IAMD CoE's JOURNAL

Vol. 3 | December 2024
iamd-coe.org

Table of Contents

04 EDITORIAL

Brig. General (OF-6)
Nikolaos MAKRIGIANNIS (AF)
IAMD COE DIRECTOR

10 STRENGTHENING THE ALLIANCE CYBER DEFENCE CAPABILITIES

Sozon A. LEVENTOPOULOS, MSc, PhDc
Cyber | Warfare Expert @ ZONOS SYSTEMS

20 EMERGING CAPABILITIES FOR SMALL TACTICAL UCAVS AND LOITERING MUNITIONS

Fotios Kampiotis
Aeronautical Engineer

34 SIMULATION OF A MACH-7 WAVERIDER IN OFF-DESIGN CONDITIONS

Dr. Ioannis K. Nikolos
Mechanical Engineer
Angelos G. Klothakis
Producton Engineering & Management

42 THE AIRE5G PROJECT

Dr. George Tzagkarakis
Scientific Data Analyst

50 THE RENEWED APPROACH

Arturo Arribas
Lieutenant Colonel

56 **JOINT MULTI-DOMAIN OPERATIONAL ADVANTAGE**

Wendi O. Brown
Lieutenant Colonel (Retired),

66 **AUTOMATING GEOGRAPHIC CONTENT**

Richard Goodman
Geography Specialist

74 **TRAIN AS YOU FIGHT REINVENTED**

Fotios Kampiotis
Aeronautical Engineer

Editorial

Dear reader,
As the Director of the Integrated Air & Missile Defense Centre of Excellence, it is a great pleasure and privilege to welcome you all, to the 3rd Annual IAMD COE Conference here in Chania/Crete.

Having in mind the valuable experience that the Centre gained from our 2nd Conference during June last year, I strongly believe that this conference will also have the same success and would be beneficial for the whole Integrated Air & Missile Defense community.

Based on our motto "Act Knowing", a phrase of Pittacus (640 - 568 b.c), a Mytilenean General and one of the seven wise men of ancient Greece, which means to be fully aware of the situation before acting – IAMD COE strives to support, inter alia, NATO's efforts to achieve Cognitive Superiority considering the increasingly diverse and challenging air and missile threats ranging from UAVs to sophisticated hypersonic missiles.

As NATO IAMD remains key for credible deterrence and defence, to maximize commanders' ability to anticipate, think, decide, and act, our COE puts an emphasis on IAMD integration to Multi-Domain Operations, mainly exploring emerging and disruptive technologies to support warfighting. On such endeavor, not only we capitalize on partnership opportunities with NATO entities, COEs in our COI, Industries, and Academics, but as well seek foster new mutually supportive and habitual relationships with the Operational and Training Community, locally here in Souda Bay (e.g NAMFI, NMIOTC, 115 CW) and remotely through exploitation of the Synthetic Environment (e.g ABTC/ HATC/ UAWC).

Since our previous conference in June 2023, and despite the limited workforce due to many vacant SUBJECT Matter Experts positions, the Center presented some significant achievements. The most important of them, from our perspective, are the following:
- The publication of its 2nd journal following the previous Conference with the subject 'Integrated Air and Missile Defence: a valuable pillar in NATO's Deterrence and Defence".
- Funding of a 2nd Study in collaboration with the Turbomachines & Fluid Dynamics Laboratory (Turbo Lab) of the School of Production Engineering & Management of the Technical University of Crete (TUC), with the theme:

"Analysis of the related Physical Phenomena and Aerodynamic Performance of Hypersonic Vehicle(s) and possible ways of exploiting those data in order to improve Surveillance Capabilities".

That study report, created by Dr. Ioannis Nikolos and Mr. Angelos Klothakis that we have the honor to host them both in our Conference, has been delivered to all NATO stakeholders and the Center's Framework and Sponsoring Nations with great appreciation, igniting the discussion for a new study on hypersonics to be delivered by late 2025.

- The collaboration with the Foundation For Research And Technology - Hellas Institute Of Computer Science (FORTH -ICS) to build an "Artificial Intelligence (AI) - Empowered Drone Detection Passive Radar using 5G signals – AIRE5G", a project under the direction of Professor George Tsagkarakis that we have the honor to host him in our Conference. The AIRE5G passive radar prototype is going to be delivered by the end of December 2025 and the effective exploitation by Ukrainians of innovative products to passively detect and track such threats highlights its value.

- Moreover, the Center successfully conducted the 1st Surface Based Air and Missile Defense Common Education and Training Program (SBAMD CET-P) iteration in April 2024. This course held by the IAMD COE aims to educate and train tactical-level SBAMD operators in NATO Tactics, Techniques, and Procedures (TTPs) regarding the execution of SBAMD operations in the NATO environment. The course was attended by 39 officers from 11 different countries and delivered by experts from various NATO entities, such as IAMD COE, AIRCOM, CCSBAMD, CAOC UEDEM, CAOC TORREJON, and JAPCC. The SBAMD CET-P contributes to the development of a common understanding and interoperability among NATO SBAMD forces. A 2nd iteration will follow in November 2024.

Hosting the 2nd Integrated Air & Missile Defense Annual Coordination Meeting, which has been attended by relevant representatives from COEs and NATO entities to synchronize the main IAMD stakeholders' efforts and to identify opportunities to collaborate efficiently and effectively.

- The active participation in the Allied Joint Operations Doctrine Working Group (AJOD WG), an important event for the Alliance's Doctrines & Standardization.

- Supporting continuously at our best capacity the development and revision of IAMD-related documents, having the lead in writing the "Operational Guidance" Chapter of the new C-UAS Doctrine which is under approval from NATO Standardization Office (NCO), and as a member of the writing team of Allied Administrative Publications revisions, in accordance with the Allied Joint Doctrine Campaign Plan (AJDCP).

- Participating at the Situational Understanding Thematic Working Group (SU TWG), part of the concept of Layered Resilience (LR), one of the five Warfare Development Imperatives of NWCC, thus, directly supporting the transformation effort of SACT.

- Finally, throughout our participation in various conferences, meetings, and exhibitions and we have expanded our network, inter alia, with academia and industry.

Such efforts are being continued with our 3rd Annual IAMD Conference which has the theme:

" Integrated Air and Missile Defense:

Shaping the Operational Environment to our advantage."

During this conference, we intend to build a picture of the current geostrategic military situation for Euro-Atlantic Allies and Partners. This will lead us to discuss the new era of Challenges, focusing on Emerging Threats, Hypersonic Weapons, and developments in Unmanned Aerial Systems (UAS), how NATO will respond to IAMD's current and future challenges, Integration and Interoperability, Effectiveness and Sustainability, as well as on Innovation, Experimentation and Wargaming.

The ability to foster persistent preparation in the modern arena, requires a Synthetic Environment of live and advanced modelling and simulation (M&S) constructs to identify areas for improvement, build trust in new capabilities and plans, and support leadership development by wargaming and experimentation. Moreover, frequent realistic training, exercises, and technology development using live, virtual, and constructive (LVC) venues to enable the conservation of resources, improve the realism of training for combat and multi-domain challenges, and facilitate the development of innovative and collaborative solutions.
IAMD COE interrogates NATO Nations relevant capabilities to identify modern M&S endeavors and new ways of IAMD training exploiting inter alia Serious Games & Modern XR technologies, to highlight risks and opportunities in the development of an envisaged simulated battle network of sensors and effectors, an absolute necessity, in my view, to efficiently prepare our warfighters to deter and if needed fight and win. Critical in all our pillars of work to boost envisaged transformation of NATO IAMD effects is our developing M&S laboratory which will be further digitally evolved in our new building, scheduled to be delivered by the end of 2024.

As the value of sharing knowledge, ideas, and experiences among specialists to enhance the effectiveness of NATO Air and Missile Defense capabilities, cannot be overstated, our Conference success is mainly established upon our distinguished speaker's expertise and of course in all participants active engagement.

The offered compendium of selected articles seeks to enhance interest and awareness of the last evolutions, topics and developments within the Air Defence Domain.
The edition opens with an article by Sozon A. LEVENTOPOULOS, MSc, PhDc a Cyber Warfare Expert who offers a comprehensive analysis of the evolving IAMD landscape in the face of emerging cyber threats.
Continuing our exploration of the IAMD, Br.General (ret) Fotios KAMPIOTIS shares invaluable insights into the transformative changes witnessed in recent years concerning tactics and strategies related to low – cost drones, loitering ammunitions and countering electronic warfare.
The next article delves into future hypersonic vehicle developments and operational flexibility based on research of the technical University of Crete.
We then examine the AIRE5G project, with Dr. George Tzagkarakis Scientific Data Analyst, presenting a detailed article on the implications of 4G/5G signals and DVB broadcasts for detection systems in complex operational landscapes.
The journal progresses with an analysis of the European Union's renewed approach to the Air Domain, aimed at identifying key areas of focus, optimizing resource allocation, and proposing concrete actions to add value without duplicating efforts.
Lieutenant Colonel (Ret.) Wendi O. Brown from the United States Army Reserve discusses the evolution of joint doctrine over single-service approaches, emphasizing the adoption of cutting-edge technology and the importance of interoperability and joint training.
Further, we explore the role of automated geographic content in augmenting response speed for IAMD purposes.
The journal concludes with an enlightening article on the exploitation of synthetic environments to enhance NATO IAMD capabilities, addressing the growing complexity of air and missile threats, from UAVs to hypersonic missiles.

Brig. General (OF-6)
Nikolaos MAKRIGIANNIS (AF)
IAMD COE DIRECTOR

Integrated Air & Missile Defence Center of Excellence – Annual Conference
Strengthening the Alliance Cyber Defence Capabilities to protect IAMD in Current and Future Operational Arena

Research Paper: "IAMD at the Dawn of a New Threat Era"

Short Abstract : The paper "IAMD at the Dawn of a New Threat Era" explores the evolving landscape of Integrated Air and Missile Defense (IAMD) in response to new cyber threats. It emphasizes the significance of adapting defense strategies to counter advanced persistent threats (APTs) and supply chain attacks, exemplified by recent incidents such as the XZ Utils attack. The study also delves into the implications of emerging technologies, including quantum computing and artificial intelligence, highlighting their potential for both defense and offense. Moreover, it underscores the necessity of securing the supply chain and dominating the electromagnetic spectrum to maintain robust IAMD capabilities. The paper advocates for a multifaceted approach that integrates traditional defense methods with cutting-edge technologies to build a resilient and secure IAMD framework.

Keywords : Air defence, Cyber Warfare, Cognitive Warfare, IAMD

1. Introduction

The concept of Integrated Air and Missile Defense (IAMD) has become increasingly critical as the nature of global threats evolves in complexity and sophistication. Historically, air defense focused on tangible threats such as aircraft and missiles. However, the contemporary landscape requires a more holistic approach that incorporates not only physical threats but also hybrid and cognitive warfare. This approach stems from the broader technological advancements and increased connectivity that characterize modern battlefields. As nations and organizations become more reliant on the digital economy, the potential vulnerabilities multiply, necessitating a robust and adaptive defense mechanism that can address both conventional and unconventional threats.

In this new threat era, the traditional boundaries between different types of warfare are blurring. Cyber warfare, cognitive warfare, and hybrid warfare are now integral components of the strategic environment. The modern battlefield is no longer confined to physical spaces but extends into the digital realm, where adversaries (such as Advanced Persistent Threats (APTs)) employ sophisticated techniques and supply chain attacks to compromise critical systems.

The integration of emerging technologies like quantum computing and artificial intelligence further complicates the defence landscape, offering both unprecedented capabilities and new challenges. As such, a comprehensive understanding of these dynamics and the implementation of multifaceted defence strategies are essential for safeguarding IAMD systems against an increasingly diverse array of threats.

2. Background

2.1 General

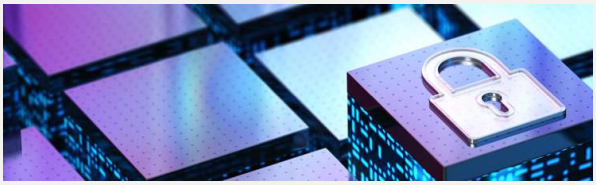
The idea of people flying like birds is as old as humanity itself. It spans more than 3000 years, dating back to a mythical time, when a craftsman named Daedalus [Wachter, 2015] managed to create a "flying device" for himself and his son, in an attempt to escape Minoan Crete [Morris, 1995]. While there were many attempts to actually build a flying machine, such as Archytas'2 "peristera"3, all of which were unsuccessful. Humanity had to wait until 1903, when the American Wright Brothers' airplane, named Flyer I, performed "the first sustained and controlled heavier-than-air powered flight"4. It required only 8 years for the airplane to be used for military purposes, when an Italian pilot, Captain Carlo Piazza5, flew a Blériot XI aircraft on a reconnaissance mission over Turkish positions in Libya. This marked the beginning of military aviation.

The concept of computers (and by extend, to the whole information technology ecosystem) has a very similar history. The definition for the word computer, is "one who calculates" and for decades that was the term used for people that could quickly and accurately perform complex computations. Early examples of "computing devices" date back to prehistoric Africa6, [Huylebrouck, 2010] while the Antikythera mechanism being the first analog (mechanical) computer [Efstathiou et al, 2018]. Charles Babbage is considered the "father of the modern computer" [Copeland, 2020], because he conceptualized and invented the first mechanical and reprogrammable computer, which incorporated all those things that are part of today's computers, like integrated memory, printing devices, programmable cards, etc., and all of that back in the 19th century. In modern terms his computer would be categorized as Turing-complete7. The concept of the modern computer was proposed by Alan Turing in 1936. Turing proposed, and proved [Copeland, 2023], a device capable of computing anything, provided it has the necessary "executing instructions", or program.

