procurement projects with an in-service date since 2017 did not complete within their P50 cost approval.
GAO Report <sup>16</sup>	US	In 2022, major procurement programmes showed cost overruns between 50–150% on average.
GAO Report	US	While successful, the F-35 program faces a 50% (233 billion USD) cost overrun by 2023.

**Table 1:** A sample of cost overruns in defence procurement projects.

Study	Country	Findings
Perry (2017)	CA	By 2016, 12 of 25 major defence acquisitions were late compared to the schedule estimate from the previous year.
15. RüRep <sup>20</sup>	GE	Major procurement programmes such as armoured vehicles, ships and airplanes are delayed about 5 years on average.
17. RüRep	GE	In 2023 newly started projects and projects still in preparation are already significantly delayed.
Gray (2009)	UK	Programs are delayed by 80% or about 5 years on average.
DE&S	UK	While improving since the 2009 Gray report, 48% of the largest defence procurement projects with an in-service date since 2017 did not complete within their P50 schedule approval.
Kvalvik et al. (2019)	NO	65% of projects (2004–2016) are delayed by more than 1 year and on average by ca. 3 years.
GAO Report 2023	US	Among 26 Major Defence Acquisition Programs (MDAPs), more than half experience delays – and have been doing so for several consecutive years. There is a trend of increasing delays in MDAPs.

**Table 2:** A sample of delays in defence procurement projects.

the Alliance. Moreover, lacking enough depth creates capacity and sustainability gaps, jeopardizing both credible deterrence and the ability to sustain combat.

Defence acquisitions are also subject to long lead times,<sup>17</sup> and most acquisitions do not manage to complete on schedule.<sup>18</sup> *Table 2* summarizes statistics on delays in defence procurement projects across nations. It shows how projects on average are typically delayed by 3–5 years with outliers of up to two decades. Even when projects are completed on time, long schedules may still cause challenges. For instance, the former United States Defence Investment Unit Director, Michael Brown, stated that acquisition of major procurement programmes has on average taken 6.9 years from initiation to initial operating capability,<sup>19</sup> requiring a long-time span for full capability replacement.

---

**[...] ‘...many of the projects that survive through the prioritization and selection process tend to be those that look best on paper. However, those are often also the ones with the largest cost and time underestimation and/or promises of unrealistic benefits, setting up the conditions for failure once initiated. Yet, it is often difficult for decision-makers to cancel poorly performing projects once initiated, for example due to political pressure or fear of embarrassment.’**

---

For rapidly developing technologies, such as cutting-edge software and IT, the long lead time coupled with a high risk of delays are particularly problematic. Long schedules and delays also increase problems with responsibility, accountability, turnover among project personnel, and institutional memory.

One major reason for both cost and time overruns in defence acquisitions, is the inclination for over-specification and changing requirements.<sup>21</sup> There are no second places in war, urging military organizations to pursue state-of-the-art technology to outperform adversaries. The requirements for system reliability and robustness are also higher in a military context. How-

ever, while some systems require cutting-edge technology, other systems would suffice with an ‘80% solution.’<sup>22</sup> In such instances, off-the-shelf solutions might exist that could provide sufficient performance, alternatively with minimal adjustments.<sup>23</sup>

Risk aversion can drive overly detailed or ambitious system requirement specifications.<sup>24</sup> ‘Gold-plating’ has also been a widespread problem in defence acquisitions for decades<sup>25</sup> – occurring due to asymmetric expert power by the vendor as well as military personnel themselves, and insufficient mechanisms for external verification of system requirements.<sup>26</sup> While risk aversion is a driver of gold-plating, studies also document how gold-plating mainly arises from overly ambitious requirements that privileges the newest and best technology.<sup>27</sup> There are also cases of system performance itself being negatively affected by over-specification. One example is Norway’s acquisition of a tailored variant of the NH90 multirole helicopter, where Norway eventually decided to terminate the contract due to persistent underperformance, cost overruns, and significant delivery delays.<sup>28</sup>

Professor Bent Flyvbjerg introduces a phenomenon he calls ‘survival of the unfittest.’<sup>29</sup> He observes how many of the projects that survive through the prioritization and selection process tend to be those that look best on paper. However, those are often also the ones with the largest cost and time underestimation or promises of unrealistic benefits, setting up the conditions for failure once initiated. Yet, it is often difficult for decision-makers to cancel poorly performing projects once initiated, for example due to political pressure or fear of embarrassment.<sup>30</sup> Although Flyvbjerg examined civilian (infrastructure) megaprojects, not defence procurement projects, scholars have observed the same tendencies in defence acquisitions, both due to the optimism bias and moral hazard.<sup>31</sup>

Additionally, it should not be ignored that many defence acquisitions are, in fact, highly complicated undertakings.<sup>32</sup> Projects comprise a diverse range of materiel, equipment, and systems. Many new technological systems are also increasingly intricate – both the technologies in themselves, but also the



*A sense of urgency acts as a catalyst for the rapid development and deployment of (initial) operational capabilities.*

---

**[...]** *'For rapidly developing technologies, such as cutting-edge software and IT, the long lead time coupled with a high risk of delays are particularly problematic.'*

---

system of systems they are part of and the process of ensuring interoperability across systems as well as Allied and Partner nations.<sup>33</sup>

In sum, beside political, economic, and industrial influence, defence acquisition programs struggle with over-specification, opposing or overly ambitious requirements, uncharted technological territory, risk-aversion, legal framework, bureaucracy, and diffusion of responsibility, resulting in major delays and cost overruns.<sup>34</sup>

## **A Hypothesis – We Can Do Better and Quicker**

In recent decades, numerous acquisition recommendations and reforms across NATO nations have been aimed at improving the ability to meet cost, time, and quality targets. Already in the early 2000s, defence acquisition experts recognized the need to move towards flexible and evolutionary acquisition approaches.<sup>35</sup> Many have also argued for differentiated, or tailored, acquisition approaches.<sup>36</sup> However, challenges persist and defence organizations across (as well as beyond) NATO seem to be stuck in a never-ending struggle to implement changes.<sup>37</sup> RAND research identifies multiple root causes, including high turnover, particularly among senior leaders, insufficient incentives and support for tailoring, and insufficient education, training and experience among





acquisition personnel to leverage tailored approaches efficiently.<sup>38</sup> Lack of institutional memory to learn from past experiences may also impede effective changes.<sup>39</sup>

The successful avoidance of a majority of the aforementioned root cases can be exemplified with Israel's 'Iron Dome' missile defence system. It went from the drawing board to combat readiness within less than four years. Following an initial operational capability in 2011, the capability of the system has been constantly upgraded while scaling capacities up to ten operational systems effectively safeguarding Israel's lower tier air domain.<sup>40</sup>

Avoiding over-specification by focusing on the threat spectrum on hand, allowing the system to be extendable in the future and following Israeli's political, eco-

nomical, and industrial priorities had been key success factors. In addition, close collaboration between user and procurement as well as technical expertise from the United States mitigated technological and programmatic risks.

In sum, despite the well-documented and recurring challenges in defence acquisitions, we put forward the hypothesis that military capabilities can be acquired both faster and better than what is currently the norm. Furthermore, in what has become an impenetrable 'jungle' of acquisition challenges and policy recommendations, we believe that the most important – and actionable – policy changes for improving defence acquisitions can be uncovered by homing in on the decades of experience and learning acquired by key defence acquisition experts in NATO. This will be the topic of the second paper.

In particular, we will investigate three key avenues for improving future procurement:

1. Increasing the use of phased development step-wise expanding new capabilities.
2. Following a more software-centric strategy with open system architectures, digital twins, and agile development processes.
3. Empowering acquisition specialists – and particularly leadership. Strong leadership is required to implement new policies and procedures, manage risk, and ultimately bring a new defence acquisition culture to life.

In our second paper, we will evaluate these hypotheses by drawing on insights from interviews with senior acquisition management leadership. The final paper then aims to derive concrete and actionable recommendations to improve future as well as ongoing national and cross-border acquisition programs. ●

1. Roblin, S., 'Why the Zumwalt-Class Destroyers Failed to Meet the Navy's Expectations', *The Reboot*, [web blog], 25 December 2021, <https://nationalinterest.org/blog/reboot/why-zumwalt-class-destroyers-failed-meet-navys-expectations-198412>, (accessed 7 April 2024).
2. Gray, B., 'Review of Acquisition for the Secretary of State for Defence: An Independent Report by Bernard Gray', BIP Solutions, 2009, p. 8.
3. Bennett, F., 'The Seven Deadly Risks of Defence Projects', *Security Challenges* vol. 6, no. 3, 2010, pp. 97–111. Smith, R., P., 'Defence Acquisition and Procurement: How (Not) to Buy Weapons', Cambridge, Cambridge University Press, 2022.
4. Johnson, W., M., and Johnson, C., O., 'The Promise and Perils of Spiral Acquisition: A Practical Approach to Evolutionary Acquisition', *Acquisition Review Quarterly*, vol. 9, no. 3, 2002, pp. 175–89. Public Accounts Committee, *Improving the Performance of Major Defence Equipment Contracts*, London, London: House of Commons 185, 2021.
5. Retter, L., et al., 'Persistent Challenges in UK Defence Equipment Acquisition', RAND Corporation, 23 June 2021, [https://www.rand.org/pubs/research\\_reports/RRA1174-1.html](https://www.rand.org/pubs/research_reports/RRA1174-1.html), (accessed 9 November 2023). Schwartz, M., *Defense Acquisitions: How DOD Acquires Weapon Systems and Recent Efforts to Reform the Process*, Washington, Congressional Research Service, 2014).
6. Wong, J., P., et al., 'Improving Defense Acquisition: Insights from Three Decades of RAND Research', RAND Corporation, 16 June 2022, [https://www.rand.org/pubs/research\\_reports/RRA1670-1.html](https://www.rand.org/pubs/research_reports/RRA1670-1.html), (accessed 12 February 2024). Stanley-Lockman, Z., 'From Closed to Open Systems: How the US Military Services Pursue Innovation', *Journal of Strategic Studies*, vol. 44, no. 4, 2021, pp. 480–514.
7. Neves, S., and Jack Strauss, J., 'Survival Guide for Truly Schedule Driven Development Programs', *Defense AT&L*, 2008, pp. 21–23.
8. Johnson, J., 'Fast, Good or Cheap: How to Achieve the Iron Triangle', *Business.com*, 10 April 2024, <https://www.business.com/articles/fast-good-cheap-pick-three/> (accessed 15 April 2024).
9. Davies, C., 'Understanding Defence Procurement', *Canadian Military Journal*, vol. 15, no. 2, 2015, pp. 5–15.
10. De Spiegeleire, S., 'Ten Trends in Capability Planning for Defence and Security', *The RUSI Journal* 156, no. 5, 31 October 2011, <https://doi.org/10.1080/03071847.2011.626270>,

(accessed 23 May 2024). Ibid., p. 2. Kvalvik, S., N., et al., *Norwegian Defence Research Establishment*, [website], 2019, <https://ffi-publikasjoner.archive.knowledgegear.net/bitstream/handle/20.500.12242/2650/19-01934.pdf> (accessed 25 April 2024).