2.2 Information and communication technology

With the term Information and Communication Technology (or ICT) we refer to an extended ecosystem that includes both the information technology and unified communications8 (including telecommunications). This umbrella – and ambiguous – terms closely relate to information, which in turn, is data in context. Within the realm of ICT, information is taking a prevalent role and importance. The whole infrastructure aims in creating, storing, retrieving, transmitting and manipulating information in its digital form. This was made possible because of the constant developments in both processing power (Moore's Law)

9 and information storage. The latter is often overlooked but is the key factor that shapes today's world10. While computing power is impressive, it couldn't have provided the boost needed for the dominance of information. Technological innovations led to more powerful, more reliable, and most important, cheaper memory devices (like SD cards, Hard Disk Drives, etc.), which can provide the desired availability and integrity of information.



3. Definitions

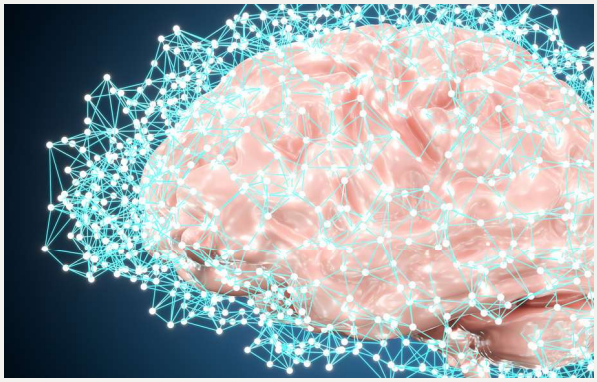
3.1 Cyberspace: For the purposes of this paper, we will follow Kuehl's definition of cyberspace11, which not only refers to the information environment, but incorporates electronic elements and the electromagnetic spectrum.

3.2 Cybersecurity: Today, the term "cybersecurity" is frequently used in the mass media as a catch-all phrase for a wide range of topics, despite the ongoing debate, even about its correct spelling. We can define cybersecurity as the concept which ensures the protection of networks, devices and data, ensuring – at all times – their Confidentiality, Integrity and Availability.

3.3 Information Security: Today, information is (or should be) considered an asset, having value to the organization or entity that holds it. Therefore, it must be protected (especially the valuable and sensitive one) irrespective of the form (or format) it might take. The main focus is to ensure that the three foundational aspects of Confidentiality, Integrity and Availability are achieved.

3.4 Hybrid Warfare: When Frank Hoffman first discussed the phenomenon or practice of hybrid warfare [Hoffman, 2009], he might not have anticipated the impact (both positive and negative) his observations would have on the development of military operations and related threats. While as a concept it is not new, the term "hybrid warfare" tends to prevail (perhaps not universally) as it allows for the integration of many diverse methods and practices within the logic of military operations.

3.5 Cognitive Warfare12: Cognitive warfare refers to strategies and tactics aimed at influencing, disrupting, or controlling the perceptions, beliefs, and decision-making processes of individuals or groups. It encompasses a range of psychological operations, including propaganda, misinformation, and psychological manipulation, often utilizing advanced technologies and social media platforms [Miller, 2023]. The goal is to achieve strategic advantages by shaping the cognitive environment of adversaries, weakening their morale, causing confusion, or manipulating their actions. Cognitive warfare exploits the human mind as the battleground, making it a critical aspect of modern hybrid warfare and information operations.



4. The Current [Cyber] Threat Environment

4.1 General

The current [cyber] threat environment is characterized by extreme sophistication, the implementation of advanced and "exotic" techniques, and a "military-like" approach in developing the attack scenarios. The term Advanced Persistent Threat refers to threat actors that not only showcase and employ these key characteristics, but also are highly skilled and knowledgeable, highly motivated, well-paid, and they have access to an extensive arsenal of tools and practices.

Modern techniques evolve around the exploitation of novel threat approaches or the exploitation of unknown vulnerabilities13 (most APTs will craft their own malware), carefully planned campaigns and novel techniques, such as:

a. Living of the Land (LOTL)14: This approach will exploit legitimate software or build-in tools or even devices (the most targeted ones are the – common – routers used at homes or small offices, which lack advanced security features), available on the target system to carry out further attacks and exploits. This technique leverages the use of trusted processes and tools, keeps the use of malware to a minimum, therefore it is extremely difficult to detect and attribute. Stealth is the key word, and malicious actors will exploit scripting languages or native functionalities, and will manipulate the device's firmware or administrative tools, to achieve their objectives.

b. Hands on Keyboard: This approach15 involves the use of direct and manual interaction between the malicious actor and the targeted system (usually after gaining the initial foothold). Unlike automated attacks, these involve real-time activities such as navigating the system, executing commands, and manipulating data, allowing for adaptive and precise exploitation based on the system's defenses and responses.

By exploiting this – highly demanding – method, malicious actors can have a more sophisticated and targeted approach, dynamically adjust their tactics, or exploit opportunities as they arise.

4.2 The XZ Utils attack16

In April 2024, a "lone developer" working on the PostgreSQL database for Microsoft, tried to identify why the SSH (secure socket)17 was using 40% more resources than it should. Soon it was discovered that within the source code of the XZ utils, a program used for lossless compression in Linux, a malicious "part" has been added. The interesting part of this attack, is that the malicious code was "introduced" via a legitimate update process. The malicious actor (or actors) implemented a two year long social engineering campaign, convincing both the initial developer and the companies that their intentions were pure. In summary:

a. This attack is a typical supply chain attack (similar to the SolarWinds hack) which "incorporated" a malicious part within a legitimate program (LOTL technique).

b. It exploited (for malicious purposes) the very heart of the concept of the Free and Open-Source Software (FOSS), which most of the time is maintained by a handful of zealous developers and software engineers. It should be stated that the European Union supports the transition towards a FOSS environment.
c. It exploited (again for malicious purposes) one of the fundamental "cyber hygiene" methods, which dictates that systems and software should be constantly remain up-to-date and patched. On the other hand, none of the companies have followed best practices, and rushed to implement the update, without proper validation and code analysis.

4.3 Quantum Computers
This new form of computers leverages the quantum mechanical phenomena, associated with qubits, which have the ability to represent both 0 and 1 (in "classical" computers these are known as bits – the smallest unit of data) simultaneously, through a phenomenon known as superposition [Zeilinger, 1999]. Furthermore, qubits can also be entangled, meaning that these particles are interconnected in such a way that the state of one particle directly influences the state of the rest, irrespective of their distance. The combination of these two phenomena allows quantum computers to perform complex calculations at unprecedented speeds. This makes quantum computers especially useful for brute-forcing18 complex cryptographic algorithms. The modern cryptographic approaches, dictate the use of post-quantum encryption algorithms, [Kramer, 2023] meaning that these algorithms are so complex that even quantum computers will not be able to "crack" them within a meaningful timeframe.

4.4 The "electrification" of the Battlefield
While most of the conversation for modern developments considers computers and the digitalization of our lives, it is electricity the underlying constant that allows computers and networks to run. Amid the flood of new technologies and systems being introduced, the criticality of a continuous and unlimited supply of electrical power seems to go unnoticed. The ongoing war in Ukraine has showed that one of the "centers of gravity" is not the industrial and economic complex, but the uninterrupted supply of electricity , which is not only necessary for the operation of computing clusters, but also for their cooling. Modern battlefields will require extremely large amounts of electricity, especially with the extended usage of both networks and directed energy weapons (i.e., lasers).

4.5 Artificial Intelligence

Usually, the term intelligence will refer to the ability to perceive or infer information (which in turn is "data in concept")19 and further evolve it through a cognitive process to retain it as knowledge, which will later be applied to adaptive behaviors within an environment. Still, there is no concrete way on deciding "who" is actually intelligent, with several definition being proposed. Since November 2022 and the introduction of ChatGPT 20 (a large language model or LLM) the term artificial intelligence, which was established in 2017 by Google, [Vaswani et al, 2017] has gained tremendous momentum. On the other hand, there are numerous ethical, practical and technological challenges and drawbacks that need to be addressed before AI been a valid contributing factor. Nevertheless, AI (and Machine Learning) can and will be used in various ways for malicious purposes. The DAN method, or "Do Anything Now"21 for ChatGPT, which jailbreaks ChatGPT's ethical constrains is only one of the few.

5. Defending IAMD in the new Threat Era

The war in Ukraine has showcased – among other – the importance of air defence. As the modern battlefield is becoming more complex, and heavily depended upon software and networks, rather than missiles and radars, with both systems requiring huge amounts of electricity (and water for cooling purposes) is crucial to alter the way we defend IAMD in this new era.

5.1 Defence & Offence in AI

Current AI models are dependent upon an extremely large amount of annotated data (similar term to data in context). Collecting, analyzing, and exploiting these data has its own challenges. Data poisoning is one of the prominent methods for attacking AI models. Data poisoning is a form of attack on machine learning models where malicious data is intentionally introduced into the training dataset. This corrupted data can skew the model's learning process, leading to incorrect or biased outputs. The goal of such attacks is often to manipulate the behavior of the AI system, making it perform erroneously or unfairly when deployed in real-world scenarios.

5.2 Defend the Minds and Hearts

As already stated, cognitive warfare is an emerging form of warfare that specifically targets the minds of individuals or groups, aiming to influence, disrupt, or manipulate their perceptions, decision-making processes, and belief systems. This form of warfare leverages advances in technology, psychology, and communication strategies to affect the cognitive domain of targets, which encompasses the mental functions of perception, judgment, and reasoning. The best way to win a battle (or even the war) is to "convince" your opponent that there is no way of winning.

5.3 Dominate the Full Electromagnetic Spectrum

Electronic warfare (EW) refers to the strategic use of the electromagnetic spectrum to gain a military advantage. It involves a range of practices including the interception, identfication, and disruption of radio communications and other forms of electromagnetic signals. EW can be broadly categorized into three main types: electronic attack (EA), electronic protection (EP), and electronic support (ES). Thinks to consider include:

a. Build resilient communication networks and have backup and out-of-band systems ready.

b. Incorporate within Electronic Warfare, cyber defensive and offensive capabilities and doctrines.

c. Incorporate AI models for rapid signal analysis or false target creation.

5.4 Secure the Supply Chain

One of Kohen's principles22 regarding viruses dictates that is impossible to identify with 100% certainty if a program has malicious intent or not. A supply chain attack targets a trusted third-party vendor supplying essential services or software. In software supply chain attacks, malicious code is embedded into an application, affecting all users. Hardware supply chain attacks, on the other hand, involve tampering with physical components to achieve a similar outcome. With modern programs and software having million lines of code23 (a simple webpage can easily reach 5.000 lines) and more than 500 dependencies on average,24 ensure the integrity of the code and that of the hardware will be paramount in safeguarding IAMD.

6. Epilogue

In an era where Integrated Air and Missile Defense (IAMD) systems are increasingly reliant on complex networks and advanced software, it is crucial to re-examine the tools and technologies we utilize. Streamlining and simplifying the technological landscape can enhance security by reducing the threat landscape thus minimizing potential vulnerabilities. This includes evaluating the necessity of tools and considering hybrid solutions or on-premises infrastructure instead of defaulting to cloud computing. Building decentralized mesh networks can provide robust alternatives to conventional civilian networks, while returning to analogue systems can offer reliable backups that are less susceptible to cyber-attacks.

Embedding cyber offensive capabilities within IAMD systems is essential, particularly by disrupting AI and machine learning datasets. Leveraging information overload, or security by obscurity, can also serve as a strategic advantage by overwhelming attackers with irrelevant data. A multifaceted approach that balances modern technological advancements with traditional methods will help build a more resilient and secure IAMD framework.

> " The future of IAMD depends on our ability to adapt and innovate in response to the evolving threat landscape."

about the author

Sozon A. LEVENTOPOULOS, MSc, PhDc
Cyber | Warfare Expert @ ZONOS SYSTEMS

An accomplished ex-military officer (ret.) and Cybersecurity Professional/Researcher with over 25 years of active service and industry experience. Specializing in operational planning and execution, I have successfully overseen numerous projects at a national level and during my tenure at NATO. As Domain Site Administrator and Automatic Data Processing Officer, I spearheaded holistic cybersecurity and information security solutions and was instrumental in designing, testing, integrating, and implementing various ICT systems.


2408

Emerging Capabilities for Small Tactical UCAVs and Loitering Munitions

Abstract

The novel methodologies and tactics deployed in recent and ongoing operational theaters, underscore the profound influence of small cost-effective drones on contemporary warfare. This paper delves into the creative utilization of smaller, economically viable, yet pioneering drone technology, showcasing its pivotal role in granting critical strategic leverage. This phenomenon has empowered smaller armed forces and non-state entities, to effectively confront conventionally superior adversaries, challenging traditional concepts of air superiority. While conventional aircraft remain essential, drones provide a complementary capability that can operate effectively in contested environments. This dual approach complicates enemy air defense strategies and offers commanders more tactical options. The implications for future conflicts, encompassing adaptability, strategic supremacy, and the evolving paradigm of air dominance, are also thoroughly examined. Drawing insights from conflicts such as the Nagorno-Karabakh war, the Ukraine war, Houthi operations in Yemen, the Gaza conflict, and the Iran Drone Attack on Israel, this paper aims to furnish useful perspectives for military strategists and decision-makers. Furthermore, it sheds light on the technological advancements driving the capabilities of drone warfare, with particular emphasis on the contributions of Spirit Aeronautical Systems SA (SAS Technology), a leading innovator in this domain.

Introduction

The evolving tactics and strategies observed in recent operational environments, have highlighted the transformative role of lower-cost drones in contemporary military operations. This marks a notable departure from the previous dependence on larger, more advanced drones, to smaller, commercially available ones, to maintain an operational edge against formidable forces, underscoring the importance of adaptability, cost-efficiency, and innovation in modern warfare.

Evolution of Drone Use in Recent Operational Theaters

Early Reliance on Larger Drones

In the early stages of the Nagorno Karabagh and Ukraine conflicts, larger drones were utilized, such as the Turkish TB2 Bayraktar, that proved to have significant effect. These drones, equipped with advanced sensors and munitions, were used for precision strikes and intelligence gathering. The TB2's ability to loiter over targets and deliver accurate strikes made it a valuable asset.