11. Matthew Uttley, M., 'Routledge Handbook Of Defence Studies', in Galbreath, (ed.), *Defence Procurement*, London, 2018, pp. 72–86; *Ibid.*, p. 6.
12. *Ibid.*
13. Bundesministerium der Verteidigung, '17. Bericht des Bundesministeriums der Verteidigung zu Rüstungsangelegenheiten', 3 June 2023, <https://www.bmwg.de/resource/blob/5639826/45547a72b96fb60d6d82f061913d9d3a/17-ruestungsbericht-data.pdf>, (accessed 18 May 2024).
14. *Ibid.*, p. 2.
15. HCDC Sub-Committee inquiry, *Written Evidence from the Secretary of State for Defence*, London, 2023, <https://committees.parliament.uk/writtenevidence/120368/default/>, (accessed 12 May 2024).
16. US Government Accountability Office, *Weapon Systems Annual Assessment*, US, 2022, [www.gao.gov/assets/gao-22-105230.pdf](http://www.gao.gov/assets/gao-22-105230.pdf), (accessed 24 April 2024).
17. Presterud, A., O., et al., *Norwegian Defence Research Establishment FFI report*, [website], 2018, <https://www.ffi.no/publikasjoner/arkiv/effektive-materiellanskaffelser-i-forsvaret-kartlegging-av-tidsbruk-forsinkelser-og-gjennomforingskostnader>, (accessed 15 May 2024).
18. Kvalvik et al., *Norwegian Defence Research Establishment FFI report*, [website], 2019, <https://www.ffi.no/publikasjoner/arkiv/hvordan-skape-okonomisk-handlingsrom-i-den-nye-langtidsplanen-potensial-for-forbedring-og-effektivisering-20212024>, (accessed 18 May 2024).
19. Brown, M., *Statement of Michael Brown, director, Defense Innovation Unit, before the senate armed services committee on accelerating innovation for the warfighter*, [website], 2022, [https://www.armed-services.senate.gov/imo/media/doc/WRITTEN%20STATEMENT\\_DIU%20Director%20for%20SASC%20ETC%20Hearing%20on%20Accelerating%20Inno...pdf](https://www.armed-services.senate.gov/imo/media/doc/WRITTEN%20STATEMENT_DIU%20Director%20for%20SASC%20ETC%20Hearing%20on%20Accelerating%20Inno...pdf), (accessed 26 May 2024).
20. Bundesministerium der Verteidigung, '15. Bericht des Bundesministeriums der Verteidigung zu Rüstungsangelegenheiten', 3 June 2022, <https://www.bmwg.de/resource/blob/5456944/a2db4d6cb4c5873113e39ad9292f269/20220629-download-15-bericht-des-bmwg-zu-ruestungsangelegenheiten-data.pdf>, (accessed 18 May 2024).
21. Hambleton, K., et al., 'Ten Chronic Challenges', *Defence Studies*, 5 December 2013, <https://www.tandfonline.com/doi/abs/10.1080/14702436.2013.845384>, (accessed 4 June 2024). *Ibid.*, p. 5. Hedvall, M., 'Change as a Cost Driver in Defence Procurement', *Defence and Peace Economics* vol. 15, no. 1, 2004, <https://doi.org/10.1080/1024269042000164522>, (accessed 29 May 2024); Brooke-Holland, L., *House of Commons Library*, [website], 2023, <https://commonslibrary.parliament.uk/research-briefings/cbp-9764/> (accessed 3 June 2024).
22. *Ibid.*, p. 2.
23. Presterud, A., O., et al., *Norwegian Defence Research Establishment FFI report*, [website], 2016, *Effektive materiellanskaffelser i Forsvaret – økonomiske gevinster ved økte hyllewareanskaffelser* (ffi.no), (accessed 14 May 2024).
24. Michèle A. Flournoy, M., A., 'AI Is Already at War', *Foreign Affairs*, 24 October 2023, <https://www.foreignaffairs.com/united-states/ai-already-war-flournoy> (accessed 19 May 2024).
25. Presterud, A., O., et al., *Norwegian Defence Research Establishment FFI report*, [website], 2015, <https://www.ffi.no/en/publications-archiv/effektive-materiellanskaffelser-i-forsvaret-okonomiske-gevinster-ved-okte-hyllewareanskaffelser>, (accessed 19 May 2024).
26. *Ibid.*, p. 18.
27. *Ibid.*, p. 17.
28. Olsen, J., M., 'Norway Ends Contract for NH90 Helicopters, Wants Full Refund', *Defense News*, 10 June 2022, <https://www.defensenews.com/industry/2022/06/10/norway-ends-contract-for-nh90-helicopters-wants-full-refund/>, (accessed 18 May 2024).
29. Bent Flyvbjerg, B., 'Survival of the Unfittest: Why the Worst Infrastructure Gets Built – and What We Can Do about It', *Oxford Review of Economic Policy* vol. 25, no. 3, 1 October 2009, <https://doi.org/10.1093/oxrep/grp024>, (accessed 2 June 2024).
30. *Ibid.*, p. 5.
31. *Ibid.*, p. 21.
32. *Ibid.*, p. 3.
33. Gilli, A., and Mauro Gilli, M., 'Why China Has Not Caught Up Yet: Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage', *International Security*, vol. 43, no. 3 2019, pp. 141–89, [https://doi.org/10.1162/isec\\_a\\_00337](https://doi.org/10.1162/isec_a_00337); Gorod, A., Tiep Nguyen, and Leonie Hallo, 'Systems Engineering Decision-Making: Optimizing and/or Satisficing?', *2017 Annual IEEE International Systems Conference (SysCon)*, April 2017, pp. 1–6, <https://doi.org/10.1109/SYSCON.2017.7934775>, (accessed 5 June 2024).
34. *Ibid.*, p. 3.
35. *Ibid.*, p. 4.

36. Stanley-Lockman, Z., 'From Closed to Open Systems', *Journal of Strategic Studies*, vol. 44, 13 May 2021, <https://www.tandfonline.com/doi/full/10.1080/01402390.2021.1917393>, (accessed 5 June 2024); *Ibid.*, p. 6.

37. *Ibid.*, p. 10.; *Ibid.*, p. 6.

38. Bartels, E., M., Jeffrey A. Drezner, and Joel B. Predd, 'Building a Broader Evidence Base for Defense Acquisition Policymaking' *RAND Corporation*, 19 May 2020, [https://www.rand.org/pubs/research\\_reports/RR4202-1.html](https://www.rand.org/pubs/research_reports/RR4202-1.html), (accessed 5 June 2024); Mayer, L., A., et al.,

'Prototyping Using Other Transactions: Case Studies for the Acquisition Community', *RAND Corporation*, 2020, [https://www.rand.org/content/dam/rand/pubs/research\\_reports/RR4400/RR4417/RAND\\_RR4417.pdf](https://www.rand.org/content/dam/rand/pubs/research_reports/RR4400/RR4417/RAND_RR4417.pdf), (accessed 9 June 2024).

39. *Ibid.*, p. 5.

40. Vick, K., 'The Secret of the Wonder Weapon That Israel Will Show Off to Obama', *Time*, 13 March 2013, <https://world.time.com/2013/03/19/the-secret-of-the-wonder-weapon-that-israel-will-show-off-to-obama/>, (accessed 12 June 2024).

---

## ABOUT THE AUTHORS

---

### Ms Kristin Waage

Norwegian Defence Research Establishment (FFI), Norway

Kristin Waage works as a researcher at the division for Strategic Analyses and Joint Systems at FFI since August 2018. She holds a MSc in Economics and Business Administration from the Norwegian School of Economics (NHH), a Master in International Management from CEMS, and an MA in Science and International Security from King's College London. Her research areas at FFI include military technology acquisition and implementation, particularly focusing on artificial intelligence, and geoeconomics.

### Mr Sascha Krell

MBDA Missile Systems, Germany

Sascha Krell works as Technology Project Manager at MBDA Missile Systems Germany since July 2022. He contributed in different functions to the development of ground based air defence systems in various stages of project life-cycle. Currently he has a focus on integrating effects from various systems in Multi-Domain environments. Mr Krell also served twelve years in the German Armed Forces Navy including work as of a project officer in the mid-life modernization of F123 type frigates.

### Mr Christoph Müller

MBDA Missile Systems, Germany

Christoph Müller works as Head of Hypersonic Solutions at MBDA Missile Systems Germany since November 2023. Previously, he was Executive Board Representative for Defence and Security Research at the German Aerospace Centre and from 2017 to early 2020 Executive Office at the NATO Science & Technology Organization, where he is currently Vice Chairman of the Applied Vehicle Technology Panel. He also served twelve years in the German Armed Forces as commander of an explosive ordnance disposal platoon specializing in CBRNe, including a deployment with the International Security Assistant Force (ISAF) in Afghanistan.

### Dr. Dirk Zimmer

MBDA Missile Systems, Germany

Dr. Dirk Zimmer has been Director Future Systems and a member of the Management Board of MBDA Missile Systems Germany since November 2022. In his role, he is responsible for the future topics of MBDA Germany, including high-energy lasers, hypersonic applications, the further development of ground-based air defence and remote carriers for the Future Combat Air System. Previously, he worked for the German Aerospace Centre and was in charge of security and defence research as Executive Board Representative. His military career started in 2004 when he joined the German Armed Forces and completed the 92<sup>nd</sup> officer training course at the Air Force Officer School. Dr. Zimmer studied aerospace engineering at the University of the German Armed Forces in Munich and completed his doctorate in engineering in 2015.

### Honourable Mr Alan R. Shaffer

Washington Operations for MIT Lincoln Laboratory, United States

Alan R. Shaffer brings over four decades of distinguished leadership in defence and technology to his current role as Director, Washington Operations for MIT Lincoln Laboratory since April 2022. Previously, from 2019 to 2021, he served as Deputy Under Secretary of Defense for Acquisition and Sustainment. His career highlights include directing the NATO Collaboration Support Office from 2015 to 2018. Mr Shaffer's extensive government tenure also includes significant roles like Principal Deputy Assistant Secretary of Defense for Research and Engineering from 2007 to 2015. Before his civilian career, he served 24 years in the United States Air Force, retiring as a Colonel, with diverse assignments in command, intelligence, and acquisition oversight globally. Mr Shaffer holds advanced degrees in Meteorology and National Resource Strategy and has received prestigious awards for his public service, including multiple Presidential Rank Awards and the Secretary of Defense Medal.



**LEAD  
WITHOUT  
LIMITS**

**SNC<sup>®</sup>**





Heads of State meet for the NATO Summit in Washington D.C., 9–11 July 2024.

# The Evolving Context for Deterrence

## *Technology and Policy Challenges*

By Prof. Stephen J. Cimbala and Dr. Adam Lowther

The member-states of the North Atlantic Treaty Organization (NATO) face an unprecedented challenge in Russia's aggression against Ukraine and their threats to employ nuclear weapons against NATO.<sup>1</sup> There is also the potential risk of Chinese aggression against Taiwan; should the United States come to the aid of Taiwan and China attack the United States, the US would likely seek support under Article 5 of the NATO charter. Either directly or indirectly, Europe cannot avoid the consequences of a war in the Pacific. This makes it imperative for NATO member-states that deterrence holds.

The following discussion identifies eight of the most important challenges facing alliance efforts to maintain deterrence. The reality of modern deterrence is

that it is more uncertain, and difficult to maintain because of the added complexities of the cyber and space domains and additional post-Cold War geopolitical variables. With both the space and cyber domains playing a prominent role that did not exist during the Cold War and new technologies reshaping deterrence, understanding deterrence is certainly a more pressing need than ever before.<sup>2</sup>

### **Eight Challenges of Modern Deterrence**


**1. The threat of cyberattacks.** Cyberwar among state and non-state actors is already a significant danger to international security.<sup>3</sup> Cyberattacks occur as solo excursions or as supplements to kinetic attacks. Should

Russia ever attack NATO, it would likely lead with a cyberattack to leave NATO blind, deaf, and dumb.<sup>4</sup> China would likely follow a similar approach. Both authoritarian regimes understand that there is a chance for victory if the United States and its allies are prevented from mobilizing combat forces and supporting logistics. This makes the early use of cyberattack enticing for potential aggressors, and countering them an essential aspect of NATO's deterrence strategy. After all, if NATO is paralyzed by cyberattacks to alliance C2 networks, or by a combined cyber & Information Operations (IO) campaign which undermines or delays political unity, airpower becomes impotent.

It is important to keep in mind that both the public and private sectors are vulnerable to cyberattack. The possibility of a crippling attack against, for example, the private firms that support US Transportation Command's logistics network is very high.<sup>5</sup> A cyberattack on the United States' integrated tactical warning and attack assessment network and nuclear command and control networks would likely precede the use of a nuclear weapon by the Russians, for example. This makes a robust and secure cyber domain a fundamental component of a deterrence strategy, writ large, and nuclear deterrence, more specifically, by denying a key vulnerability to the adversary.

**2. NATO's reliance on space assets.** NATO relies heavily on space assets for intelligence collection and military operations. Airpower is particularly dependent upon space to employ precision-guided munitions. It should come as no surprise that Russia has an array of anti-space capabilities designed to prevent the use of those space assets that are critical to Allied air, land, and sea operations.<sup>6</sup> American and European government agencies are already working with defense contractors to explore ways to increase the reliability and resilience of space-based and space-dependent systems for reconnaissance and surveillance, communications, early warning, command and control, and other functions.<sup>7</sup> Russia and China tested satellites for Rendezvous and Proximity Operations (RPO) in various orbits, ostensibly for inspection and repair of friendly satellites, but which would also be capable of close inspection or destruction of NATO member-state satellites, if so tasked.<sup>8</sup> Options for increasing the resilience of orbital platforms include

*Should Russia ever attack NATO, it would likely lead with a cyberattack to leave NATO blind, deaf, and dumb.*

 © PopTika/Shutterstock.com

deploying numerous smaller satellites in critical orbits, equipping satellites with defensive measures (including stealth and manoeuvrability), and offensive capabilities for responding to perceived threats.<sup>9</sup> Legal issues arise with respect to whether an attack on critical mission satellites for national defence constitutes an attack on NATO, but it is undoubtedly a real challenge the Alliance must deter.

**3. The Role of Hypersonics.** Adversaries' development of hypersonic weapons, including delivery systems for nuclear warheads, raises serious issues for deterrence and defence planners.<sup>10</sup> In the case of nuclear deterrence, a reliable second-strike capability is a necessary condition for the success of deterrence by

credible threat of retaliatory punishment. Hypersonic weapons compress the time available for warning and selection of an appropriate response.<sup>11</sup> This is particularly problematic in Europe, where distances from Russian bases are shorter, and hypersonic weapons can easily reach targets. The only viable option may be possessing a secure second strike capability in order to ride out a first strike, determine whether it is conventional or nuclear, and respond accordingly.