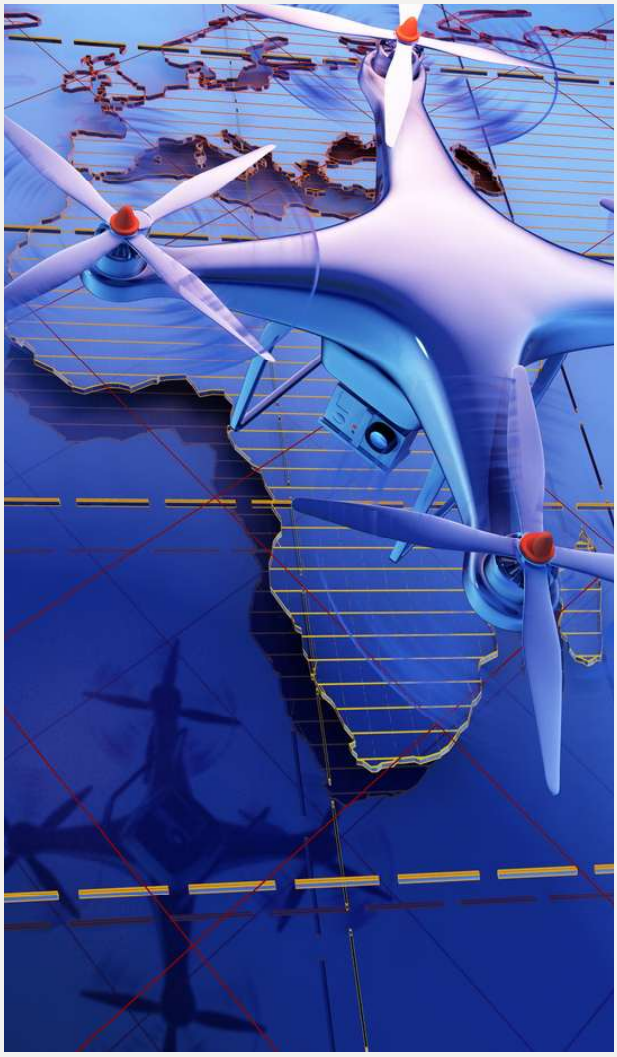
Shift to Smaller, Commercially Available Drones

As adversaries improved their air defense capabilities, military strategies in these operational theaters adapted by incorporating smaller, commercially available drones into their operations. These drones were often repurposed from civilian use, offering a cost-effective and adaptable solution.

Their smaller size and lower cost reduced in an affordable way the risk of detection and interception, allowing forces to maintain surveillance and strike capabilities despite evolving threats. The challenge of effectively countering the operational use of custom-made smaller drones lies mainly in their agility, versatility and the difficulty in detecting and neutralizing them before they can cause harm.

Here are some reasons why modern countermeasures may struggle in this regard:

- Size and Speed: Smaller drones are harder to detect due to their size and can move swiftly, making them difficult targets for traditional anti-drone systems.
- Adaptability and Maneuverability: Small drones can be highly maneuverable and adaptable, can be designed with various capabilities, such as autonomous navigation or payload delivery, making them versatile and unpredictable. They can fly at low altitudes, hide behind terrain, and change direction rapidly, making them quite challenging to track and engage.
- Low Detectability: These drones often operate at low altitudes, evading radar detection systems designed to track larger aircraft.
- Ease of Acquisition and Deployment: Advances in technology have made it easier for adversaries to acquire or manufacture drones, allowing them to deploy them quickly and in large numbers.
- Low Vulnerability to Electronic Warfare: The simplistic and sturdy design of small drones renders them less susceptible to electronic warfare, making traditional countermeasures less effective against them.
- Electronic Countermeasures: Some modern drones may be equipped with countermeasures against traditional anti-drone technologies, such as jamming or spoofing systems.
- Cost-Effectiveness: Traditional air defense systems such as fighter jets and surface-to-air missiles are designed to counter larger, high-value threats like enemy aircraft or ballistic missiles.



Deploying these systems against small drones, which are relatively cheap and can be produced in large numbers, is definitely not cost-effective.
- Lack of Scalability of the Expensive air defense assets: Such systems are mostly designed for high-intensity conflicts against well-equipped adversaries. However, the proliferation of small drones has introduced a new type of threat that may not fit into the traditional paradigm of military operations, requiring more scalable and adaptable countermeasures.
- Civilian Considerations: In many conflicts, small drones are used by non-state actors or insurgent groups operating in civilian areas. Deploying expensive air defense assets in such environments carries the risk of collateral damage and civilian casualties, which can have significant political and humanitarian implications.

To effectively confront the threat of small drones, military forces are increasingly turning to a combination of tactics and technologies tailored specifically for this purpose. This includes the development of specialized counter-drone systems, such as jamming devices, drone detection radars, and kinetic interceptors, as well as the use of tactics like swarm defense and rapid response teams. Additionally, efforts to improve situational awareness and information sharing among military units and civilian authorities can also enhance the overall effectiveness of counter-drone efforts. To confront the threat of small drones effectively, fighting parties have employed various lessons and strategies:

- **Integrated Defense Systems:** Combining multiple layers of defense, including radar detection, electro-optical/infrared sensors, and kinetic or non-kinetic countermeasures, which can improve the chances of detecting and neutralizing small drones.
- **Agile and Mobile Countermeasures:** Deploying mobile anti-drone systems that can quickly reposition and adapt to changing threats can enhance response capabilities.
- **Collaborative Efforts:** Cooperation between military, law enforcement, and civilian agencies, can improve situational awareness and coordination in countering drone threats.
- **Technological Innovation:** Continued research and development of advanced detection and mitigation technologies, such as machine learning algorithms for drone detection or directed energy weapons for neutralization, can enhance capabilities against small drones.
- **Education and Training:** Providing training to military personnel, law enforcement officers, and security personnel on the detection and mitigation of drone threats can improve response effectiveness.
- **By combining these approaches and continuously adapting to evolving threats**, fighting parties can better confront the operational use of custom-made smaller drones. However, it remains a challenging and ongoing endeavor requiring constant vigilance and innovation.

Strategic Advantages of Low-Cost Drones

"Strategic Imbalance": The Economic Dilemma of Low-Cost Drone Defense

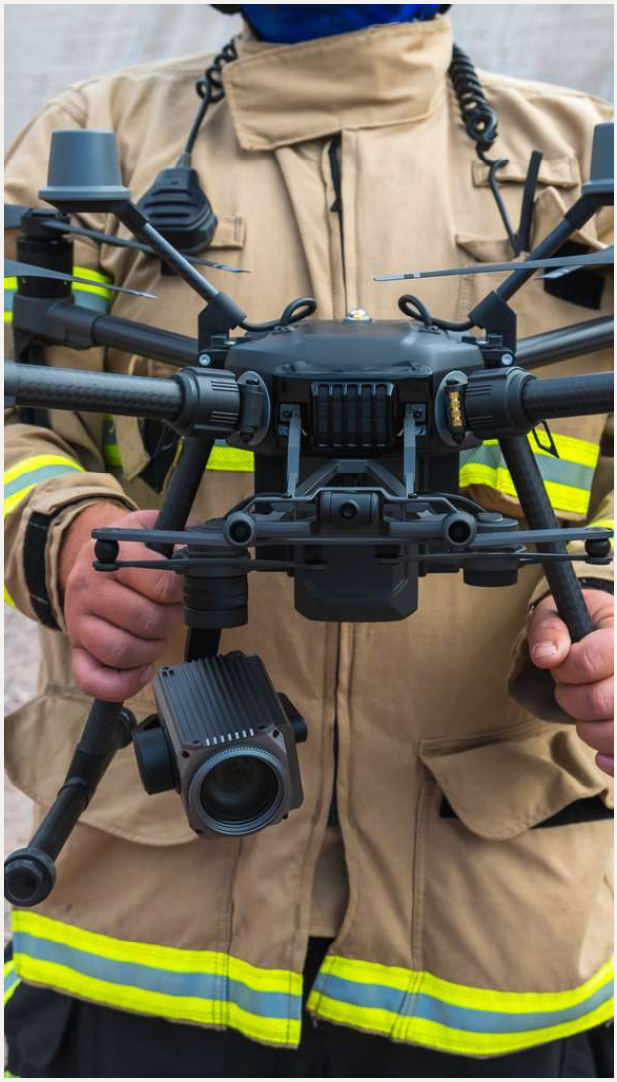
Despite advancements in counter-drone technologies, the widespread adoption of low-cost drone strategies, forces defenders to allocate substantial resources, creating a significant cost disparity between the threat and the deterrence. This dynamic represents a fundamental change in modern warfare, as many countries' air defense structures and organizations are primarily designed to counter traditional threats such as costly fighter aircraft and ballistic missiles, rather than the affordable and ubiquitous low-cost drones. Consequently, defenders are often compelled to deploy their high-value air defense systems, to counter relatively inexpensive drone threats. This scenario leads to an economically and strategically unsustainable situation for the defending party.

Persistent Surveillance and Reconnaissance, at minimal risk

Low-cost drones offer a significant advantage in providing persistent surveillance and reconnaissance capabilities with minimal risk to the user. These drones enable continuous monitoring of enemy movements, real-time battlefield assessments, and timely (prompt) decision-making. This capability is crucial for maintaining situational awareness and responding effectively to dynamic battlefield conditions.

Enhanced Offensive Capabilities

The adaptability of purpose-built and highly customizable systems, such as weaponized drones or loitering munitions, allows them to be equipped with a variety of weapons and explosives, including legacy systems already abundant in military inventories. When used on innovative unmanned systems, these munitions gain new improved capabilities and expanded operational perspectives. The use of such systems, provides even small army units with organic Close Air Support (CAS) and precision strike capabilities, reducing their dependency on high-value assets like fighter planes and helicopters. This flexibility enables forces to disrupt enemy operations and gather critical intelligence with minimal risk of loss of expensive assets or lives. The cost-effective nature of these operations proves to be a valuable force multiplier, significantly enhancing offensive capabilities.



Learning from Low-Cost Drone Operations: Insights from Recent Operational Theaters

Nagorno-Karabakh War

The Nagorno-Karabakh war between Armenia and Azerbaijan in 2020, debuted the widespread use of drones in modern warfare with significant impact to the conflict outcome. Nevertheless, this first case was based mainly to the extensive use of larger systems like the Turkish and Israeli drones by Azerbaijan, enabling it to achieve significant battlefield successes. These drones were used for surveillance, target acquisition, and precision strikes, effectively neutralizing Armenian defenses and artillery. This conflict underscored essentially for the first time in a real operational environment, the importance of integrating drone technology into conventional military operations to achieve strategic and tactical advantages.

Ukrainian Front

The war in Ukraine is entering its third year and Europe's second biggest country is short of manpower and ammunition. According to Ukraine's Minister for Digital Transformation, Michelo Federov, “in certain areas of the front, FPV or first-person view drones are destroying more targets than artillery". Obviously, Russia is also extensively using UAVs into theater. As military analysts point out, the crucial factor for the success of these low-cost systems, is the fact that they can approach at very low altitudes (<100 ft). Consequently, because of the curvature of the earth, they cannot be seen with a regular radar, because they approach below the line of sight over the horizon.

The use of low-cost drones in the Ukrainian conflict, has demonstrated their significant tactical advantage in providing real-time intelligence and reconnaissance capabilities to both conventional and unconventional actors. This accessibility to advanced technology has spurred innovation in adapting drones for military purposes, highlighting the need for effective countermeasures to mitigate their threat, while also emphasizing the evolving dynamics of asymmetric warfare and the blurring lines between conventional and unconventional tactics.

Houthi Activities in Yemen

In 2021, The Houthi rebels in Yemen have effectively utilized low-cost drones to counter the superior technological and military capabilities of the Saudi-led coalition. Their latest attacks to commercial ships in the greater region of the red sea, has caused significant disruption to the international flow of trade. These drones have been used for reconnaissance, targeted strikes, and even psychological warfare. The Houthi's ability to locally manufacture and deploy drones has allowed them to sustain their operations despite limited resources. This demonstrates the potential for low-cost drones to provide strategic advantages to non-state actors and insurgent groups.

"Just think of what just happened. One-way UAVs, put everyone in the game to include the Houthis. The crew of the guided missile destroyer USS Carney shot down three land attack cruise missiles and several drones that were launched by Houthi forces in Yemen. And when they did their attack on 18 October, they had 21 come over at $7,000 apiece and we shot them down with $700,000 SM2 missiles. That is not the right side of the cost curve."

[Gen. James B. Hecker, (Commander, U.S. Air Forces in Europe; Commander, U.S. Air Forces Africa; Commander, Allied Air Command). Interview, 21 Feb 2024, AFA Warfare Symposium]

Gaza Conflict

In Gaza, beyond the IDF that extensively and successfully uses all drone types (from sophisticated to low cost) in their operations, the non-state actors such as Hamas and Hezbollah, have also leveraged low-cost drone technology. These drones have been used to gather intelligence, conduct surveillance, and carry out targeted attacks against Israeli forces. The ability to operate these drones within the dense urban environment of Gaza has provided tactical advantages, complicating Israel's efforts to maintain air superiority and ground security. This conflict highlights the challenges posed by drone proliferation in asymmetric warfare environments.

IRAN Drone Swarm Attack to Israel

The five-hour drone swarm attack of Iran against Israel, with more than 300 drones and ballistic missiles last April, was reported to have been successfully confronted. Iran launched around 170 drones, over 30 cruise missiles and more than 120 ballistic missiles during its attack, the vast majority of which were successfully intercepted by the formidable and multi-layered missile defense deployed by Israel and its allies. However, this is the one side of the coin, the other being the economic impact of the attack and the questions about the capability of any country to sustain such defense measures for an extended period of time. According to sources the cost of Israeli defense, is estimated to be between 1 to 1.3 BUSD. The cost of each Arrow missile is estimated to be around $3.5 million and the corresponding cost for a David's Sling missile is estimated to $1 million. In contrast, Iranian ballistic missiles cost around $100,000 each, and its Shahed drones only $20,000-$50,000, resulting in a total cost for the attacking side within a range of $18.4 M to $23.5 M (1,8 % of the cost borne by the defending side).

"the question is about the capability of any country to sustain such defense measures for an extended period of time"

Air Defenses Readiness to Counter the Emerging Drone Threat

Tactical forces around the world appear to be caught off guard, in view of this emerging threat, resorting to improvised, ad hoc solutions. As highlighted above, use of expensive assets to counter the new threat is neither economically nor strategically a viable solution. The use of electronic and drone countermeasures is a tactical choice and has created a booming market of anti-drone systems and strategies, capable of undertaking various counter drone tasks.

Nevertheless, this battle of dominance between the drones and the anti-drones, is a race that will continue to the future without a profound winner and the key to this is the capability of innovation primarily on the drone side, which will always be the leader in the race. To the moment, the main efforts in the modern operational theaters have focused on the electronic countermeasure's domain, but have not yet been able to provide comprehensive protection.

Strategies for Countering Electronic Warfare

Drones have faced during operations, sophisticated electronic countermeasures (ECM) designed to jam communications, GPS signals, and even to take control of the drones. Despite these challenges, several strategies analyzed below, have been employed to overcome ECM:

- **Frequency Hopping:** Many drones are now equipped with frequency-hopping spread spectrum (FHSS) technology, which changes rapidly the frequency of the communication signal, making it difficult for adversaries to jam the signal effectively.
- **Autonomous Navigation:** Advanced drones can switch to autonomous navigation if they lose communication with the operator. Using pre-programmed waypoints and onboard sensors, these drones can continue their mission even in the presence of jamming.
- **Encrypted Communications:** By encrypting the communication signals, drones can protect (safeguard) the integrity of their data link against interception and jamming attempts.
- **Redundancy and Backup Systems:** Implementing redundant systems for communication and navigation ensures that if one system is jammed or disrupted, the drone can switch to a backup system to maintain operational effectiveness.

The continuous advancement in counter-drone technologies has sparked a new type of arms race, compelling the development of drones that are more resilient to these countermeasures. This creates a complex cost-benefit dynamic, as integrating increasingly expensive systems to counteract electronic countermeasures (ECM), undermines the goal of maintaining low-cost drones. Recent operations have demonstrated that the solution lies in achieving a delicate balance through technological moderation, ensuring cost-effectiveness. To counter the lack of technological edge in ECCM (Electronic Counter-Counter Measures) technology, greater number of "affordable" systems can be used to saturate enemy defenses and acquire significant strategic and tactical advantages, especially when combined with innovative tactics that introduce elements of surprise. This latest factor increases the need of use of "less known", locally manufactured, customized systems, in contrast with the more expensive export type versions, whose capabilities are well known and military defense systems are adequately prepared to confront.

Limitations of Electronic Countermeasures

Despite the advancements in ECM, these systems have limitations and are not foolproof against low-cost drones:

- Sheer Volume of Drones: Low-cost drones can be deployed in large numbers, overwhelming ECM systems that are not designed to handle swarms of small, inexpensive drones.
- Decentralized Control: Some drone operations utilize decentralized control mechanisms where multiple drones operate semi-autonomously, reducing the effectiveness of jamming a single control signal.
- Improvised Solutions: Adversaries have developed improvised methods to counter ECM, such as using visual signals for drone control or deploying drones with minimal reliance on GPS, making them less susceptible to jamming.
- Terrain and Urban Environment: Operating drones in complex terrains and urban environments can shield them from ECM, as buildings and natural features can block or reflect jamming signals.

SAS Technology Innovative Unmanned Systems

Spirit Aeronautical Systems (SAS Technology), is a prominent UAS manufacturer based in Greece. SAS is notable for being the first Greek company to design, manufacture, and test armed unmanned systems and its defense division is specializing in lower cost mobile and versatile weaponized drones.

Even prior to the aforementioned conflicts, SAS showcased a forward-thinking strategy at DEFEA 2021, introducing innovative systems that challenged the conventional operational thought process. Among these innovations was the debut of SARISA equipped with 2.75 rocket launchers, alongside suicide USVs (USV Pyrpolitis), and drones outfitted with mortar cells and hand grenade payloads. Subsequently, SAS has maintained its commitment to innovation, field-testing and refining its primary systems into mature operational tools. These advancements have positioned SAS to not only complement but also enhance capabilities of traditional military platforms, such as helicopters.

SAS Technology's SRS-1X multicopter and AHM-1X loitering munition, demonstrate the practical application of lower-cost innovative drones in warfare. With these efforts, SAS Technology has made significant contributions to the development of innovative, lower-cost, professional weaponized unmanned systems, showcasing a new category of operational systems. These purpose-built and highly customizable professional systems, bridge the gap between the successful low cost modified commercial drones and the larger advanced and expensive unmanned platforms.

SARISA SRS-1A with RL275-1S (2.75" Rocket launcher)

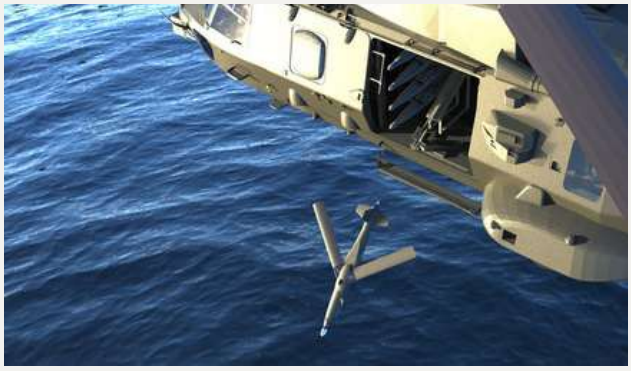
SAS' flagship, the UAV/UCAV, the SARISA, exemplifies the versatility and operational capability of modern drones. SARISA can integrate various weapons and payloads, making it suitable for diverse operational scenarios, providing organic close air support and resupply capabilities to Army units. Some of the payload capabilities of the SRS-1X are:

- The 2.75" Rocket (Unguided and Laser Guided);
- Various types of RPGs (M72 LAW, RPG-18, RPG26 etc.);
- Various Anti-Tank weapons;
- Various types of hand grenades and mortar cells;
- Cargo Payloads;
- Rescue equipment (life rafts and other floating devices).

SARISA SRS-1A Releasing AIHMI (AHM-1X) Stand Off Loitering Munition

The AIHMI SOLM (AHM-1X), is a special type of loitering munition with stand-off capability to launch a 2.75" (70mm) LASER Guided Rocket, thus, the designation SOLM (Stand Off Loitering Munition). The AIHMI can be launched from:

• The SARISA UCAV;
• Attack Helicopters, with a use of the ACP-1S (AIHMI Carrier Pod), equipped with NATO 14" suspension lugs, suitable for standard NATO pylons;
• SAS technology has also designed a special capability that allows any helicopter, even the ones not equipped with weapon pylons, to store multiple AIHMI within the cabin and launch one by one from the helicopter side door, using a special slider platform.
• The advanced AIHMI communication suite, that is customizable to the customer requirements, includes satcom communications allowing the control of AIHMI from command centers, without reliance on the carrier platform operators (Helicopter Crew).



ACP-1S AIHMI CARRIER POD

The Thales 275LGR, the AIHMI firing weapon, is a sophisticated LASER Guided Rocket system, (LGR) designed for precision strikes on the battlefield. It can be fired from a safe distance of up to 7 kilometers away from the target, minimizing exposure to enemy defenses. The AIHMI further enhances the LGR capabilities by extending its effective range to over 60 kilometers, depending on release altitude and other factors. This combination of long-range assault capability and LASER terminal guidance provides unparalleled tactical advantages to this integrated system, making it a formidable asset for military operations

Adapting to the Evolving Battlefield

Redefining Air Superiority

The widespread use of drones in these theaters, challenges traditional concepts of air superiority. While conventional aircraft remain essential, drones provide a complementary capability that can operate effectively in contested environments. This dual approach complicates enemy air defense strategies and offers commanders more tactical options.

Adaptability and Innovation

The experiences in recent operational theaters, underscore the importance of adaptability and innovation in military strategy. Leveraging commercially available technology, even smaller militaries and non-state actors can achieve significant operational advantages. This approach reduces dependence on high-cost, sophisticated systems and fosters a culture of innovation and resilience within the military.

Procurement, Training Practices and Continuous Innovation

The success of low-cost drones has, prompted a reevaluation of procurement and training practices. By nurturing local innovation and manufacturing capabilities and fostering balanced technological collaboration among allies, the alliance can harness a force multiplier effect. This collaborative effort will empower nations to lower their reliance on foreign suppliers and fortify a more resilient supply chain. Such an approach not only enhances military effectiveness but also bolsters domestic industries and propels technological advancement.The use of drones in the theater, highlights the necessity for continuous innovation in military operations. As drone technology evolves, military strategies must adapt to incorporate these advancements. This involves developing new doctrines, investing in research and development, and integrating drones into broader operational framework.

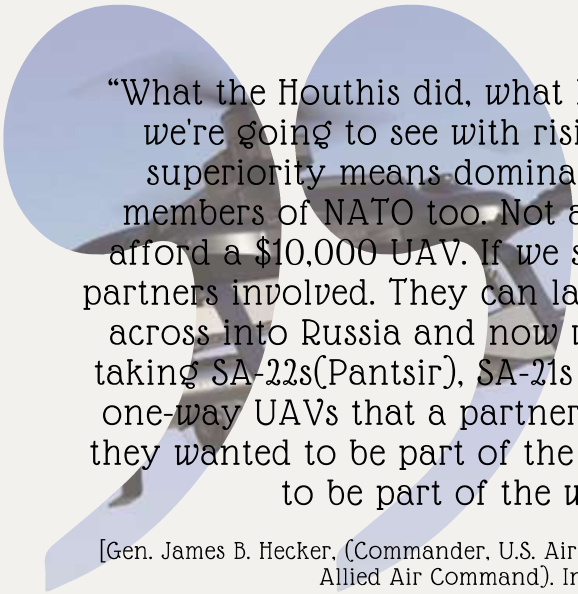
Critical to fostering the much-needed local advancement and innovation in drone technology is the establishment of suitable operational sandboxes within a flexible regulatory framework tailored to their specific needs. These sandboxes will enable uninterrupted testing and evaluation of systems, as well as the development of specialized tactics and training methodologies, involving operational entities. This collaborative approach will significantly enhance the operational effectiveness of the developed systems.

"The success of low-cost drones has, prompted a reevaluation of procurement and training practices."

Conclusion

The integration of low-cost, innovative drone solutions has redefined modern warfare, offering significant operational advantages in both offensive and defensive roles. By embracing these technologies and the lessons learned from recent conflicts, nations can better navigate the complexities of asymmetric warfare. Increasing self-sufficiency in the development and production of such systems, ensures a steady supply line to meet increased wartime demands. Cooperation between Allies in this emerging technological field, in a balanced and inclusive manner, would be a major force multiplier for the alliance. Adopting ECCM technologies in a cost-effective way maintains affordability and scalability. Establishing operational sandboxes under proper regulatory frameworks is essential for ongoing testing, tactics development, and comprehensive training.

The applications of drone technology in military strategy will undoubtedly continue to expand, presenting ever evolving threats, but also offering new opportunities to enhance operational effectiveness and achieve strategic objectives.



“What the Houthis did, what Russia's doing, is nothing compared to what we're going to see with rising threats across the world. Retaining air superiority means dominating domain awareness, and that goes for members of NATO too. Not all of them can afford F35s but they can all afford a $10,000 UAV. If we start doing the same thing, we'll get 15 other partners involved. They can launch and put a bunch of these, if we have to, across into Russia and now we can empty their magazines where they're taking SA-22s(Pantsir), SA-21s (S-400), and 23s (S-300) going after $10,000 one-way UAVs that a partner produced and it cost us no money, because they wanted to be part of the war. And now we just found a way for them to be part of the war and really part of deterrence”

[Gen. James B. Hecker, (Commander, U.S. Air Forces in Europe; Commander, U.S. Air Forces Africa; Commander, Allied Air Command). Interview, 21 Feb 2024, AFA Warfare Symposium]

By analyzing publicly available information and SAS Technology’s proprietary information, this paper provides a comprehensive analysis of the strategic implications and lessons learned from the innovative use of low-cost drones in recent operational theaters.

about the author

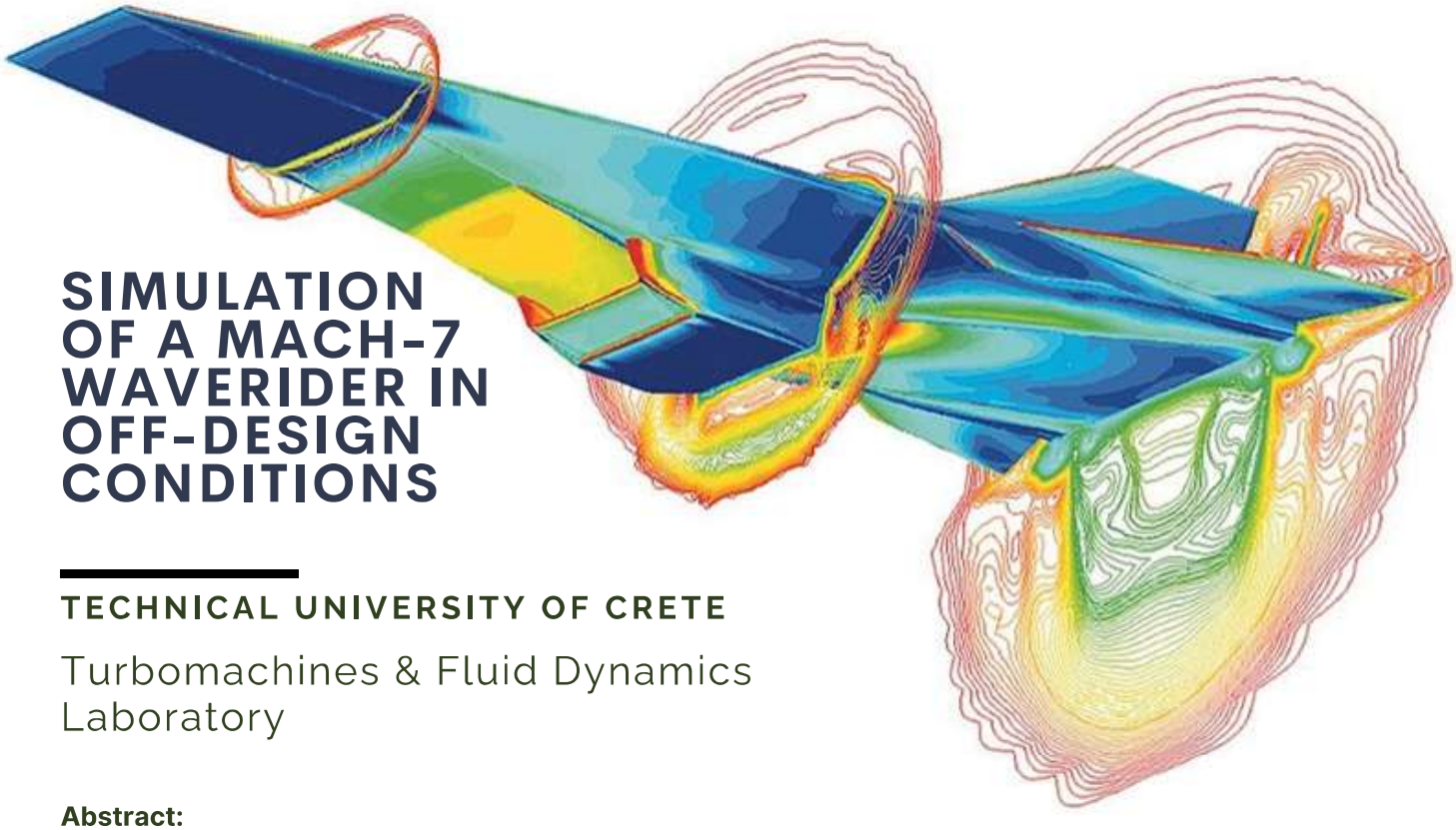
Fotios Kampiotis
Emerging Capabilities for Small Tactical UCAVs and Loitering Munitions.