National leaders might have only a few minutes from the initial launch detection of an enemy's first strike to the arrival of warheads at their assigned targets. This 'attack time compression challenge' can leave leaders fearful of losing their deterrence assets.<sup>12</sup> With the United Kingdom, France, and NATO possessing small nuclear arsenals that, in the case of NATO specifically, are vulnerable to first strike elimination, a national command authority (president or prime minister) may view pre-emptive nuclear employment as a necessary option in a 'use it or lose it' circumstance. NATO's collective decision-making process, however,

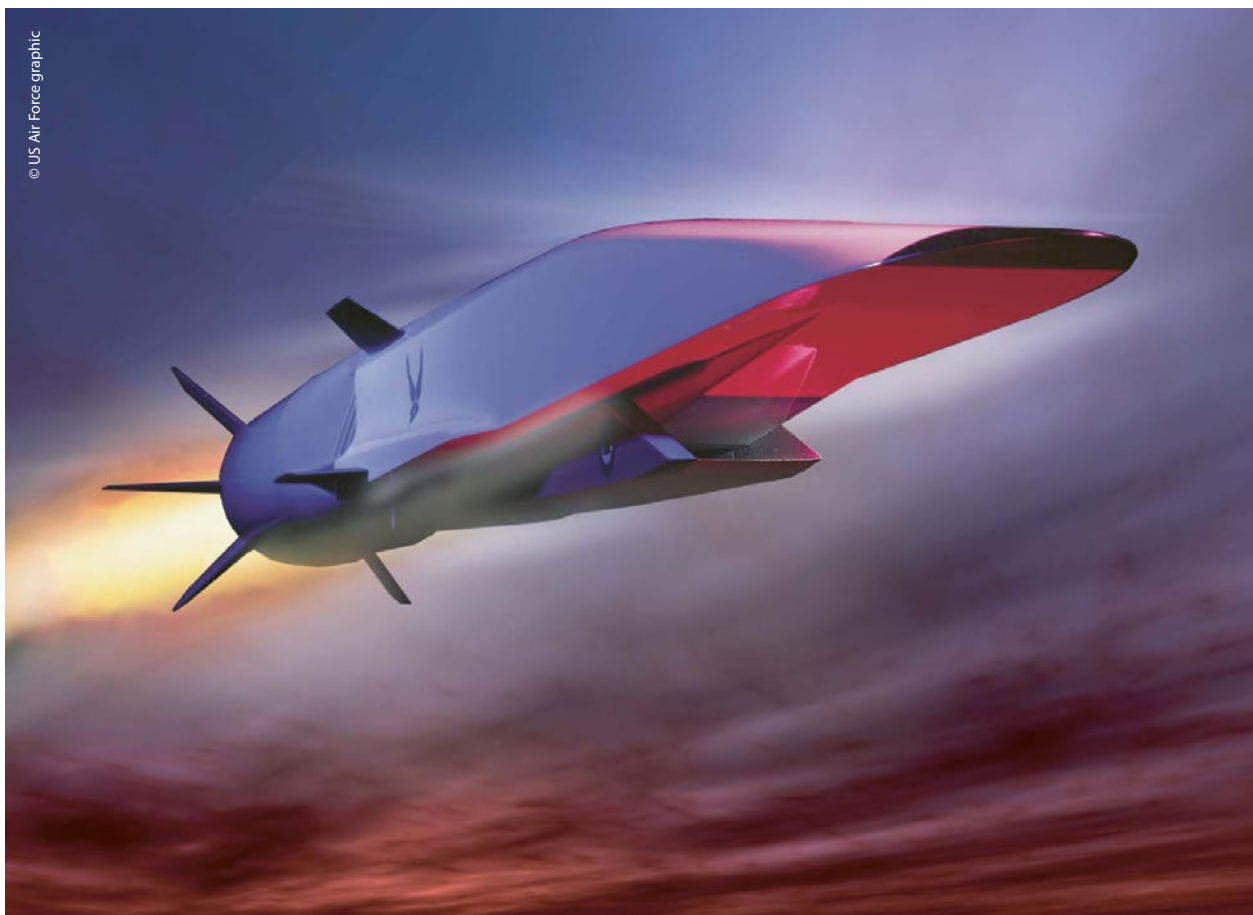


makes pre-emptive use of dual-capable aircraft for the nuclear mission highly unlikely, which means the most vulnerable nuclear capability is the least likely to see actual use in conflict. The addition of hypersonic weapons to the NATO nuclear umbrella or the British or French arsenals could give Russia pause to reconsider an escalation against NATO in retaliation for member-state support for Ukraine or because of further Russian territorial ambitions – buying restraint from a Russian attack on air bases with nuclear capable fighters.

**4. Ballistic and Cruise Missile Defences.** Improving missile defence systems make the success of ballistic or cruise missile strikes less certain.<sup>13</sup> Concerning ballistic missiles, the Cold War was marked by the dominance of offensive systems over defences. Improved technologies for short-, medium-, and intermediate-

range missile defences are demonstrating their utility in Ukraine and are improving. NATO's primary challenge is its almost complete lack of air and missile defence systems across Europe. Missile defences play a numbers game, but they must first be present, and they are insufficient in quantity in Europe.

Soviet leaders once feared American ballistic missile defences protecting US Intercontinental Ballistic Missile (ICBM) fields would give the US an opportunity for a first strike and be safe from counter-attack. The Soviets would therefore need to increase the ratio of attacking Soviet ICBMs from 2-to-1 to 4-to-1 to ensure a similar probability of success. The lack of missile defences across NATO today offers a degree of assurance to Russian leaders that the Alliance cannot effectively prevent an attack which increases Russian confidence in their ability to coerce and deter NATO.<sup>14</sup>



*Russia's development of nuclear-capable hypersonic glide weapons increases the uncertainty of deterrence.*



Advances in Western missile defence technologies, including space-based systems, undermine Russia's planned use of missile attacks against NATO by reducing their probability of success. Ukrainian and Israeli air and missile defence successes create a fundamental challenge for Russia because they offer lessons learned for improving NATO missile defences. However, there is the real challenge that the more successful and proliferated defences become, the greater Russia's desire to field systems that subvert or defeat them. This is particularly important as Russian President Vladimir Putin grows increasingly dependent on the credibility of his first-strike weapons as a deterrent against more substantive NATO intervention in Ukraine, for example.

**5. The Impact of Drones.** Russia's war against Ukraine only underscores the significance of this rapidly growing military capability, and the equalizing role drones

can play for the weaker side in a conflict. Ukraine's ability to strike Russian military targets hundreds of kilometres inside Russian territory with relatively primitive drones is a game changer with respect to shaping a future aggressor's willingness to go to war.<sup>15</sup> As drone technologies mature, rather than relying on 'first person view' aerial drones equipped with small explosives, which are playing an important role on the battlefield in Ukraine today, it is probable that a near future battlefield will see AI-enabled drones roam the battlefield looking for pre-programmed targets. No longer will they need a pilot in a nearby bunker flying them. Drone swarms may be used for large-scale attacks against military facilities or civilian infrastructure as well.<sup>16</sup> Drones may also take the place of expensive manned aircraft, which potentially benefits Russia more than NATO because Russia cannot match NATO traditional



*The MIM-104 Patriot Surface-Based Air Defence (SBAD) system is capable of engaging manned and unmanned aircraft, cruise missiles, and tactical ballistic missiles.*

airpower capability. The creative use of drones in ways not seen today, but derived from lessons learned in Ukraine, may either improve or reduce the effectiveness of stabilize or destabilize deterrence. It is too early to tell.

**6. Conventional Nuclear Integration.** Conventional war waged within a nuclear context is something NATO prepared for during the Cold War, and is a prospect that has regrettably returned. Now called ‘conventional-nuclear integration’, Russia’s ‘escalate to win’ strategy envisions a Russian nuclear response to a NATO conventional action.<sup>17</sup> Deterring Russia’s use of a small number of low-yield tactical nuclear weapons is now a real challenge for NATO planners. Real Russian fears of NATO’s overwhelming conventional superiority, particularly its airpower, could lead Russia to see such an ‘escalate to win’ strategy as its best option for avoiding conventional defeat and attrition of its already limited forces.<sup>18</sup> Ukraine’s request for eventual admission into the Alliance reinforces Russian paranoia, even if such discussions are aspirational.

**7. China’s Nuclear Breakout.** China’s nuclear breakout may encourage Russian aggression because President Putin sees American attention and capability split between NATO and Asia.<sup>19</sup> A Pentagon report to Congress has noted that China ‘will likely field a stockpile of about 1,500 warheads by its 2035 timeline’ and is improving its conventional and nuclear military capabilities across the board.<sup>20</sup> China’s emergence as a nuclear superpower is not a problem for the United States and its Asian allies alone. Europe cannot avoid a potential conflict in Asia because of the US’s membership in NATO.

Thus, NATO’s European member-states must both prepare for a conflict with Russia while also preparing to assist the United States in Asia. This will all take place within a context in which both Russia and China may resort to the use of nuclear weapons to halt Western efforts to intervene. Sizing up the Chinese nuclear arsenal and understanding China’s evolving thinking about nuclear use, which is moving away from a ‘no first use’ policy, is especially challenging.<sup>21</sup> Regrettably for Europe, geography is no longer a barrier to conflict with Asia.



© US DoD, Alejandro Pena

*Drones are playing an increasingly important and versatile role on the battlefield, though the implications for deterrence remain uncertain.*

**8. Domestic Politics.** Challenges to maintaining political unity within the borders of NATO member-states are growing. Modern democracies, including the United States and its European allies, face challenges within their own domestic polity that bear, at least indirectly, on their ability to sustain military power in support of deterrence. Within the United States, for example, domestic politics are more divisive than during the Cold War, when there was a common enemy. Across Europe, similar political divisions are tearing at the cohesion and common vision of a number of societies. With consensus-building more difficult than during the Cold War, agreeing on a national approach to addressing Russia and China is difficult.

When the citizens in a democracy no longer believe in democratic constitutionalism, especially among elites, it is difficult to engage citizens to make the necessary sacrifices to ensure militaries are effective deterrent forces. This is, of course, exactly what both Russia and China desire. However, as General Colin Powell, the former Chairman of the Joint Chiefs of Staff in the United States, once noted, no foreign power can defeat the United States; only Americans can do that. The same is true of NATO and its member-states.

## Conclusion

It is imperative for stable deterrence that Vladimir Putin and Xi Jinping never believe they can wedge the Alliance apart. A united NATO is far more capable



© US Air Force, Senior Airman Tessa B. Corrick

*B-52H Stratofortress from the 2<sup>nd</sup> Bomb Wing line up (Elephant Walk) on the runway as part of a readiness exercise at Barksdale Air Force Base, La., 14 October 2020.*

of effectively deterring across the spectrum of threats discussed above. Admittedly, the challenges are numerous and offer no ready solutions. However, the current sense of urgency generated by Russian aggression is a good start.

But this sense of urgency must be accompanied by real progress in matching Russian capabilities across the spectrum of conflict. It is no longer enough to protest to Russia that NATO means no harm. Instead, it is time to field a similar set of capabilities to those fielded by Russia, including hypersonic weapons, next-generation air and missile defences, space defences, cyber defences, and a full spectrum of nuclear capabilities. The Russians understand their own capabilities and the implications of their employment, which may lead Russia to exercise restraint. During the Cold War, it was NATO's fielding of the Ground Launched Cruise Missile (GLCM) and Pershing II in the mid-1980s that caused the Soviet Union to seek a reduction of nuclear forces and deterred Soviet aggression because the USSR had more to lose. The same can be true again if NATO takes a strong stance and fields the capabilities Russia respects.