Aeronautical Engineer (Hellenic Air Force Academy).

• Br. General (ret) of the Hellenic Air Force with 31 years of service 1981-2012 including service in command and technical management positions at all levels.

• Three-year service (2013-2015) as Quality Manager in a multinational MRO Aircraft company in the UAE. (AMMROC, a Lockheed - Sikorsky - Mubadala Military MRO Consortium).

• Nine-year (2015-present) experience in the design and manufacturing of unmanned systems,



SIMULATION OF A MACH-7 WAVERIDER IN OFF-DESIGN CONDITIONS

TECHNICAL UNIVERSITY OF CRETE

Turbomachines & Fluid Dynamics Laboratory

Abstract:
This study investigates the performance of a Mach-7 waverider under off-design conditions through detailed simulations.
Two distinct off-design scenarios were analyzed, revealing that the waverider maintained robust aerodynamic performance, despite the deviations from optimal conditions.
The simulations employed advanced computational fluid dynamics (CFD) techniques to evaluate the aerodynamic efficiency of the vehicle. Results indicated that the waverider performed admirably, without severe losses in aerodynamic efficiency.
These findings underscore the resilience and adaptability of the waverider design, providing valuable insights for future hypersonic vehicle development and operational flexibility.

Introduction

The waverider is a prominent concept in hypersonic vehicle design, known for its superior aerodynamic efficiency at high speeds. Originally conceived in the 1960s [1], waveriders leverage shockwave structures to produce lift, minimizing drag and enhancing overall performance. These characteristics make them ideal candidates for applications such as hypersonic reconnaissance, rapid transportation, and spaceplane operations. The focal point of this study is the simulation of a Mach-7 waverider in off-design conditions, a critical aspect given the practical operational environments where deviations from ideal flight parameters are inevitable. Hypersonic flight presents unique challenges, including extreme aerodynamic heating, high dynamic pressures, and complex shockwave-boundary layer interactions. Designing vehicles capable of maintaining performance in such regimes necessitates robust simulation and analysis techniques.

While significant research has been conducted on waverider performance at design conditions [2, 3, 4, 5], there is a relative paucity of data on their behavior under off-design scenarios. This gap is particularly significant given that real-world operations seldom adhere strictly to optimal flight conditions. Hence, understanding the performance of waveriders in off-design conditions is crucial for their practical application and reliability.

In this work, we focus on a Mach-7 waverider, a vehicle designed for sustained flight at seven times the speed of sound. The choice of Mach 7 is pertinent, as it represents a critical regime in hypersonic travel, balancing technological feasibility and performance demands. The study aims to simulate the waverider's performance in distinct off-design conditions, providing insights into its aerodynamic behavior and potential adaptability. The off-design conditions examined in this study involve variations in altitude and angle of attack.

The waverider was originally designed for an altitude of 90 km, optimized for this specific high-altitude environment to achieve maximum aerodynamic efficiency. The first off-design condition simulates flight at an altitude of 45 km and a speed of Mach 6.2. Under these conditions, the calculated lift-to-drag (L/D) ratio was found to be less than one, indicating a significant deviation from optimal performance. This scenario helps us understand the waverider's performance in a mid-altitude environment where atmospheric density is higher and the aerodynamic forces differ markedly from the design specifications. The second off-design condition examines flight at an altitude of 30 km with a 2-degree angle of attack and a speed of Mach 6. In this case, the L/D ratio was computed to be 1.463. This scenario provides insights into the vehicle's performance at a lower altitude, with a small deviation in the angle of attack, simulating a realistic operational condition where slight adjustments in flight parameters are necessary.

To conduct these simulations, we employ advanced computational fluid dynamics (CFD) tools, leveraging high-fidelity models to capture the complex interactions between the waverider and the hypersonic flow field. CFD has become an indispensable tool in hypersonic research, offering detailed insights into flow phenomena that are often challenging to measure experimentally. Our simulations provide a comprehensive analysis of aerodynamic forces, pressure distributions, and thermal loads under off-design conditions. The simulations for the 90 km altitude, where the atmosphere is rarefied, were conducted using the DSMC solver SPARTA [6] while simulations for the off-design altitudes were conducted using SU2 solver [7]. By exploring the performance of a Mach-7 waverider in off-design conditions, this work aims to bridge the knowledge gap in hypersonic vehicle behavior under non-ideal scenarios. The insights gained from this study are expected to inform the design and operation of future hypersonic vehicles, enhancing their robustness and operational flexibility in practical applications.

Results

This section presents the outcomes of the computational simulations conducted to evaluate the performance of the waverider under the aforementioned off-design conditions. More specifically, the study focuses on two different altitudes, 45 km and 30 km, and variations in angle of attack at Mach 6. These off-design conditions were chosen to assess the vehicle's aerodynamic and thermal behavior in environments deviating from its optimal design altitude of 90 km.

The simulations provide comprehensive insights into the Mach number distribution, pressure and temperature fields, turbulent viscosity, and heat flux around the waverider, elucidating its adaptability and performance robustness under these challenging scenarios.

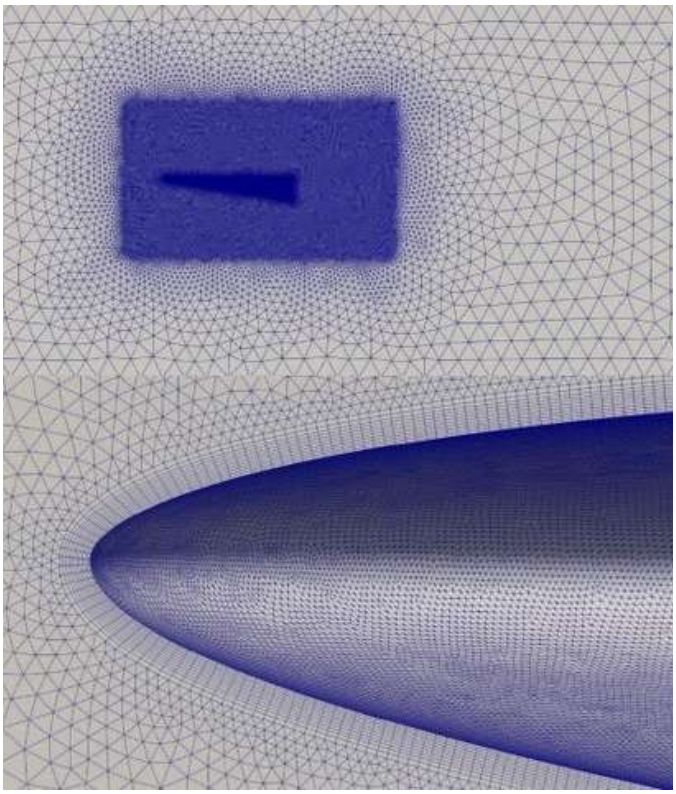


Figure 1. Computational grid overview.

Figure 1 provides an overview of the computational grid used for the simulations. A very dense surface grid was constructed on the vehicle's solid surface to allow for a detailed description of the geometry and the accurate simulation of the related flow phenomena.

The unstructured (hybrid) computational grid comprises of 54,484,085 elements and 15,732,524 nodes. While solving the Navier-Stokes equations requires fewer computational resources compared to the Direct Simulation Monte Carlo (DSMC) method, it is not without significant challenges. Solving the extended Navier-Stokes equations to accommodate reacting flows in thermochemical non-equilibrium conditions at high Mach numbers is particularly demanding. These equations form a complex system of interconnected nonlinear partial differential equations (PDEs), and their iterative solution can present numerous convergence issues. Consequently, multiple attempts may be necessary to achieve a converged solution.

Figure 2 depicts the velocity magnitude on the symmetry plane (top) and Mach number contours (bottom) at a plane parallel to the vehicle, for an altitude of 45 km. The contours highlight the flow acceleration around the waverider, with a clear visualization of the shockwaves formed at the leading edges. The Mach number distribution indicates significant deceleration as the vehicle interacts with the denser atmosphere at this altitude. The interaction with the denser atmospheric layers results in more intense shockwave-boundary layer interactions, which are critical for understanding the aerodynamic performance under these conditions.

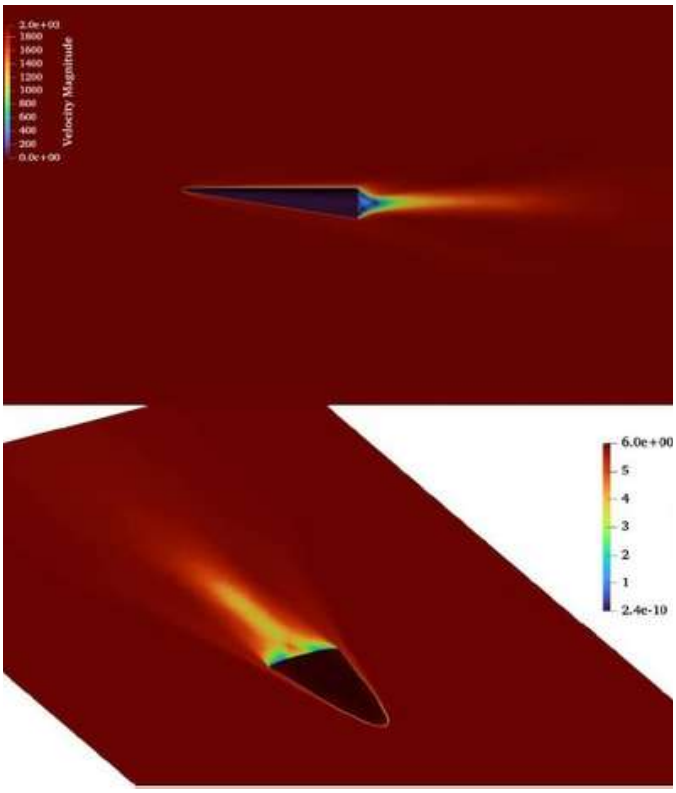


Figure 2. Velocity and Mach number contours, at an altitude of 45 km.

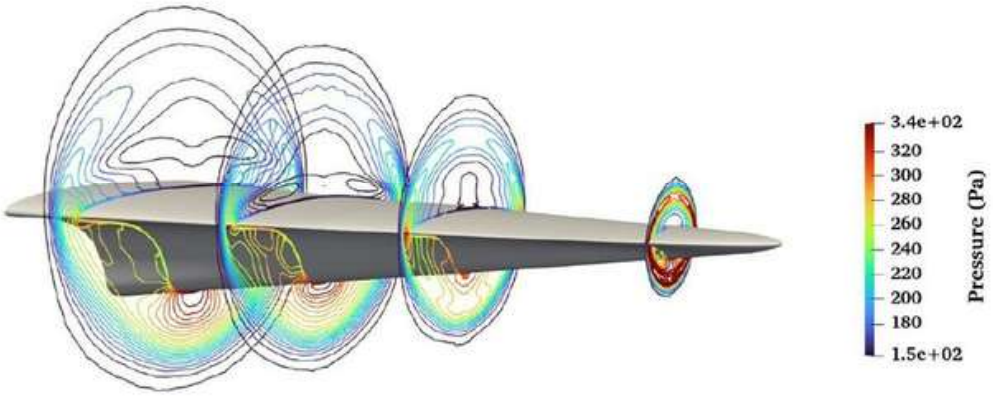


Figure 3. Contours of static pressure at various planes normal to the symmetry plane at an altitude of 45 km.

Complementing the Mach number contours, **Figure 3** shows the static pressure contours at various planes normal to the symmetry plane at an altitude of 45 km. These contours illustrate the pressure distribution around the vehicle, revealing high-pressure regions at the lower surfaces. This pressure differential is essential for generating lift and maintaining aerodynamic stability. The pressure gradients observed are indicative of the intense aerodynamic forces acting on the vehicle, which are critical for ensuring its structural integrity during high-speed flight.