A future crisis instigated by Russia is certain to include what the Soviets called 'dezinformatsia', or disinformation, as Russia seeks to convince the West to doubt what it knows to be true.<sup>22</sup> China will follow a similar game plan if conflict comes. Ensuring that NATO addresses the challenges discussed above, and is not caught unprepared can make such disinformation

efforts far less successful. In the end, NATO and its 32 member-states have a daunting task ahead of them. However, it is important to remember that the Alliance was successful in its first 75 years in preventing war and deterring Soviet/Russian aggression. The same is possible over the next 75 years. ●

1. See Mykhaylo Zabrodskiy, Jack Watling, Oleksandr V. Danylyuk, and Nick Reynolds, *Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February–July 2022* (London: Royal United Services Institute, 2022). Susan D'Agostino and François Diaz-Maurin, 'Putin Threatens Again: An Updated Timeline on Potential Nuclear Escalation of the Russia-Ukraine War', *Bulletin of the Atomic Scientist* (29 February, 2024), <https://thebulletin.org/2024/02/putin-threatens-again-an-updated-timeline-of-commentary-on-potential-nuclear-escalation-of-the-russia-ukraine-war/>.
2. Erica Loneragan and Mark Montgomery, 'What Is the Future of Cyber Deterrence?', *SAIS Review of International Affairs* 41, No. 2 (Summer–Fall 2021), pp. 61–73; and Forrest E. Morgan, *Deterrence and First-Strike Stability in Space: A Preliminary Assessment* (Santa Monica, CA: RAND Corporation, 2010), <https://www.rand.org/pubs/monographs/MG916.html>. Also available in print form.
3. David E. Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age* (New York: Crown Publishing, 2018); Andrew Futter, *Cyber Threats and Nuclear Weapons: New Questions for Command and Control, Security and Strategy* (London: Royal United Service Institute, 2016); and Erik Gartzke and Jon R. Lindsay, 'Thermonuclear Cyberwar', *Journal of Cybersecurity* 3, No. 1, (2017), pp. 37–48.
4. Grace B. Mueller, Benjamin Jensen, Brandon Valeriano, Ryan Maness, and Jose Macias, *Cyber Operations During the Russo-Ukrainian War* (Washington, D.C.: Center for Strategic and International Studies: 2023), pp. 1–3.
5. Jason Wolff, *The Department of Defense's Digital Logistics Are Under Attack* (Washington, D.C.: Brookings Institute, 2023).
6. Jaganath Sankaran, 'Russia's Anti-Satellite Weapons: An Asymmetric Response to US Aerospace Superiority', *Arms Control Today*, March 2022, <https://www.armscontrol.org/act/2022-03/features/russias-anti-satellite-weapons-asymmetric-response-us-aerospace-superiority>.
7. Micah Maidenberg and Drew FitzGerald, 'Elon Musk's SpaceX Courts Military with New Starshield Project', *Wall Street Journal*, 8 December, 2022, <https://www.wsj.com/articles/elon-musks-spacex-courts-military-with-new-starshield-project-11670511020>.
8. A taxonomy for classifying different kinds of RPOs in geosynchronous orbit and options for dealing with them are discussed in Kaitlyn Johnson, Thomas G. Roberts, and Brian Weedon, 'Mitigating Noncooperative RPOs in Geosynchronous Orbit', *Aether: A Journal of Strategic Airpower and Spacepower*, No. 4 (Winter, 2022), pp. 79–94.
9. Theresa Hitchens, 'To Protect and Maybe Defend: NRO, SPACECOM Ponder Commercial Satellite Defense Options', *Breaking Defense*, 1 September, 2022, <https://breakingdefense.com/2022/09/to-protect-and-maybe-defend-nro-spacecom-ponder-commercial-satellite-defense-options/>.

10. See Kelly Saylor, *Hypersonic Weapons: Background and Issues for Congress* (Washington, D.C.: Congressional Research Service, 2024).
11. Stephen J. Cimbala and Adam B. Lowther, 'Hypersonic Weapons and Nuclear Deterrence', *Comparative Strategy*, 41, No. 3 (2022), pp. 285–293. See also Stephen Reny, 'Nuclear-Armed Hypersonic Weapons and Nuclear Deterrence', *Strategic Studies Quarterly*, No. 4 (Winter 2020), pp. 47–76.
12. Adam Lowther and Curtis McGiffin, 'America Needs a Dead Hand', *War on the Rocks*, 19 October, 2019, <https://warontherocks.com/2019/08/america-needs-a-dead-hand/>.
13. Lynn Savage, 'US INDOPACOM's Integrated Air and Missile Defense Vision 2028', *Journal of Indo-Pacific Affairs* (January 2022), pp. 1–10.
14. Michael J. Mazarr, *Understanding Deterrence* (Santa Monica, CA: RAND Corp., 2018), pp. 4–7.
15. Kristen Thompson, 'How the Drone War in Ukraine Is Transforming Conflict', *Council on Foreign Relations*, 16 January, 2024, <https://www.cfr.org/article/how-drone-war-ukraine-transforming-conflict>.
16. Jonathan D. Bell, 'Countering Swarms: Strategic Considerations and Opportunities in Drone Warfare', *Joint Force Quarterly* 107, No. 4 (2022), pp. 4–14.
17. For a discussion of conventional nuclear integration, see Justin Anderson and James McCue, 'Deterring, Countering, and Defeating Conventional-Nuclear Integration', *Strategic Studies Quarterly* (Spring 2021), pp. 28–60. For a discussion of Russian nuclear doctrine, see Mark Schneider, *The Leaked Russian Nuclear Documents and Russian First Use of Nuclear Weapons* (Fairfax, VA: National Institute for Public Policy, 2024), pp. 5–7.
18. James R. McCue, Adam Lowther, and James Davis, 'A Tactical Nuclear Mindset: Deterring with Conventional Apples and Nuclear Oranges', *Aether: A Journal of Strategic Airpower & Spacepower* 2, No. 2 (2023), pp. 5–17.
19. Lindsey W. Ford and James Goldgeier, *Retooling America's Alliances to Manage the China Challenge* (Washington, D.C.: Brookings Institute, 2021).
20. Nancy A. Youssef, 'China's Swelling Nuclear Stockpile Makes It a Growing Rival to US, Pentagon Finds', *Wall Street Journal*, 29 November, 2022, <https://www.wsj.com/articles/chinas-swelling-nuclear-stockpile-makes-it-a-growing-rival-to-u-s-pentagon-finds-11669741977>. See also Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China* (Washington, D.C.: US Department of Defense, 2020); and Chris C. Demchak, 'China: Determined to Dominate Cyberspace and AI', *Bulletin of the Atomic Scientists*, no. 3 (2019), pp. 99–104.
21. For additional perspective, see Henry Sokolski, 'What Missile-driven Competition with China Will Look Like', *American Purpose*, 21 October, 2020, <https://nppolicy.org/what-missile-driven-competition-with-china-will-look-like-american-purpose/>.
22. Richard Shultz and Roy Goodson, *Dezinformatia: Active Measures in Soviet Strategy* (Washington, D.C.: Pergamom-Brassey's, 1984), pp. 53–100.

---

ABOUT THE AUTHORS

---



### Dr. Adam Lowther

Vice President of Research at the National Institute for Deterrence Studies

Adam Lowther is the Vice President of Research at the National Institute for Deterrence Studies. He has deep expertise in nuclear deterrence and the nuclear programs of Russia and China. He previously served as the Director of Strategic Deterrence Programs at the National Strategic Research Institute (NSRI) – serving US Strategic Command. Dr. Lowther was a Professor of Political Science at the Army's School of Advanced Military Studies (SAMS). Previously, he served as the founding director of the School of Advanced Nuclear Deterrence Studies (SANDS), Kirtland AFB. Dr. Lowther was a research professor at AFRI where he led and participated in studies directed by the Chief of Staff of the Air Force. Early in his career, Petty Officer Lowther served in the US Navy aboard the USS RAMAGE (DDG-61), at CINCUSNAVEUR – London, and with the Seabees (NMCB 17).



### Prof. Stephen J. Cimbala

Professor of Political Science,  
Pennsylvania State University

Stephen J. Cimbala is Distinguished Professor of Political Science, Penn State Brandywine, an American Studies faculty member and is the author of numerous books and articles in the fields of international security studies, defence policy, nuclear weapons and arms control, intelligence and other fields. He serves on the editorial boards of various professional journals, has consulted for a number of US government agencies and defence contractors, and is frequently quoted in the media on national security topics. Dr. Cimbala has taught courses in international relations, comparative politics, national security policy, US intelligence, political thought and other topics. He has team-taught courses in philosophy and communications with professors in those fields. He is a past recipient of Penn State's Eisenhower Award for excellence in teaching. Cimbala is a member of Penn State's graduate faculty.



# Technology and Trust

## *Interoperability for NATO's Multi-Domain Operations and US Combined Joint All Domain Command and Control*

By Commander Michael Posey, US Navy, US Army War College

By Colonel Jörg Stenzel, GE Army, US Army War College

---

“*Never fight unless you have to, never fight for long, and never fight alone.*”<sup>1</sup>

General Fox Conner,  
mentor of both Eisenhower and McArthur

---

As NATO considers how to conduct Multi-Domain Operations (MDO), the Alliance must consider interoperability across four dimensions: technical, procedural, informational, and human.<sup>2</sup> Although technical capability and interoperability receive much attention, network-building technology cannot function without the requisite human and procedural dimensions of interoperability. Human interoperability requires trust built through shared experiences, like exercises, ultimately

leading to decision advantage. This paper will describe and define interoperability, address why NATO needs a decision-making command and control network such as the US's Combined Joint All Domain Command and Control (CJADC2), discuss CJADC2 across the four dimensions of interoperability, and conclude with recommendations of how and why all dimensions of CJADC2 interoperability could be addressed.

### **Never Fight Alone**

This paper will focus on the implications of Conner's advice to never fight alone on NATO. Although the US fought nearly all of its major expeditionary conflicts, from the Boxer Rebellion to Afghanistan, with allies and partners, interoperability remains a challenge.<sup>3</sup>

In an alliance such as NATO, interoperability generally means all elements of military operations work together smoothly, which has been an area of effort since the organization's foundation.<sup>4</sup> On a strategic level, interoperability means the ability for Allies to act together coherently, effectively, and efficiently to achieve national and coalition objectives. On an operational level, NATO defines interoperability as enabling forces, units, and systems to operate together, allowing them to communicate and share common doctrine and procedures, along with each other's infrastructure and bases.<sup>5</sup> In other words, interoperability must encompass virtually every aspect of military activities and provide the option to 'plug in' allies and other partners. It is essential to ask why interoperability efforts still do not meet current requirements and what can be done to improve them, as interoperability challenges become more demanding.

## CJADC2 Enables MDO for NATO

As the character of war rapidly changes and threats in the security environment evolve, NATO's success in competition and armed conflict will depend upon optimizing effects from all domains. NATO developed and is refining the concept of MDO,<sup>6</sup> which enables joint NATO forces to orchestrate military activities across all five operating domains.<sup>7</sup> MDO, when realized, requires much greater data-driven agility than traditional joint operations. Leveraging data-advantage as an enabler, MDO synchronizes military effects with non-military operations, other national instruments of power, and the activities of NATO's partners and stakeholders. Because NATO's multifaceted concept of MDO requires synchronization, the command-and-control mechanism must be sophisticated, resilient, agile, and interoperable. The US's solution is CJADC2, which will be a comprehensive network of all command-and-control systems. The US Department of Defense first conceived of the evolving Joint All-Domain Command and Control (JADC2) network in 2019 and tasked the US Air Force to lead implementation for US forces.<sup>8</sup> Realizing the importance of integrating Allies and partner nations, the US renamed the concept the Combined Joint All-Domain Command and Control (CJADC2) in May 2023.<sup>9</sup>

Integrating Allies and partners into CJADC2 network makes sense.<sup>10</sup> A combined force is essential in competition or armed conflict against sophisticated adversaries such as the People's Republic of China or Russia. According to an old proverb, 'Who works alone adds, who works together multiplies.' This sentiment aptly captures the necessity for NATO to work collaboratively. However, interoperability challenges rise as alliances garner more partners and assets. Although the network of systems cannot be a panacea for NATO's challenges in competition and armed conflict, CJADC2 and its aspirational technology can be a solution to NATO's need for C2 interoperability.

Interoperability means much more than just connectivity. CJADC2 architects seek to facilitate decision advantage by providing the right decision-maker with useful information. Vice Admiral (ret.) Ann Rondeau describes decision advantage in military operations as 'the rapid discernment of trusted information for a decision-maker to act confidently – and first'.<sup>11</sup> Useful information means that common form data moves from a relevant sender to the correct receiver (i.e., a decision maker or other actor) in the proper format. Connectivity, therefore, is a vital first step to sharing useful information. CJADC2 designers strive to connect sensors and data systems from NATO forces in a cloud architecture that uses Artificial Intelligence (AI) or automation to link the optimal weapons system to each target. While ambitious, the concept of networking existing C2 systems is feasible, although progress remains piecemeal.<sup>12</sup> CJADC2 would link sensors, shooters, and decision-makers, to rapidly converge fires and then disperse for survival, much like the Uber ride-sharing application, where a machine learning algorithm optimizes the driver's fares, rider routes, and many other factors.<sup>13</sup> The most important takeaway is that CJADC2 will enable enhanced military decision-making; it is not a single product. Some aspects of CJADC2 will soon become operational, with others coming online in the next few years. Similarly, some NATO capabilities can integrate into the CJADC2 architecture sooner than others.

Robust interoperability is critical to implementing CJADC2 and can be described in many ways. US



© Gorodenkoff/Shutterstock.com

*Unity of effort will be needed to leverage disparate systems' data together autonomously in a Systems of Systems approach.*

Joint Publication 1-02 (2010) defines interoperability as 'the ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces, and to use the services so exchanged to **enable them to operate effectively** together'.<sup>14</sup> (*Emphasis ours.*)

Interoperability is the ability to provide military services from one nation to another. The end goal of CJADC2 is achieving decision advantage, where NATO forces make better decisions faster to achieve an operational advantage. CJADC2 will leverage human and AI decision-makers, often called human-machine teaming, and will favor either the human or automation depending on a bevy of factors related to a decision's context and authority level. Human-Machine Teaming (HMT) requires defined architectures and engineering that enable the timely exchange of appropriate information to facilitate both human and machine decision-making. Given the importance of decision advantage, the four interoperability dimensions of CJADC2 are worth examining.

### Technical Dimension of CJADC2 Interoperability

CJADC2 requires technical interoperability with NATO Allies' disparate systems to communicate with each other. Conceptually, a multinational, joint task force that achieves unity of effort can be understood as cooperation and collaboration among autonomously operating systems, a System of Systems (SoS). These SoS have four main characteristics: autonomy, belonging, connectivity, and heterogeneity.<sup>15</sup> The heterogeneity of SoS, meaning that constituent systems employ different technologies and software interfaces, creates challenges. Data standards (discussed later) and software are two key components that allow systems to 'plug in' to the network architecture.

Software must be backward compatible and able to translate to older systems in the field. Novel technology like multi-static arrays, which use several overlapping transmission and receiver sensor nodes across a battlespace, can increase situational awareness and

agility on the battlefield. If multi-static arrays become commonplace among NATO sensor systems, they will facilitate faster and more efficient targeting. For instance, compatible, multi-static radar networks will allow for more rapid, precise localization of objects – adversary or otherwise.<sup>16</sup> Similarly, multi-static sonar systems allow for speedier triangulation undersea.<sup>17</sup>

Therefore, systems must be acquired with technological interoperability built-in and ideally designed for quick removal and replacement to facilitate software and hardware upgrades. Further, electromagnetic compatibility must be a consideration when purchasing systems. When transmission capabilities and antennas of NATO sensor systems are designed with the same DNA (frequency, encryption, programming languages, and human interfaces), such multi-static sensing and communication have the potential to empower sensor-to-shooter interoperability and could aid MDO. Emerging technical solutions like Edge AI, which computes at each network node, can aid tools such as agile frequency hopping to ensure radio transmission can connect sensors, shooters, and decision-makers.<sup>18</sup> Getting these advanced technologies into the hands of warfighters requires considerable collaborative efforts in developing and purchasing enabling command and control systems. NATO must consider how it wishes to leverage the potential of AI, enabling computing in individual platforms and speeding up the OODA (Observe-Orient-Decide-Act) loop.<sup>19</sup> However, in so doing, AI data streams must be digestible by all AI-enabled platforms. These AI-capable platforms must also be technically interoperable with legacy NATO platforms to share ‘sensor-to-shooter’ computations. This means dynamically establishing interoperability between various heterogeneous cyber-physical systems, which is enormously challenging. Ideally, this should be solved by a common development of architecture, software data stacks, and open upgradeable system solutions within acquisition strategies.

Since its founding, NATO has been an accelerator for human interoperability through standardization and joint exercises. The yearly NATO Coalition Warrior Interoperability eXploration, eXperimentation, eXamination eXercise (CWIX) combines all four dimensions, focusing on human and technical interoperability.

This event is a testbed oriented on the requirements specified by Federated Mission Networking (FMN) Spirals. FMN is how affiliates come together to achieve a standard level of interoperability. NATO members have vastly different requirements, both in technology, operational principles and training. In a federation, one’s own networks and systems are maintained and coordinated under the umbrella of FMN. In a federated manner, NATO nations can coordinate actions together without giving up national independence. NATO, therefore, speaks of *day zero* interoperability. The likelihood of achieving day zero interoperability increases by using ‘spiral development’. Spirals, defined periods with a specified degree of interoperability, provide waypoints for FMN development in events like CWIX.

While FMN illustrates technological changes, how humans respond to differing technology matters and ultimately defines the level of human interoperability necessary with a machine. Despite creating advanced autonomous machines, humans must never give total control to the algorithms as we create automated systems.<sup>20</sup> In the context of connecting a massive, allied military architecture, this means NATO must adapt to the evolving relationships between human operators and automated machines.

### **Procedural Dimension of CJADC2 Interoperability**

Aligning language, processes, procedures, and products is a precondition to making the technological solutions work together seamlessly. The NATO Standardization Office (NSO) is responsible for developing common standards and ways of working together. This is mainly done through Standardization Agreements. The sheer number of such agreements – their official website lists 1149 – gives an idea of the challenge.

Despite the challenges, cross-domain solutions for sensing and targeting are necessary against a near-peer adversary. Developing the federated requirements and doctrinal procedures for air assets using cyberspace fires, maritime Intelligence, Surveillance, and Reconnaissance (ISR), or fires coming from the land domain requires coordinated doctrine and Tactics,



Techniques, and Procedures (TTP) by all services. One way to develop doctrine and TTP is through robust simulations and exercises.

---

**[...]** *‘Our shared values and experiences since 1949 continue to be one of our strengths, and human interoperability cannot be lost.’*

---

NATO’s simulations, exercises, and iterative design are exponentially more valuable when lessons are learned and procedures are written down. For instance, NATO’s Command and Control Simulation Systems Interoperation (C2SIM) demonstrates how to elevate operator proficiency of C2 software and procedures among nations, as new technologies emerge.

### Human Dimension of CJADC2 Interoperability

Human factors play a crucial role in achieving interoperability, which involves interaction between individuals, teams, and their technologies or systems. The human and procedural aspects of interoperability are closely linked. In strategic organizations like NATO, humans make choices and codify them in policies that increase interoperability. Central to interoperability efforts in the Alliance are the willingness and ability of leaders to communicate and collaborate. Interoperability is much more than the capability to exchange data; disparate human systems across nations and HQs must also be aligned.

Therefore, a common lexicon, common symbology, and procedures are just the beginning. Humans take data and assign meaning to it to make the information useful. Useful information can be applied to become knowledge and develop understanding. From this understanding of what one does alongside a fellow warfighter and what the fellow warfighter will do in turn, we begin to form innately human bonds of trust. Trust comes from serving together, drilling together, and putting your life into another service-member’s hands. This is why NATO must continuously train together.



© DC Studio/Shutterstock.com

*CJADC2 will require advances across multiple dimensions to be successful.*

### Information Dimension of CJADC2 Interoperability

The information dimension of interoperability refers to data integrity, standards, and conduits that carry and compile the data. Language, syntax, and transmission means are all part of the information dimension. The information dimension is essential because humans assign meaning to data in context and make decisions based on this information. Given the volume of information humans must digest in MDO, CJADC2 should employ computational aids. AI, particularly machine learning, can aid humans in making decisions.



© PeopleImages.com - Yuri A/Shutterstock.com

*In order for CJADC2 to succeed, there must be synergistic collaboration between the nations of NATO, as well as linkages between those militaries and their corresponding industries.*

There are three requirements to use machine learning: computing power, trained algorithms, and interoperable data.<sup>21</sup> AI programmers spend excessive time data wrangling to ensure data are interoperable.<sup>22</sup> NATO should continue to develop practical data standards for AI and machine learning applications. Data standards ensure that the format, lexicon, and measurements of different NATO platforms from various NATO nations share compatible data. When the data are wrangled (or groomed) before proceeding the AI tool is more likely to produce meaningful results. Neural networks examine many factors to classify data.<sup>23</sup> When the data are standardized, the algorithms can be trained through supervised learning to yield better predictive models, like those used by Uber.<sup>24</sup> In essence, without groomed data, machine learning functionality will be limited at best or woe-

fully incorrect at worst. The NSO could contribute meaningfully to data standardization efforts.<sup>25</sup> Similarly, NATO will need to develop a robust data repository where data can be shared. Additionally, programmers must think through how to best compartmentalize information in the cloud. For example, despite reducing operational effectiveness, some information may not be shared due to a NATO member's national caveats.<sup>26</sup> Therefore, cloud storage will require some data to go through 'gates' and other data to flow freely among Alliance platforms. Thinking through these restrictions requires a partnership between programmers and military experts who can technically and procedurally ensure the protection of information. As CJADC2 becomes operational, the importance of informational interoperability cannot be understated.



## CJADC2 Requires Technical and Human Interoperability

'Interoperability is often considered to be a desired but unattainable goal rather than a condition that can be quantified.'<sup>27</sup> One way to frame successful interoperability is to minimize missed opportunities. As CJADC2 begins to link networks, we should emphasize both the technological and human dimensions of interoperability.

As the character of war rapidly evolves, NATO nations must seek collaboration with each other and with their industries. If countries and their industries share algorithms, leverage standardized and translatable datasets, and compatible, upgradable equipment, NATO will benefit from technological and informational

interoperability efforts. The 'evolving construct' of CJADC2 has achieved its minimum viable capability, meaning that NATO could use CJADC2 and update it for the Alliance.<sup>28</sup> Likewise, NATO's FMN is proving that technical interoperability can happen. Beyond the information sharing that FMN portends, NATO must ensure that the right information, in the right format, gets to the right user to allow for decision advantage.<sup>29</sup> Technology alone as an enabler for MDO cannot be the solution. As NATO Allied Command Transformation *Strategic Foresight 2023* notes, 'Potential adversaries will also seek to erode NATO's technological edge by seeking dominance in non-traditional technological areas.'<sup>30</sup> Therefore, beyond technical interoperability, NATO forces must build resilience by integrating into the CJADC2 network through sound procedures and human aspects, such as education, training, and adopting a common lexicon. Doing so will forge trust, the 'secret sauce' of human interoperability.

As such, it is the human aspect that NATO must focus on. NATO members must continue to train together and think deeply together. Our shared values and experiences since 1949 continue to be one of our strengths, and human interoperability cannot be lost. Successful interoperability – synchronizing the Alliance's actions in time, space, purpose, and information that provides decision advantage – will prove critical to NATO, ensuring that MDO and the requisite CJADC2 architecture are not a series of buzzwords, but an emerging reality. ●

1. Gates, R., 'Reflections on Leadership', *Parameters*, vol. 40, no. 4, 2010, <https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=2553&context=parameters>, (accessed 4 May 2024).
2. NATO, 'Interoperability: Connecting Forces', *NATO*, 11 April 2023, [https://www.nato.int/cps/en/natohq/topics\\_84112.htm](https://www.nato.int/cps/en/natohq/topics_84112.htm), (accessed 2 May 2024).
3. Grobe, A., M., 'War in Afghanistan: What Has NATO Learned from 20 Years of Fighting?', *Christian Science Monitor*, <https://www.csmonitor.com/World/Europe/2021/0106/War-in-Afghanistan-What-has-NATO-learned-from-20-years-of-fighting>, (accessed 21 March 2024).
4. NATO, 'Founding Treaty', *NATO*, 2 September 2022, [https://www.nato.int/cps/en/natohq/topics\\_67656.htm](https://www.nato.int/cps/en/natohq/topics_67656.htm), (accessed 21 March 2024).
5. *Ibid.*, p. 1.
6. Milley, M., A., 'Strategic Inflection Point', *Joint Forces Quarterly*, vol. 110, no. 3, 2023, [https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-110/jfq-110\\_6-15\\_Milley.pdf](https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-110/jfq-110_6-15_Milley.pdf), (accessed 15 March 2024).
7. NATO, 'Multidomain Operations in NATO – Explained', *NATO*, 25 October 2023, <https://www.act.nato.int/article/mdo-in-nato-explained/>, (accessed 4 May 2024).
8. Hoehn, 'Joint All Domain Command and Control', *Congressional Research Services*, 21 January 2022, <https://crsreports.congress.gov/product/pdf/IF/IF11493>, (accessed 14 May 2024).
9. Jaspreet, G., 'Return of CJADC2: DoD Officially Moves Ahead with "Combined" JADC2 in a Rebrand Focusing on Partners', *Breaking Defense*, [web blog], 16 May 2023, <https://breakingdefense.com/2023/05/return-of-cjad2-dod-officially-moves-ahead-with-combined-jadc2-in-a-rebrand-focusing-on-partners/>, (accessed 19 May 2024).