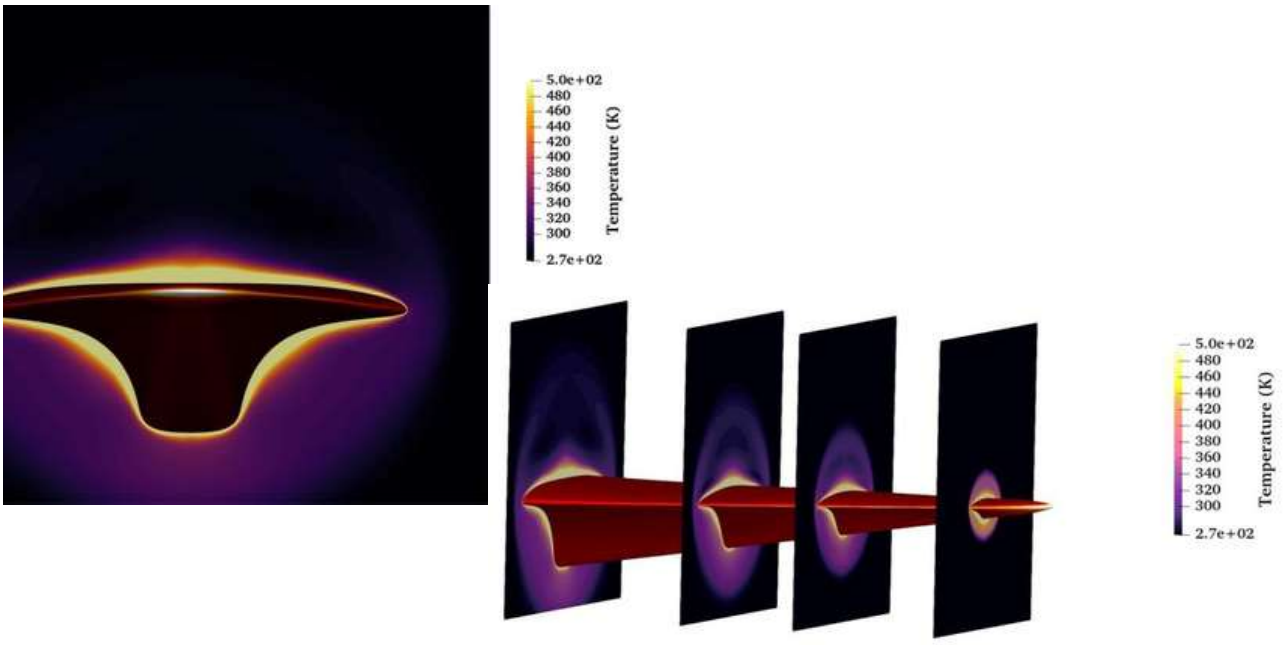


Figure 4. Temperature field around the vehicle at different planes normal to the vehicle's axis (top) and at a plane normal to the vehicle's axis, at an altitude of 45 km.

Further details of the thermal environment are captured in **Figure 4**, which depicts the temperature field around the vehicle at different planes normal to the vehicle's axis (top) and at a plane normal to the vehicle's axis, at an altitude of 45 km. The temperature distribution is crucial for understanding the thermal loads experienced by the waverider. The results show significant heating near the leading edges and lower temperatures in the wake regions, consistent with shockwave heating effects.

Expanding on this, **Figure 5** offers a volumetric three-dimensional rendering of the thermal trace at 0.0 degrees angle of attack at an altitude of 45 km. This perspective view provides a comprehensive visualization of the thermal footprint of the waverider, highlighting regions of intense heating and the overall thermal environment surrounding the vehicle. This volumetric rendering is particularly useful for identifying hotspots and understanding the overall heat distribution patterns, which are critical for effective thermal management.

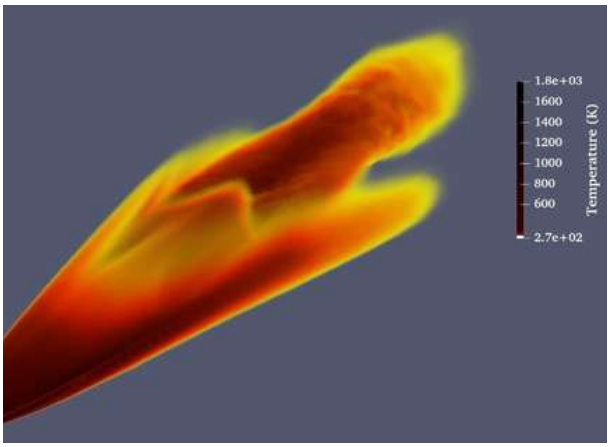


Figure 5. Volumetric three-dimensional rendering of the thermal trace at 0.0 AoA, at an altitude of 45 km (perspective view).

Transitioning to a lower altitude, **Figure 6** illustrates the Mach number contours at an altitude of 30 km on the symmetry plane (top) and a plane normal to the vehicle's axis. The contours at this lower altitude show a similar pattern of shockwave formation and flow deceleration, but with more pronounced effects due to the increased atmospheric density. This increased density at lower altitudes results in stronger shockwaves and higher aerodynamic heating, which are key considerations for vehicle performance and thermal protection.

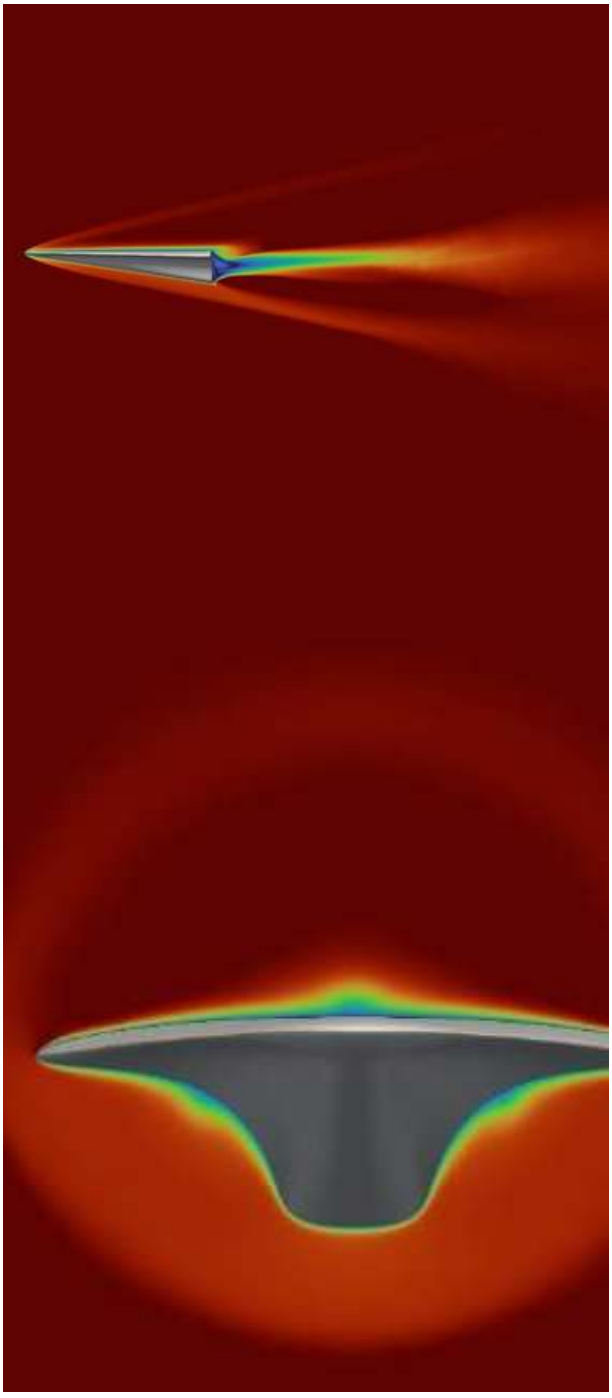


Figure 6. Mach number contours at an altitude of 30 km on the symmetry plane (top) and at a plane normal to the vehicle's axis.

Figure 7 combines the visualization of turbulent viscosity downstream with the pressure distribution around the vehicle at a plane normal to the vehicle's axis, at an altitude of 30 km. This combined view provides insights into the interaction between pressure forces and turbulent effects, which are critical for vehicle stability and control.

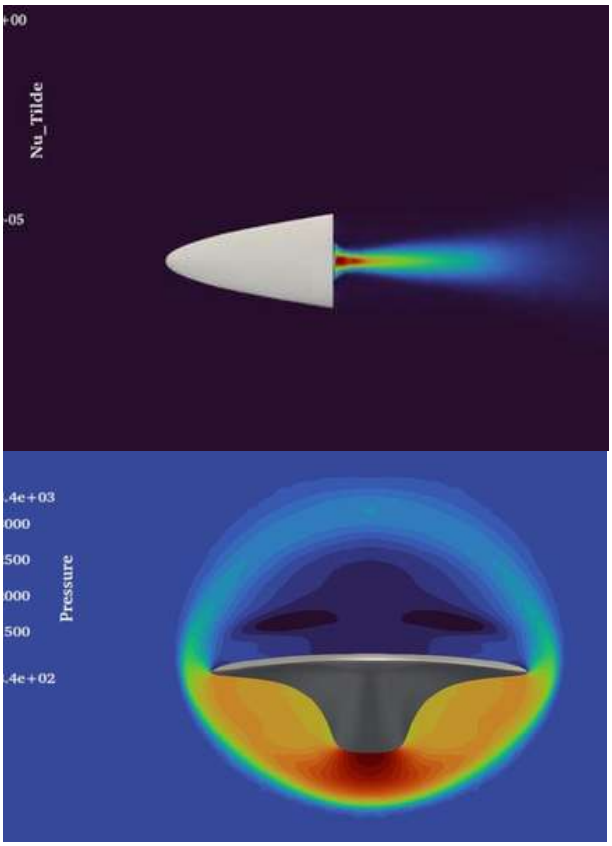


Figure 7. Turbulent viscosity downstream (top), and pressure distribution around the vehicle, at a plane normal to the vehicle's axis (altitude 30 km).

To further assess the aerodynamic forces acting on the waverider, **Figure 8** depicts the pressure contours on the vehicle's surfaces, at an altitude of 30 km. This detailed pressure mapping helps in optimizing the aerodynamic design for enhanced performance and efficiency.

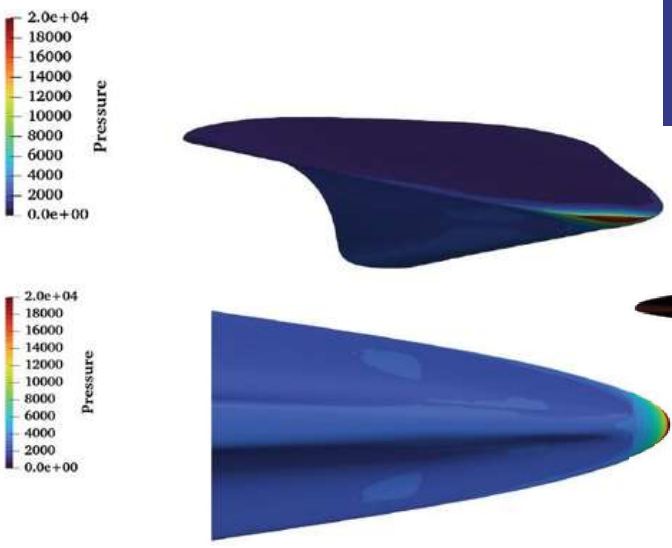


Figure 8. Pressure contours on the vehicle's surfaces (altitude 30 km).

To understand the thermal stresses experienced by the vehicle, Figure 9 depicts the temperature distribution at the symmetry plane, while Figure 10 illustrates the heat flux distribution at the symmetry plane, at an altitude of 30 km. These figures highlight the thermal gradients experienced by the vehicle, with significant heating occurring near the stagnation points and cooler regions in the vehicle's wake. This distribution is critical for understanding the thermal protection requirements for the waverider. Effective thermal management is essential to prevent structural damage, due to high-temperature exposure. The colormap has been adjusted for clarity, with the maximum heat flux value recorded as 255.376 kW/m². The highest temperature occurs around the vehicle's nose, reaching a maximum temperature of 1910.82 K. The minimum temperature observed at the back surface of the vehicle is approximately 1200 K, reflecting the thermal complexity of the flow field. Accurate heat flux and temperature predictions are vital for developing materials and coatings that can withstand the extreme thermal environment of hypersonic flight and support the thermal management.

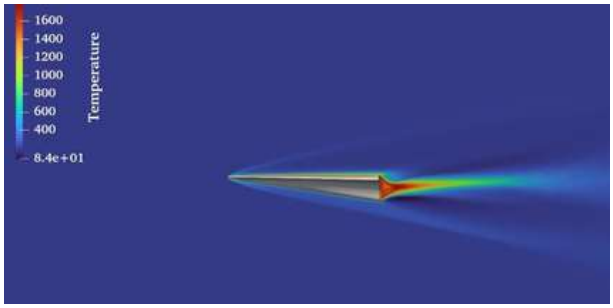


Figure 9. Temperature distribution at the symmetry plane (altitude 30 km).

Figure 10. Heat flux distribution on the surface (altitude 30 km).

Conclusions

This study investigated the performance of a Mach-7 waverider under off-design conditions through detailed computational simulations. By examining the aerodynamic and thermal behavior of the waverider at altitudes of 45 km and 30 km, and varying the angle of attack at around Mach 6, we have gained valuable insights into the vehicle's robustness and adaptability in non-ideal operational environments. The simulations revealed that the waverider maintains significant aerodynamic efficiency even when operating outside its design altitude of 90 km. The detailed analysis of Mach number distributions, pressure and temperature fields and heat flux provided a comprehensive understanding of the vehicle's performance under different conditions. Notably, the pressure and thermal gradients observed highlight the critical areas requiring attention for structural integrity and thermal protection.

Future work will focus on enhancing the fidelity of the simulations by incorporating chemical reactions and non-equilibrium effects. These factors are crucial for accurately predicting the behavior of hypersonic vehicles in realistic operational environments. By addressing these additional complexities, we aim to further refine our understanding of waverider performance and contribute to the development of more resilient and efficient hypersonic technologies.

Acknowledgements

This study was funded by the Integrated Air and Missile Defense Centre of Excellence (IAMD COE) under contract number 22-10 “Analysis of the related Physical Phenomena and Aerodynamic Performance of Hypersonic Vehicle(s) and possible ways of exploiting those data in order to improve Surveillance Capabilities”. The authors would also like to thank the UKTC and EPSRC for computational time on the UK supercomputing facility ARCHER2 via project EP/R029326/1.