10. Biden, J., 'National Security Strategy', *The White House*, October 2022, p. 22, <https://www.whitehouse.gov/wp-content/uploads/2022/11/8-November-Combined-PDF-for-Upload.pdf>.
11. Rondeau, A., 'Rebalancing the Science and Art of War for Decision Advantage', *Proceedings*, vol. 148, no. 8, August 2024, <https://www.usni.org/magazines/proceedings/2022/august/rebalancing-science-and-art-war-decision-advantage>, (accessed 18 May 2024).
12. Harper, J., 'Pentagon Eyeing "Bridging" Solutions for JADC2', *DefenseScoop* [web blog], 14 December 2023, <https://defensescoop.com/2023/12/14/pentagon-eyeing-bridging-solutions-for-jadc2/>, (accessed 18 May 2024).
13. Dobler, Y., 'Uber Knows You: How Data Optimizes Our Rides', *Digital Innovation and Transformation*, 4 October 2022, <https://d3.harvard.edu/platform-digit/submission/uber-knows-you-how-data-optimizes-our-rides/>, (accessed 26 May 2024).
14. Pemin, C., G., et al., 'Chasing Multinational Interoperability: Benefits, Objectives, and Strategies', *RAND Corporation*, 8 April 2020, [https://www.rand.org/pubs/research\\_reports/RR3068.html](https://www.rand.org/pubs/research_reports/RR3068.html), (accessed 28 May 2024).
15. Maier, M., W., 'Architecting principles for systems-of-systems', *Journal of the International Council on System. Engineering*, vol. 1, 1998, pp. 267–284.
16. Griffiths, H., and Farina, A., 'Multistatic and Networked Radar: Principles and Practice', *2021 IEEE Radar Conference Atlanta, GA*, 2021, pp. 1–5.
17. Coraluppi, S., et al., 'Wide-Area Multistatic Sonar Tracking', *2021 IEEE 24th International Conference on Information Fusion Sun City, South Africa*, 2021, pp. 1–8.
18. Yeung, T., 'What Is Edge AI and How Does It Work?', *NVIDIA* [web blog], 17 February 2022, <https://blogs.nvidia.com/blog/what-is-edge-ai/>, (accessed 25 May 2024).
19. Ibid.
20. Mindell, D., A., 'Our Robots Ourselves: Robotics and the Myth of Autonomy', Viking Press, 2015, p. 9.
21. Brown, S., 'Machine Learning, Explained', *MIT Sloan*, 2 May 2024, <https://mitsloan.mit.edu/ideas-made-to-matter/machine-learning-explained>, (accessed 2 June 2024).
22. Woodie, A., 'Data Prep Still Dominates Data Scientists' Time, Survey Finds', *Datanami*, 2020, <https://www.datanami.com/2020/07/06/data-prep-still-dominates-data-scientists-time-survey-finds/> (accessed 27 March 2024).
23. Hardesty, L., 'Explained: Neural Networks', *MIT News*, 14 April 2017, <https://news.mit.edu/2017/explained-neural-networks-deep-learning-0414>, (accessed 7 June 2024).
24. ProjectPro, 'How Uber Uses Data Science to Reinvent Transportation?', [web blog], 11 April 2024, <https://www.projectpro.io/article/how-uber-uses-data-science-to-reinvent-transportation/290>, (accessed 4 May 2024).
25. Hegykozi, V., 'Expanding Interoperability Integrating Interoperability Tools in Multinational Exercises', *Atlantic Forum*, 1 October 2023, <https://www.atlantic-forum.com/atlantica/expanding-interoperability-integrating-interoperability-tools-in-multinational-exercises>, (accessed 27 March 2024).
26. Saideman, S., M., and Auerswald, D., P., 'Comparing Caveats: Understanding the Sources of National Restrictions upon NATO's Mission in Afghanistan', *International Studies Quarterly*, vol. 56, 2012, pp. 67–84, <https://academic.oup.com/isq/article-abstract/56/1/67/1941598?redirectedFrom=fulltext>.
27. Grace Lewis, G., 'The Role of Standards in Cloud Computing Interoperability', *Carnegie Mellon Technical Note*, October 2012, The Role of Standards in Cloud-Computing Interoperability (cmu.edu).
28. Vincent, B., 'What's next for the New CJADC2 Minimum Viable Capability', *DefenseScoop* [web blog], 26 February 2024, <https://defensescoop.com/2024/02/26/dod-cdao-ai-cjad2-minimum-viable-capability/>, (accessed 14 May 2024).
29. *Federated Mission Networking – FMN*, 2021, [online video], 2021, [https://www.youtube.com/watch?v=\\_9FvEVS0YiM](https://www.youtube.com/watch?v=_9FvEVS0YiM), (accessed 16 May 2024).
30. NATO, 'Navigating the Future: Key Findings from Allied Command Transformation's 2023 Strategic Foresight Analysis', NATO Allied Command Transformation, 7 June 2024, <https://www.act.nato.int/article/navigating-the-future-2023-sfa/>, (accessed 22 June 2024).

---

#### ABOUT THE AUTHORS

---



#### Commander Michael Posey

Commander Michael Posey is an active-duty US Naval Flight Officer. He has served in various carrier-based flying assignments in the E-2C Hawkeye and F/A-18F Super Hornet. He has flown in combat in the US Central Command area of responsibility, served as a plans and exercises officer for the US 7<sup>th</sup> Fleet (Western Pacific) area of responsibility, and holds a subspecialty in Information Systems and Operations. He holds master's degrees from the University of Florida, Air University, and the US Army War College. He currently serves on the US Army War College faculty.



#### Colonel Jörg Stenzel

Colonel Jörg Stenzel is a German Army Armored officer. Before becoming a faculty member at the Department of Military Strategy, Planning, and Operations at the United States Army War College, he served at the German Joint Operations Command, the Ministry of Defense, commanded an Armored Battalion, was the Military Assistant to the German Chief of Army and Executive Officer of the Commander NATO Joint Force Command Brunssum. He was deployed 3 times in Afghanistan. He holds master's degrees in history, Business Administration, and Strategic Studies. He currently serves as the J3 of the German Homeland Defence Command.



# Non-Lethal Measures of Effectiveness in Targeting

By Mr Adam T. Jux, BA, Civilian Targeting Consultant

“Not everything that counts can be counted. Not everything that can be counted counts.”

William Bruce Cameron

## Introduction

In a world of rapid technological advances, specialists in non-lethal warfare face a persistent challenge: measuring the intangible effectiveness of non-lethal operations. Whereas lethal engagements, delivered through land, maritime, and air, often have visible and

measurable results, non-lethal effects may have outcomes that are obscured, delayed, or subjective in nature. It is crucial, therefore, to recognize the characteristics and challenges of non-lethal actions by first understanding the current assessment process and then proposing methods which may improve future analysis. Within NATO, there is an ongoing discussion regarding the definition of the terms ‘lethal/non-lethal’ versus ‘kinetic/non-kinetic’. So far, the term ‘lethal/non-lethal’ is used to referring to NATO targeting capabilities.<sup>1</sup> US doctrine, however, uses the term ‘kinetic/non-kinetic’ for capabilities and means, and the term ‘lethal/non-lethal’ for effects.<sup>2</sup> Although there are trade-offs between both framings of the issue, this article will use the NATO lexicon.

## Measuring Lethal and Non-Lethal Effects

Military combat performance is typically evaluated through Measures of Performance (MoPs) and Measures of Effectiveness (MoEs):

- 1. Measures of Performance (MoP):** Metrics used to determine the accomplishment of actions, answering the question, 'Are the actions being executed as planned?'
- 2. Measures of Effectiveness (MoE):** Metrics used to measure a resulting system state, answering the question, 'Did we achieve the intended effects within the planned timescale?'<sup>3</sup>

From a campaign assessment perspective, lethal effects are easier to quantify both in terms of MoPs and MoEs, as they offer tangible metrics, such as the number of tanks destroyed or the percentage of a facility's destruction. However, non-lethal options are often opaque and obfuscated by design. A non-lethal effect often requires extensive time to prepare, execute, and

evaluate; incorporating this constraint is particularly important when planning a cohesive Multi-Domain Operation (MDO). Furthermore, it may ultimately contribute to a lethal effect, which complicates MoP and MoE evaluation, as the final target may be degraded or destroyed. Thus, MoPs of non-lethal means may be nearly impossible to assess, whereas MoEs are more likely to be qualitative and may be difficult to attribute directly to the non-lethal effect, but assessment of both will almost certainly be delayed.

## Characteristics of Non-Lethal Targeting

Non-lethal targeting can be divided into three focus areas:

- 1. Lethal actions with second or third-order non-lethal effects:** This includes exploitation of lethal effects through a non-lethal medium such as strategic messaging following a strike, which requires detailed coordination to ensure complementary and non-detrimental effects.



*Disinformation – intentionally misleading, false, or biased information – is a potent tool that can persuade numerous influential individuals and the general public by undermining shared understanding and truth.*

**2. Pure non-lethal campaigns:** There are many examples of pure non-lethal campaigns. STRATCOM is one such example where there is a need for coordination among all targeting working groups to deconflict and ensure there are no detrimental effects through other campaign methods.

**3. Non-lethal actions complementing lethal actions:** For complex targets like Counter-A2AD, effects planned in all domains should come together and be complementary at the same time to achieve an effect.

Non-lethal targeting includes multiple disciplines with differing procedures and objectives. A selection of these may include:

**Strategic Communications (STRATCOM).**<sup>4</sup> Strategic communications encompass multiple elements of public diplomacy, political marketing, persuasion, international relations, military strategy, and many other approaches.

These areas can be subdivided into:

**1. Public Affairs (PA).** Engagement through the media to inform the public of policies, operations, military aims and objectives into a timely and accurate manner.

**2. Information Operations (IO).** Creating desired effects on the will, understanding, and capabilities of adversaries and other parties in support of operations, missions and objectives.

**3. Psychological Operations (PSYOPS).** Methods of communications directed at audiences to influence perceptions, attitudes, and behaviour, affecting the achievement of political and military objectives.

**4. Key Leader Engagement (KLE).** Communications and outreach efforts to influential individuals intended to promote awareness of and building understanding and support for policies, operations, and activities.

The assessment of STRATCOM effects can be both quantitative and qualitative, and it is often inferred by examining changing perceptions by way of social media chatter, the tone of media reports, political rhetoric, or trends in public opinion, movement, or preferences.

As a cognitive effect, STRATCOM is often divided between strategic long-term objectives and specifically targeted, short-term effects, which can then be fused within the normal targeting cycle. One important characteristic of STRATCOM is that its assessment cannot be judged based on a single report, impression, or observation, but rather, as an evaluation of trends over time. As such, this non-lethal effect is not easily replicated within exercise domains. However, STRATCOM is highly conducive to future Artificial Intelligence (AI)-driven planning, execution, and assessment. Current AI technology already includes regular automated interactions between businesses and consumers, and regularly shapes social media interactions, quantifies audience engagement, and analyses diverse feedback loops,<sup>5</sup> however these commercial applications contrast with military effects due to the availability of measurable metrics.

**Civil and Military Cooperation (CIMIC).**<sup>6</sup> The military recognizes that not all crises and conflicts require lethal military capabilities, and that crises are often complex and interlinked, requiring whole-of-government subject matter expertise on issues such as ethnic, religious, ideological, and socioeconomic fields. Oversight of these crises therefore requires CIMIC to synchronize management of challenging social, economic, and environmental sectors.

Cooperation and coordination between military forces and local or indigenous authorities is an important and commonly overlooked non-lethal effect, as it may yield more influence than official heads of state at distant capital cities and may enable the achievement of military goals. The importance of shared understanding through cooperative working, liaison, and education needs to be understood so collaborative work, based upon mutual trust and a willingness to cooperate, benefits both sides.

CIMIC provides a crucial non-lethal mechanism for commanders, since the level of human interaction between civil and military personnel facilitates the continual assessment of both the desired interactions (MoPs) and actual results (MoEs). However, this effect must be cultivated continually, and requires extensive and continual investment and foresight to be effective.

**Cyber Operations.** The cyber domain is relatively new compared to traditional land, maritime and air domains, but it is equally as important and perhaps even more contested, particularly in peacetime. While effects in the cyber domain can be lethal, it is more commonly associated with non-lethal operations. Furthermore, cyber operations are an escalating threat; NATO, which until recently did not have its own cyber capabilities, now faces hundreds of hacking attempts every month.<sup>7</sup> The NATO Cyber Operations Centre (CyOC) in Mons, Belgium recognizes this ever-growing threat from states and non-state actors, hackers, and hacktivists, and can execute operations in response to attacks.<sup>8</sup> There is a perception that cyber acts take place in isolated incidents. However, the Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA), a conglomeration of nations overseen by the CyOC, increasingly understands that cyber incidents represent broad, comprehensive campaigns from both state and non-state actors.<sup>9</sup>

Operational-level JTF commanders own the targeting process and decide which effects to deliver on a given target. However, they will not be able to task any nation to provide such effect. As opposed to conventional means and capabilities, command of national cyber effects will not be ceded to an operational-level commander, as opposed to other conventional capabilities, which upon appropriate transfer of authority will fall under the NATO commander's command and control. Although an effect may be delivered by a nation upon an operational-level commander's request, the nation delivering it will do so on an 'I will tell you what I can do, but not how' basis; here you can see the significance of 'sovereign' in the SCEPVA construct.<sup>10</sup> It is clearly difficult to collaborate when elements are close hold. Notwithstanding long and persistent access to requirements to target networks, many planners can be unaware of available capabilities or what to ask for in order to form a multi-spectral approach to targeting.