Dr. Ioannis K. Nikolos
Mechanical Engineer

Dr. Ioannis K. Nikolos, Mechanical Engineer, is a Professor with the School of Production Engineering & Management, Technical University of Crete, Greece and Director of the Turbomachines & Fluid Dynamics Laboratory (TurboLab – TUC). He has more than 30 years of experience in R&D projects funded by the EU, the Industry, and the Greek State. He has coordinated 41 R&D Projects, while he participated as a researcher in 13 additional ones. His research work is in the fields of Computational Fluid Dynamics, Fluid Dynamics, Turbomachinery, Computational Engineering, Engineering Design Optimization, and Traffic Flow Modelling. He has co-authored one patent family, three books, 61 journal papers and book chapters, 112 conference papers and 16 posters. His work attracted more than 3400 citations. He is a member of ASME, AIAA, and IEEE

Angelos G. Klothakis
Producton Engineering & Management

Angelos G. Klothakis was born in Chania, Greece in 1985. He successfully finished his undergraduate studies in the School of Producton Engineering & Management, Technical University of Crete, Greece, in 2010 and his postgraduate studies in Producton Systems, in the same School, in 2015.

He is currently working for his Ph.D. Thesis in the same School, enttled “On the solution of high Mach number flows”. He has been a researcher since 2020 in a joint research project entitled "Mult-scale Modeling of Unsteady Shock-Boundary Layer Hypersonic Flow Instabilities," funded by the Office of Naval Research (ONR) and conducted by the University of Illinois at Urbana Champaign.

Comparative Analysis of System Architectures for Passive Radars in Drone Detection – The AIRE5G Project

Abstract:
Drone detection poses significant challenges, especially in complex aerial warfare scenarios. Traditional methods rely on dedicated, high-cost transmitters, but passive radar systems (PRS) offer a promising alternative due to their cost-effectiveness, low power consumption, and resilience to electronic warfare.
Leveraging signals from existing infrastructure such as cellular networks and DVB broadcasts, PRS have garnered attention for their potential in drone surveillance. Our research delves into the comparison of system architectures, specifications, and requirements for PRS tailored to drones, focusing on the utilization of reflected 4G/5G signals and DVB broadcasts.

We examine the implications of these signal sources on detection range, accuracy, and robustness in diverse operational environments. Furthermore, we provide insights for the development of an efficient and adaptable drone detection system in complex operational landscapes, through the integration of deep learning techniques and software-defined radio technologies, as part of the AIRE5G project.

1. Introduction

The advent of drones has revolutionized various sectors, from commercial deliveries to critical military operations. However, this technological advancement has also introduced significant challenges, particularly in the realm of aerial warfare and security. Detecting and tracking these small, agile, and often low-flying objects is a complex task that has traditionally relied on dedicated high-cost transmitters. While effective, these systems are not without their drawbacks, including high power consumption and susceptibility to electronic warfare tactics. In this context, passive radar systems (PRS) have emerged as a promising alternative, offering a cost-effective and resilient solution to the problem of drone detection.

Passive radar systems operate by utilizing ambient signals from existing infrastructure, such as cellular networks and digital video broadcasting (DVB). This approach not only reduces the overall system cost but also enhances the stealth and survivability of the detection system, as it does not emit any signals that could be intercepted or jammed by adversaries. The potential of PRS to leverage 4G/5G signals and DVB broadcasts has garnered considerable interest, particularly for applications in drone surveillance. These signals, ubiquitously present in modern environments, provide a rich source of data for detecting and tracking drones without the need for additional transmitters.

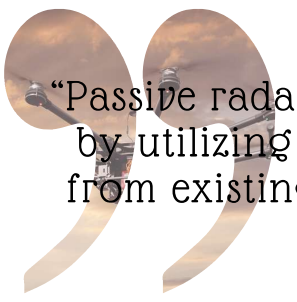
Our research focuses on the comparison of different system architectures and the specific requirements needed to tailor PRS for effective drone detection.

By examining the utilization of active sources (in the case of active radars) or reflected signals from 4G/5G cellular networks (in the case of passive radars), we aim to evaluate the impact of these signal sources on critical performance metrics such as detection range, accuracy, and robustness in various operational environments. This comparative analysis is crucial for identifying the most suitable configurations and technologies that can enhance the effectiveness of PRS in real-world scenarios.

In addition to evaluating the technical specifications, our study explores the integration of advanced technologies like deep learning and software-defined radio (SDR) to further augment the capabilities of PRS. Deep learning techniques offer powerful tools for signal processing and pattern recognition, which are essential for improving detection accuracy and reducing false positives.

Meanwhile, SDR provides the flexibility to adapt and optimize the radar system in response to dynamic operational requirements. Together, these technologies form the backbone of the AIRE5G project, fully funded by the IAMD COE, which aims to develop an efficient and adaptable drone detection system for complex operational landscapes.

Through this research, we seek to provide comprehensive insights into the development of next-generation passive radar systems for drone detection. By leveraging the synergies between existing communication infrastructure and cutting-edge technological advancements, we aim to pave the way for robust and resilient drone surveillance solutions. Our findings will contribute to the broader field of radar technology and offer practical implications for enhancing security and operational efficiency in both military and civilian contexts.



“Passive radar systems operate by utilizing ambient signals from existing infrastructure”

2. Role of Drones in Modern Warfare

Drones have become integral to modern warfare, significantly enhancing operational efficiency and reducing human risk. By utilizing unmanned aerial vehicles (UAVs) for tasks traditionally carried out by manned aircraft, military forces can conduct operations more swiftly and with greater precision. This increased efficiency is particularly evident in logistics, where drones can transport supplies and equipment to remote or hostile areas without the delays and vulnerabilities associated with ground convoys. Furthermore, the deployment of drones minimizes the exposure of military personnel to dangerous environments, thereby reducing the risk of casualties. This shift not only preserves human lives but also allows for more aggressive and sustained operational strategies.

Another critical advantage of drones in modern warfare is their capability for autonomous operations. Advanced drones equipped with artificial intelligence and machine learning algorithms can execute complex missions with minimal human intervention. These autonomous systems can perform surveillance, reconnaissance, and even targeted strikes, adapting to real-time changes in the battlefield environment. The ability to conduct expanded surveillance and reconnaissance is particularly valuable, as drones can cover vast areas and gather intelligence without the need for extensive ground operations. This continuous, real-time data collection enhances situational awareness and informs decision-making processes, contributing to the overall effectiveness of military operations.

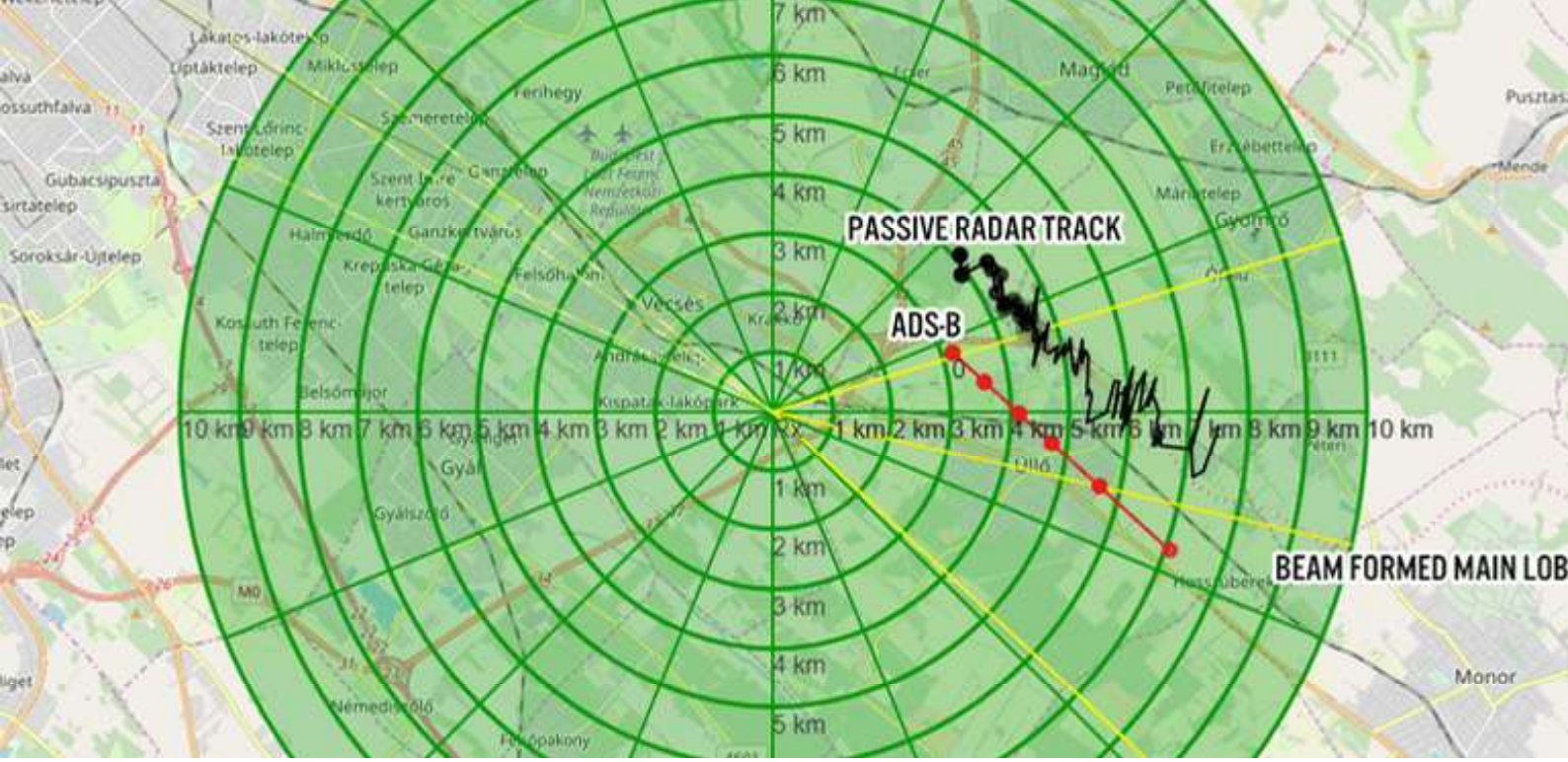
Drones also offer significant cost-effectiveness and act as a force multiplier in network-centric warfare. Compared to traditional manned aircraft, drones are relatively inexpensive to produce, maintain, and operate. This affordability allows for the deployment of larger fleets, increasing the breadth and depth of military capabilities. As force multipliers, drones enable smaller units to achieve the impact of much larger forces by providing critical support such as real-time data transmission, targeting information, and battlefield coordination. The integration of drones into network-centric warfare frameworks allows for seamless communication and coordination across various military assets, ensuring that commanders have access to the latest intelligence and can respond swiftly to emerging threats. This synergy of real-time data and networked operations significantly enhances the agility and effectiveness of modern military forces.

3. Drone Detection Technologies

Currently, there are four main technologies for drone detection, as briefly summarized below.
Radio Frequency (RF) Analyzers are a versatile and effective technology, leveraging the ability to intercept and analyze the communication signals between drones and their controllers. This method offers real-time detection and identification, making it particularly useful for monitoring and responding to unauthorized drone activity promptly. RF analyzers are relatively low-cost and can cover large areas, providing a significant advantage in diverse environments. They are also passive, thus they don't need any license to operate. However, their performance can be hindered in locations with high RF interference, which can lead to false positives or missed detections. Additionally, RF analyzers may struggle to detect drones utilizing encrypted communications or frequency-hopping techniques, which can mask the signals and complicate detection efforts.
Acoustic Sensors (Microphones) detect drones by capturing and analyzing the unique sounds produced by drone motors and propellers. These sensors are particularly advantageous in environments where RF and optical methods may fail, such as in urban areas with high signal clutter or poor visibility conditions like fog and darkness. Acoustic sensors can be deployed relatively inexpensively and can be effective in detecting low-flying drones. However, their effectiveness is limited by the range of sound propagation and can be significantly reduced in noisy environments where background noise may mask the drone's acoustic signature. Additionally, drones with quieter propulsion systems can evade detection by acoustic sensors, making them less reliable in certain scenarios. Optical Sensors (Cameras) provide high-resolution visual data for detecting and identifying drones, offering the benefit of visual confirmation, which can be critical for threat assessment and response. These sensors excel in well-lit conditions and can be integrated with advanced image processing algorithms to enhance detection capabilities.
They are particularly useful for distinguishing between drones and other objects, ensuring precise identification. However, the effectiveness of optical sensors is heavily dependent on lighting and weather conditions; their performance diminishes significantly in low light, fog, rain, or when the line-of-sight is obstructed. This dependency on environmental factors can limit their reliability in various operational scenarios.
Finally, Active Radar systems are robust and reliable for drone detection, providing comprehensive coverage and the ability to measure the range, speed, and trajectory of detected objects. They can operate effectively in various weather conditions and over long distances, making them suitable for large-area surveillance. Active radar can penetrate through obstacles like foliage and maintain detection capabilities in challenging environments. However, these systems are typically high-cost, both in terms of initial setup and maintenance. Additionally, they are susceptible to electronic countermeasures such as jamming and spoofing, which can degrade their performance and reliability. The high power consumption and potential interference with other radar systems or communication devices are also considerations when deploying active radar technology.

4. The AIRE5G Project

Passive Radar systems (PRS) offer several advantages over the main drone detection technologies mentioned above. They operate by leveraging existing ambient signals, such as those from 4G/5G cellular networks and DVB broadcasts, making them highly cost-effective as they do not require dedicated transmitters.
This reliance on pre-existing signals also means passive radars have low power consumption and are less detectable, enhancing their resilience to electronic warfare tactics like jamming and spoofing.