The most important thing about NATO's use of cyber capabilities, therefore, is the need to achieve interoperability, starting with an understanding of capabilities to integrate effects into planning cycles. This begins with education in effects and dissemination of SMEs at different levels of command to effectively support and integrate those effects to best fit.

**Electronic Warfare (EW).** Electronic warfare has been around for well over a century. The first credited use of EW was well documented by Winston Churchill during the Boer War (1899–1902). At the time, the British Army used searchlights to bounce morse code off clouds. This was spotted by The Boers who then tried to jam the signals by using one of their own searchlights in the same fashion.<sup>11</sup>

Today, while EW techniques have evolved considerably, the goal remains largely unchanged – to disrupt or destroy an enemy's ability to observe, orient, decide, and act on the battlefield by degrading, neutralizing, or destroying its combat capabilities. Denial of the electromagnetic spectrum gives a considerable advantage when integrated into a layered, multi-domain attack. Further, the evolution and integration of Cyber Electro Magnetic Activities (CEMA)<sup>12</sup> sees an overlap of two distinct, but complementary disciplines; one primarily concentrated on software and data (cyber), while the other is focused on hardware and signals (EW).<sup>13</sup> Primarily, EW activities are leveraged to seize, retain, and exploit an advantage over adversaries and enemies in both cyberspace and the electromagnetic spectrum, while simultaneously denying and degrading adversary and enemy use of the same and protecting the mission command system.<sup>14</sup>

It should be remembered that member nations provide specialist support to enhance NATO's capability, which can then lead to problems associated with national security. If member nations provide specialist capabilities, then it is likely that these are sensitive in nature, would not be for public consumption, and would likely need to be kept in a 'grey zone' in terms of deniability and attribution. Thus, nations typically maintain full ownership of those capabilities. This is normal, as opposed to conventional military equipment from member nations that operates under a NATO command structure.

As with other types of non-lethal effects, a dilemma still exists in measuring how well an offensive EW plan has worked. To this end, several MoPs and MoEs are available, including quantifiable parameters such as detecting an adversary's alternative radio frequency, to more subjective parameters, such as the use of electronic





deception to confuse an enemy's Intelligence, Surveillance, and Reconnaissance (ISR) systems. In a recent example, Russia has used the Orlan-10 UAV to insert propaganda SMS messages directly to Ukrainian soldiers by impersonating cell towers and hijacking communications. UAVs, and other platforms, can easily be modified to achieve similar techniques and results, but measuring success will continue to challenge post-targeting assessment due to lagging indicators of effectiveness, such as monitoring defections, changes in patterns of life, and unexpected troop movements in response to propaganda, to name a few examples.<sup>15</sup>

### **Non-Lethal Considerations**

As previously discussed, lethal engagements are often conducive to post-strike analysis, permitting Bomb Hit Analysis (BHA) and Battle Damage Assessment (BDA). However, when targeting cognitive elements, the results can take longer to achieve, and the effects may not always be visible or easily distinguished. Examples of such cognitive elements may be changing a mindset, influencing a population, or forcing a change of posture. General challenges in understanding how to complement effects in those specialist non-lethal fields results in planners not always knowing what effects to ask for and enunciates the difficulty of marrying actions to achieve a synchronized multi-spectrum effect.

All HQs tend to have specialists in non-lethal fields who are integrated into a joint effects branch, but not all specialties are represented at every command echelon. It is imperative, with such long planning times for effects, that all HQs invest in specialist non-lethal fields at all levels of their command structures.

It is reasonable for a Commander to expect feedback regarding non-lethal campaigning, but effects should be expected through broader explanations, as measures

cannot be as exact as a number of destroyed tanks following a strike. Have piracy operations stopped within a specific region? Has NATO won support from a host nation through our outreach programmes? Has Nation 'X' stopped supporting and led to more pressure being brought to bear against antagonist Nation 'Y'? These are all reasonable questions for a commander to ask regarding non-lethal campaign development.

It is expected that many answers would be drawn from trends over time, but favourable situations can be exploited in real-time for further gains, and this is the fusion of effects within an MDO construct. A host nation's piracy problem may be influenced through aggressive patrolling, strategic messaging regarding presence of deterring vessels, or cooperation to train and embolden that host nation to be self-sufficient in the future, as well as media campaigns showing NATO as a force for good and the good work of the nation in question. A full-spectrum approach to a problem, but one that can be exploited by a strike against a piracy stronghold with follow-on messaging.

'Measuring Effectiveness in the Information Environment' highlighted where planners of non-lethal actions should have an expectation of second or third order effects before achieving goals.<sup>16</sup> Each effect results in corresponding reactions in a complex, tiered set of causes and effects that need to be interpreted so as to assess the overall impact. An example of this would be effects resulting from an attack against enemy information systems (first order), setting out to achieve

an effect on information and information flow (second order), to seek to achieve an impact on an enemy Commander's decision-making (third order and the intended target), requiring an inductive analysis of intelligence reporting and assessments.

However, not every situation requires an MDO solution, but better education and understanding of multi-domain effects will improve the utilization of non-lethal actions and result in a vast array of potential options to Commanders. As member states embrace the MDO concept, the Alliance's integration at the strategic and operational levels should significantly improve regarding targeting as old and varied Tactics, Techniques and Procedures (TTPs) are replaced.

## Multi-Domain Considerations

While the term has been around for a several years, MDO is a NATO operations concept where synchronization and collaboration between the military domains and the other Instruments of Power (IoP) create effects in the physical, cognitive and virtual dimensions. Whereas the term Joint is commonly used within current command structures to describe inter-service deconfliction and teamwork, MDO promotes service-agnostic, domain-oriented coordination, including both military and non-military stakeholders, which is the key differentiation between the two terms.<sup>17</sup> The varied complexities of non-lethal assessment are enunciated further through not only coordination with other domains, but finding a cohesion of effects amongst non-military stakeholders, including political domains, economic domains, Non-Governmental Organizations (NGOs), etc. The list is

not exhaustive, but whilst it might seem easy to control the flow of information within a military context, the same cannot be said within non-military organizations and decision timelines.

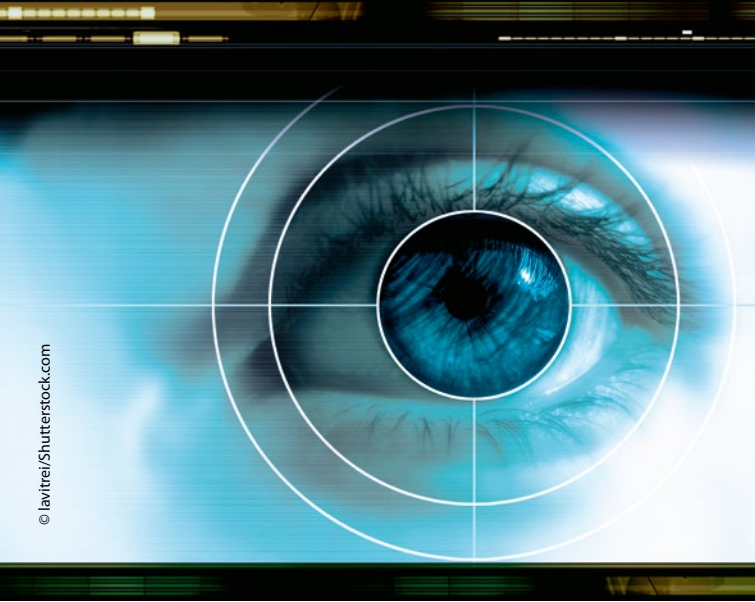
Examples of non-military non-lethal targeting might include sanctions, seizure of assets, etc. Clearly, from a military perspective, NATO would not wish to undermine a member nation's government by having a lethal effect against assets that would otherwise be seized in order to bring pressure against the owner and maintain a non-escalatory posture. How should those two actions be deconflicted or synchronized?

## Recommendations

Having considered the challenges and considerations pertaining to the evaluation of non-lethal effects, we propose three overall recommendations:

- 1. Review Non-Lethal Targeting Education.** Education is key for integration and understanding of non-lethal effects. Current NATO targeting training does not cover all specialist non-lethal fields and national assessments have documented this as an area that is lacking.<sup>18</sup> It is common for planners and leadership to underutilize or undervalue speciality fields due to a lack of familiarity, especially in terms of their time requirements and risk analysis.
- 2. Adopt MDO as concept and doctrine.** MDO are not required for every target but will improve understanding across the force. Establishing a liaison element or representation at the strategic level in order to deconflict non-military targeting and complement non-NATO actions should be considered and be understandable to planners within the NATO command structure through doctrine.
- 3. Invest in computer-aided analysis tools.** Training within the cognitive space should consider the benefits of including AI-generated models to assist with assessment and MoE.





© lavitrei/Shutterstock.com

## Conclusion

Advances in battlefield C2, the proliferation of advanced unmanned systems, and the proliferation of EW capabilities among state and non-state actors, makes it critical that commanders understand and maximize their own non-lethal capabilities. While non-lethal targeting is difficult to quantify, commanders have several tools available to maximize the planning, execution, and evaluation of non-lethal effects in the battlespace. First, they must educate themselves and their service members concerning the capabilities and limitations of non-lethal effects. Second,

they must demand deeper and more thorough integration across domains and services. Finally, they must promote and utilize emerging technologies which promise to reduce planning, execution, and analysis timelines. By understanding the importance of non-lethal effects, managing expectations, and pursuing new processes and tools, they will expand their warfighting tool chest for tomorrow's conflict. ●

1. [https://assets.publishing.service.gov.uk/media/618e7da28fa8f5037faa03f/AJP-3.9\\_EDB\\_V1\\_E.pdf](https://assets.publishing.service.gov.uk/media/618e7da28fa8f5037faa03f/AJP-3.9_EDB_V1_E.pdf)
2. [https://www.doctrine.af.mil/Portals/61/documents/AFDP\\_3-60/3-60-Summary-of-Key-Changes.pdf](https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-60/3-60-Summary-of-Key-Changes.pdf)
3. Definitions – CIMIC Handbook (cimic-coe.org).
4. StratCom | NATO Strategic Communications Centre of Excellence Riga, Latvia (stratcomcoe.org).
5. <https://www.researchgate.net/publication/379299506>
6. NATO and a comprehensive approach – CIMIC Handbook (cimic-coe.org).
7. NATO cyber command to be fully operational in 2023 | Reuters.
8. Ibid, 5.
9. Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA) – Cyber Defense Magazine.
10. Ibid, 7.
11. Churchill, W. S. (1900) London to Ladysmith via Pretoria. London. Longmans, Green, and Co.
12. Cyber Electro Magnetic Activities (CEMA) – EMSOPEDIA.
13. Blurring the Lines: The Overlap Between Cyber and Electronic Warfare (jedonline.com).
14. <https://securityanddefence.pl/pdf-103299-36215?filename=Electronic%20warfare%20in.pdf>
15. SAIC | Why Integrated Electronic-Cyber Warfare Is Crucial.
16. [https://jpsc.ndu.edu/Portals/72/Documents/JC2IOS/Additional\\_Reading/3F\\_Measures\\_of\\_Effectiveness\\_In\\_the\\_Information\\_Environment.pdf](https://jpsc.ndu.edu/Portals/72/Documents/JC2IOS/Additional_Reading/3F_Measures_of_Effectiveness_In_the_Information_Environment.pdf)
17. Multi-Domain Operations in NATO – Explained – NATO's ACT.
18. Integrating Lethal and Nonlethal Effects > Air Land Sea Space Application (ALSSA) Center > News (alsa.mil).

---

### ABOUT THE AUTHOR

---



### Mr Adam T. Jux

Civilian Targeting Consultant

Mr Adam T. Jux is a retired Royal Air Force Officer who served in the Royal Australian Air Force and the Australian Army over his 27 years of military experience. He is a qualified targeteer and has worked in the discipline for the last 14 years, including on operations. He has instructed in targeting and collateral damage estimation and has mentored targeting at the Joint and Component levels. He has

published a number of articles and contributed to white paper research regarding targeting in general and its interaction with intelligence and other disciplines, and is an advocate for targeting development and doctrine. He is currently working as a civilian targeting consultant for NATO's Joint Warfare Centre in Stavanger, Norway, under contract for Calian Europe AS.



Joint Air & Space Power  
Conference

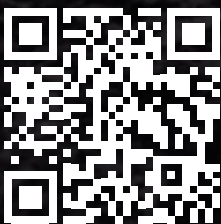
20  
24



# Challenges and Opportunities for Air and Space Power in an Evolving Security Environment

SAVE THE DATE

8–10 October 2024  
Essen, Germany



[www.japcc.org/conference](http://www.japcc.org/conference)

Joint Air Power  
Competence Centre



# The Joint Air and Space Power Think Tank Forum

## *Adapting to the Evolving Landscape of Modern Warfare*

The 11<sup>th</sup> annual Joint Air and Space Power Think Tank Forum (TTF) in 2024 stood out for several reasons. Notably, it marked the first time that the event was jointly organized by the JAPCC and Headquarters Allied Air Command (HQ AIRCOM). However, what truly made this year's TTF memorable was the diverse participation of individuals not only from national entities, but also from NATO and international organizations. Over sixty distinguished attendees gathered for this significant event.

Taking place in Ramstein Air Base from 13 to 14 March 2024, the forum was hosted by HQ AIRCOM and

brought together representatives from 31 exceptional entities, particularly national Air Warfare Centres (AWC). Chaired by Deputy Commander, AIRCOM, Air Marshal Johnny Stringer, and JAPCC Assistant Director Air Commodore Paul Herber, the forum introduced five multinational syndicate working groups to address pre-identified challenges such as Close Air Support/Air-Land Integration, Integrated Air and Missile Defence, Force Protection, Agile Combat Employment, and Air-Maritime Integration. The syndicate leaders from JAPCC and AIRCOM meticulously prepared these group discussions.



*This year's Think Tank Forum was unique in that it was the first time that it was jointly led by the JAPCC and HQ AIRCOM.*

This year's TTF was structured into two parts: the participating agencies shared their Programmes of Work (POWs) and an innovative segment featuring active syndicate work. The initial phase allowed participants to exchange information about major projects in their respective POWs, while the syndicates primarily revolved around AIRCOM's five priorities. The meeting served as a valuable platform for offering innovative, timely advice and subject matter expertise to address the challenges of modern warfare. Through syndicate discussions, it became evident that Alliance capabilities must be effective, interoperable, and integrated across all domains to support Multi-Domain Operations and achieve multi-domain effects.

It was widely agreed at the TTF that opportunities for interaction with others are crucial. These interactions promote cooperation, enhancing our ability to adapt to future military operations and maintain a competitive edge in warfare.

At the event, findings and developments from syndicates focusing on AIRCOM priorities and mutual concerns were compiled into fact sheets for each syndicate and distributed to participants. This initiative aims to integrate insights gained during the event into current and future projects. The event served as a starting point for work that must be carried out by nations and entities to address capability gaps and shortcomings, requiring a multinational and aligned approach to enhance Alliance readiness.

The JAPCC and HQ AIRCOM extend their sincere gratitude to all participants from various esteemed organizations for their attendance and valuable contributions to the event. These organizations include the Allied Rapid Reaction Corps, Allied Maritime Command, Belgian Air Force, Combined Air Operations Centre Torrejon, Combined Air Operations Centre Uedem, Competence Centre SBAMD, Centre d'Expertise Aérienne Militaire, Czech University of Defence, Deployable Air Command and Control Centre, Freeman Air and Space Institute Kings College London, German Air Force Forces Command – AWC Luftwaffe, German Air Operations Command, HAF General Staff – Operations Directorate, IAMD Centre of Excellence, Italian Air Force, Italian Air Warfare Centre, Military Academy of Lithuania, Naval Striking and Support Forces NATO, Netherlands Defence Academy, Polish Air Force Inspectorate, Romanian Air Component Command, Royal Danish Defence College, Royal Netherlands Air Force HQ, Spanish Air & Space Force, Swedish Defence University, Turkish Air and Space Development Centre, UK Air and Space Warfare Centre, USAFE-AFAFRICA, and USAFE-AFAFRICA Warfare Center.

We are excited about the prospect of further collaboration with these organizations at the next event planned for March 2025.

Additional Air Warfare Centres and similar entities interested in attending should contact us at: [contact@japcc.org](mailto:contact@japcc.org)

# Spotlight on Success

## *JAPCC Showcases its Achievements at the 2024 NATO COE Marketplace*

The Joint Air Power Competence Centre (JAPCC) made a strong impression at the NATO Centre of Excellence (COE) Marketplace, which took place at NATO Headquarters in Brussels from 22–23 May 2024. Air Commodore Paul Herber, the Assistant Director of the JAPCC, was accompanied by three Subject Matter Experts from the Combat Air and C5ISR & Space branches. Together, they highlighted JAPCC's significant contributions and ongoing activities, solidifying its presence among the 30 NATO accredited Centres of Excellence.

The biennial event united all COEs, NATO Headquarters staff, NATO Allied Command Transformation (ACT) personnel, and various other stakeholders to enhance collaboration and showcase the extensive expertise within the Alliance. Rear Admiral Placido Torresi, Deputy Chief of Staff Joint Force Development (NATO ACT), highlighted the vital role of COEs, especially as NATO transitions toward Multi-Domain Operations (MDO). He commended the COEs for their essential support in navigating the complex challenges that lie ahead.

During the marketplace, the JAPCC engaged with other COEs, NATO HQ staff, partner nations, and numerous visitors in the lively atrium. These interactions were crucial in promoting JAPCC's recent achievements, establishing partnerships, and offering insights into its ongoing projects. The JAPCC team participated in meaningful discussions, sharing examples of their work in areas such as the Warfare Development Agenda, MDO, artificial intelligence, machine learning, Unmanned Aerial Systems (UAS), and recent JAPCC Journal editions.

The JAPCC stand attracted significant attention at the COE Marketplace 2024, as the team distributed a plethora of informative printed publications material. These materials provided in-depth insights into JAPCC's various initiatives and the invaluable contributions it makes to NATO and its member nations. The outreach



*COE Marketplace Brussels (left to right): Air Commodore Paul Herber, the Assistant Director of the JAPCC, discusses the JAPCC's latest projects and publication releases with Mr Robert Weaver, the acting Assistant Secretary General, and Rear Admiral Placido Torresi, the Allied Command Transformation Deputy Chief of Staff for Joint Force Development.*

efforts were met with enthusiasm, as many attendees expressed a strong interest in JAPCC's expertise and the practical applications of their research and concept development. Notably, Robert Weaver, Acting Assistant Secretary General – Defence Investment, commended the exceptional work of the JAPCC.

Lieutenant Colonel André Haider showcased his work on the UAS concept, while Lieutenant Colonel Chochtoulas and Captain Stensberg emphasized how the diverse and specialized personnel of a COE like the JAPCC can deliver asymmetric enhancements to NATO. All the SMEs' participation underscored JAPCC's unwavering commitment to supporting NATO's strategic objectives through collaboration and knowledge sharing.

In summary, JAPCC's participation in the NATO COE Marketplace 2024 exemplified its steadfast dedication to advancing NATO's mission. Through active engagement and expertise, the JAPCC continues to play a pivotal role in shaping the future of NATO's strategic and operational landscape. ●





# 2024 SC/SRC Meetings with Sponsoring Nations

## *Realigning JAPCC Priorities through Collaborative Efforts*

The 2024 Joint Air Power Competence Centre (JAPCC) Steering Committee/Senior Resource Committee (SC/SRC) meetings took place in Kalkar, Germany from 17–19 June 2024. The primary objective of the SC meeting is to provide Sponsoring Nations with updates on the JAPCC Programme of Work (POW) and progress of the JAPCC's development. Meanwhile, the SRC meeting aimed to ensure that the activities of the JAPCC were in line with the allocation of resources.

### Steering Committee

The JAPCC continues to provide a significant return on investment for our nations by serving as a catalyst for NATO's improvement and transformation. The Committee has constructively discussed the issues and direction that the JAPCC must pursue in support of advancing NATO's interoperability as an Air and Space Force.

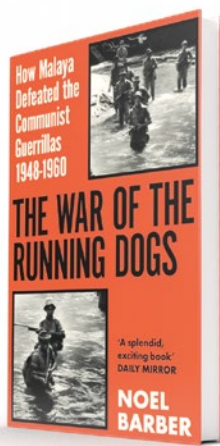
Chaired by Lieutenant General Thorsten Poschwatta, the recent meeting underscored the crucial role of the SC in shaping the future trajectory of the JAPCC. During the meeting, the Committee successfully addressed and closed all action items from 2023. Additionally, the SC thoroughly discussed key topics such as the internal survey, manning, reaccreditation by ACT, Annual Report, Areas of Interest and Focus Areas,

JAPCC Northstar Survey of Sponsoring Nations, publications, engagement and outreach, COE Cluster Meetings, JAPCC events, the addition of a C-UAS Cell, TÜ Exchange Request, and renaming the C4ISR & Space Branch to C5ISR & Space.

### Senior Resource Committee

Our goal at the JAPCC is to maximize our resources to provide unparalleled support to our member nations and NATO as a whole. Although significantly short on staff, the relevance of the JAPCC is increasing day by day. This is evident through the positive reception of our publications such as the JAPCC Journal and White Papers, the high-profile attendance at our annual JAPCC Conference, and the significant increase in Requests for Support we have received in recent years. These factors demonstrate the trust and confidence placed in the JAPCC.

During the meeting led by Brigadier General Radmann, all action items from the 2023 SRC were reviewed and closed, with completed tasks and ongoing concerns being highlighted. SRC members also addressed in detail the key topics of the SC meeting but from the resourcing perspective, and discussed the JAPCC budget for fiscal year 2025. ●



## ‘The War of the Running Dogs – Malaya 1948–1960’

With very little literature on the Malayan Insurgency (1948–1960), this book is one of the most cited examples of Counter-Insurgency (COIN) success. Such little knowledge of the conflict is surprising considering the geo-strategic importance of Singapore at the time, and the concurrent Korean and Indochina Wars. The civil authority’s insistence on leading the crisis response, rather than the military (as it was a ‘war of ideologies’), meant the military had no control over operations. The counter-insurgency forces, supported by Britain, were a mixture of planters and their

families on rubber estates, policemen, and civil powers against a ruthless enemy in a prolonged COIN war. An Information Operations response led to whole villages being relocated and provided with resources such as arable land, western medicine, and education to combat communism. The use of truthful propaganda by STRATCOM fostered civilian allegiance and prompted many terrorists to defect and be rehabilitated into law-abiding citizens. British Psyops Teams air-dropped ‘Safe Passes’ into the jungle, offering good treatment, food, and medicine, leading to insurgents becoming double agents and whole units surrendering.

Though not without controversy, it shows a British approach to COIN that succeeded where, at the time, the French (Indochina) and later US (Vietnam) failed to halt the spread of communism. In the end, Malaya became an independent nation, but on its own terms, neither British nor Chinese. ●

**By Noel Barber, Weidenfeld and Nicolson**

Reviewed by: Mr Adam T. Jux, Civilian, JAPCC



## ‘Boyd – The Fighter Pilot Who Changed the Art of War’

John Boyd is a name that is most often associated with the OODA loop. However, Colonel Boyd’s story involves many more successes, hurdles, and complexities throughout his career that many military members may not be aware of. Robert Coram’s biography of Boyd’s life clearly showcases the triumphs and difficulties of Boyd’s life, ultimately leading him to be one of the most well-known US Air Force pioneers never to

make General Officer. Boyd was both brilliant and confrontational, known for challenging the military establishment and pushing for innovations that revolutionized combat both in the air and on land. His development of the Energy-Manoeuvrability Theory which redefined fighter tactics, his involvement in designing the F-15 and F-16, and inspiring the US Marine Corps’ Manoeuvre Warfare doctrine are testaments to his lasting influence that Coram accurately depicts. This book explores Boyd’s struggles with Pentagon politics and his unwavering commitment to his principles, despite the personal and professional costs. Coram’s depiction of Boyd as a complex character offers valuable lessons on military strategy and leadership that any officer looking to grow professionally should consider reading. Boyd’s life is inspiring despite sadness and setbacks, revealing the importance of staying true to one’s convictions in the face of adversity. ●

**By Robert Coram, Back Bay Books, 2004**

Reviewed by: Captain Lucas Stensberg, US SF, JAPCC



# COMBAT-PROVEN

## IRIS-T SLM

Tactical interoperability meets strategic agility:  
IRIS-T SLM protects urban areas, critical infrastructures  
and military formations from airborne threats.



**Protector RG Mk1**



**Gambit Series**

# POWERING RPA INNOVATION FOR THE WORLD'S TOUGHEST MISSIONS

We deliver remotely piloted aircraft innovation powered by experience, ingenuity, and performance — backed by world-class partners.

That means unmatched pole-to-pole strategic ISR from the multi-mission, long-endurance MQ-9B. For short takeoff and landing in the most austere environments, deploy our groundbreaking MQ-9B STOL. And for the best all-domain awareness deep within the battlespace, look to our jet-powered Gambit Series combat aircraft.

These next-gen solutions deliver affordability at scale for any mission anywhere. And they're ready today.



**MQ-9B STOL**



Scan to learn more

©2024 GENERAL ATOMICS  
AERONAUTICAL SYSTEMS, INC.



Enabling Information Dominance

**GENERAL ATOMICS**  
AERONAUTICAL