Unlike optical sensors, passive radars are not affected by lighting conditions, and unlike acoustic sensors, they are not hampered by environmental noise. Furthermore, passive radars provide extensive coverage and can detect drones over long distances and through various obstacles, offering a more robust and stealthy solution for comprehensive drone surveillance.
The integration of Artificial Intelligence (AI) in the design of passive radars can revolutionize the industry by significantly enhancing detection capabilities and operational efficiency. AI algorithms, particularly those in machine learning and deep learning, could enable passive radar systems to analyze vast amounts of signal data more accurately and quickly, improving the identification and tracking of drones amidst complex and noisy environments. This intelligent processing allows for real-time adaptation and optimization of radar performance, reducing false positives and increasing the reliability of detections. As a result, AI-powered passive radars can become more adept at handling the dynamic and diverse challenges of modern drone surveillance, making them an increasingly valuable asset in security and defense applications.

Motivated by these challenges, the Signal Processing Lab (SPL) and the Telecommunications & Networks Lab (TNL) at FORTH-ICS are jointly focusing on designing and developing an innovative AI-empowered PRS for drone detection in the framework of the AIRE5G project, which is fully funded by IAMD COE. This effort leverages deep learning computational tools and ubiquitous 5G networks. The urgency to address drone detection stems from several factors: the anticipated exponential increase in drone numbers in the coming years, their potential use for malicious (intentional or unintentional) purposes, and the critical need for early detection. Unlike typical radar targets, drones exhibit unique characteristics such as higher mobility, lower altitude flight, greater degrees of freedom (DoF), smaller form factors (size, shape, and other physical specifications), and operation in complex environments with numerous obstacles and non-line-of-sight conditions.

The design of AIRE5G's PRS will address specific key challenges. Achieving a high signal-to-noise ratio (SNR) is critical for clear and easy detection of signals, yet in many real-world scenarios, the SNR is low, with signals corrupted or obscured by noise, making them difficult to distinguish or recover. Additionally, the radar cross-section (RCS) of detected objects varies widely, complicating detection. Stealth objects, such as certain drones, are designed with low RCS features like absorbent paint and complex surfaces to minimize their detectability. Balancing our PRS's sensitivity to effectively detect both low RCS stealth objects and high RCS conventional aircraft across varying ranges and environments is a complex task requiring sophisticated signal processing and advanced detection algorithms.

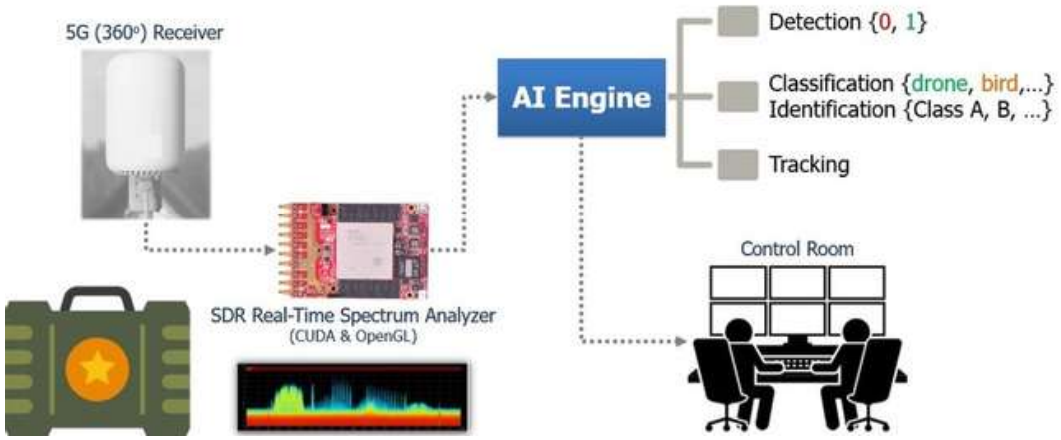


Figure 8. Pressure contours on the vehicle's surfaces (altitude 30 km).

4.1 AIRE5G's PRS Architecture

Figure 1 illustrates the high-level architecture of AIRE5G's PRS for drone detection. Specifically, the 5G signals reflected by the objects (including drones) in the monitored environment are first recorded by a 5G (360°) receiver, which captures 5G signals from all directions. The receiver's output is fed to a software-defined radio (SDR) Real-Time Spectrum Analyzer built in-house by TNL.

The spectral signatures generated by the SDR are collected in a database, which is connected with our AI engine, integrating powerful deep learning models for analyzing complex data. The AI module is responsible for performing high-level tasks, including detection (determines the presence of objects and outputs a binary result, 0 or 1), classification (distinguishes between different types of objects (e.g. drone, bird)), identification (categorizes objects into specific classes (Class A, B, etc.)) and tracking (monitors the movement of detected drones).

Finally, the processed information is sent to a Control Room, where operators view and manage the output from the AI engine, making informed decisions based on the processed data. We emphasize that our system architecture is modular enough allowing for the replacement of our trained AI models by improved learning models that may arise in the future, without affecting the remaining system components.

4.2 Key Advantages

The AIRE5G drone detection PRS offers a software-defined solution, ensuring flexibility and adaptability to evolving technological landscapes. This architecture allows for easy upgrades and futureproofing, enabling the integration of new features and improvements without significant overhauls.

As a white-box solution, it provides full access to the modules' architecture, granting users transparency and control over the system's inner workings. The inclusion of state-of-the-art machine learning (ML) and deep learning (DL) models enhances detection accuracy and efficiency. Moreover, the system features a self-training option, empowering end-users to customize and optimize the models based on their specific operational environments. Its design supports scalability to handle multi-modal data, ensuring comprehensive coverage and analysis.

Furthermore, the system is designed for interoperability with existing military systems, facilitating seamless integration and coordination within established defense frameworks.

5. Conclusions

The AIRE5G's drone detection PRS represents a significant advancement in surveillance technology, when compared against existing solutions, offering a flexible and adaptable software-defined approach. Its architecture facilitates easy upgrades and futureproofing, allowing the system to evolve with emerging technological trends.

The white-box nature of the solution ensures transparency and full access to the modules' architecture, giving users complete control and understanding of the system. Utilizing state-of-the-art machine learning (ML) and deep learning (DL) models, the system achieves high detection accuracy and efficiency.

Additionally, the inclusion of a self-training option enables end-users to tailor the models to their specific operational environments, further enhancing performance.
Designed with scalability in mind, the system can handle multi-modal data, providing robust and comprehensive surveillance capabilities.

Its interoperability with existing military systems ensures seamless integration and coordination within established defense frameworks. This comprehensive approach, combining advanced technology with user-centric features, positions the system as a future-ready solution for effective and reliable drone detection in various operational scenarios.

about the author

Dr. George Tzagkarakis
Scientific Data Analyst

Dr. George Tzagkarakis is a Scientific Data Analysis professional with more than 15 years of experience in processing and analyzing multimodal data. He holds a PhD and MSc degree in Computer Science (1st in class, highest honors) from the University of Crete, Greece [with a major in Statistical Signal Processing], a PhD degree in Management Science from the University of Bordeaux, France [with a major in Risk Quantification], and a BSc in Mathematics (1st in class, highest honors) from the University of Crete, Greece [with a major in Applied and Computational Mathematics].

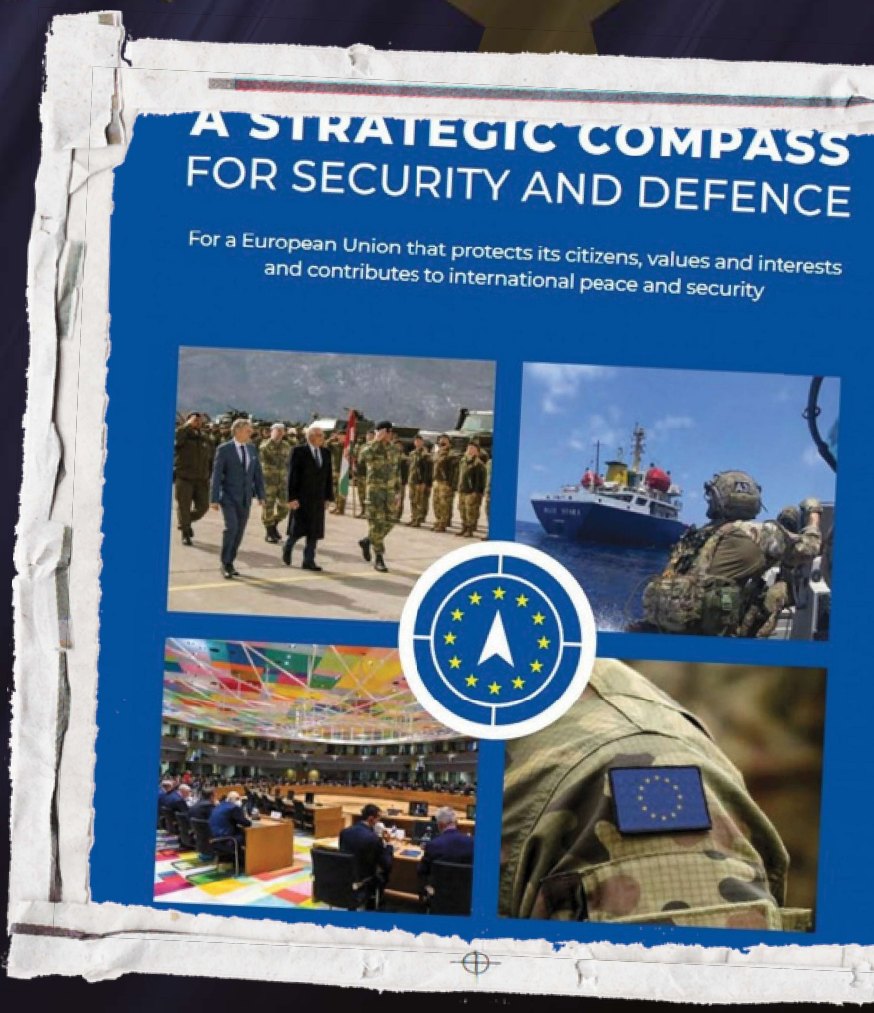
THE RENEWED APPROACH
OF THE EU TO SECURITY AND DEFENCE IN THE AIR DOMAIN

Background

During the last years, the EU leaders have become more cognizant of the need to take resolute action to protect the security of its citizens, to act in crises that affect the EU's interests and to develop itself as a stronger and more capable actor in security and defence.

This renewed mindset was codified in the Strategic Compass, approved in March 2022, where a comprehensive strategy for EU security and defence for the next decade is commonly outlined.

This document emphasizes the need for swift action in crises, securing strategic domains, investing in necessary capabilities and fostering partnerships. In this respect, the critical role of the air domain is deeply underscored throughout the Compass, codifying an EU transformed approach to address the challenges and threats in this relevant domain.



In parallel with the adoption of the Compass, EU leaders met in Versailles and reinforced the political impetus for this renewed ambition in security and defence, in particular, agreeing to bolster defence capabilities and reduce energy dependencies.

As a result, the Commission and the High Representative published a Joint Communication on the Defence Investment Gaps Analysis and Way Forward only two months after the Versailles Summit.

In this communication, the EU institutions take a step forward to foster collaborative capability development and joint procurement, committing to invest better, together and European. Within the most urgent need identified in this gap analysis, the reinforcement of the Air and Missile Defence systems of Member States and the development and procurement of counter drone-capabilities, received prominent attention.

THE RELEVANCE OF THE AIR DOMAIN WITHIN EU'S APPROACH TO SECURITY AND DEFENCE

In addition to the efforts in the field of air capability development and joint procurement, the Strategic Compass brings forward additional taskings related to the air domain. The war in Ukraine serves as a heads up call for many EU political leaders, demonstrating one more time the pivotal role that the control of the air has in wartime, and making evident that it would have been impossible to deliver all the European support to Ukraine, should Russia had achieved air superiority over the area of operations.

The two main deliverables related to the air domain that stem from the Compass were: the elaboration of a new conceptual framework for air operations on Common Security and Defence Policy and the development of the so called Strategic Reflection on the need to ensure free, safe and secure European access to airspace.

While the revision of the Air Operations Concept remains at a doctrinal level, similar to an Allied Joint Publication, the Strategic Reflection offered Member States a deeper and broad analysis of the threats and challenges in the air domain, inside and outside the EU, and how the EU can respond and be better prepared to cope with them.

In order to provide a comprehensive analysis, a deep collaborative work between the EU Institutions was conducted, integrating all the relevant civil and military actors with responsibilities in the air domain.

In this respect, the Strategic Reflection concentrates on three main questions:

- How can we ensure seamless access to European airspace for security and defence purposes?
- How can we make the best use of EU tools to contribute to the protection of EU airspace?
- How to improve European access to airspace outside the Union, in the context of Common Foreign and security Policy?

To address these questions, the need to avoid unnecessary duplications with NATO and the respect of the specific character of the security and defence policy of each nation, remain key conditions.

Concerning the potential contribution from the EU to the protection of the airspace, it is indispensable to converge to the problem in a comprehensive manner, addressing all types of threats that could be faced, looking for real added-value from the EU that could complement Member States as well as NATO efforts.

In this respect and thanks to the integrated approach, the EU is perfectly placed to coordinate efforts in different fields, not only the military.

For instance, the regulatory frameworks elaborated within the EU can ensure that security and defence considerations are taken into account, in particular in the context of new entrants, such as drones or High Altitude Operations. Likewise, stronger civil-military cooperation will be required to ensure the availability of larger volumes of airspaces for the military, from peacetime to crises.

EU financial instruments can also support civilian and military security and defence needs in a coherent manner, promoting interoperability and supporting a strong and competitive European defence technological and industrial base (EDTIB). The capacity of the EDTIB to deliver to Member States' armed forces the defence capabilities they require, when needed and in the volumes needed, is essential. More broadly, the European defence industry is a crucial contributor to the resilience, preparedness and security of the Union and its Member States.

EU programmes and instruments, such as the European Defence Fund (EDF) to support research and development, the European defence industry reinforcement through common procurement act (EDIRPA) to stimulate joint procurement, and finally the Act in Support of Ammunition Production (ASAP) to ramp up the production of ammunition, have proven the EU capacity and commitment to serve the EU's need in defence, even in cases of extreme urgency.

However, establishing the structural conditions of the EU's defence industrial readiness is paramount to make it responsive on the long run. To that end, the recently delivered European Defence Industry Strategy (EDIS) and the associated European Defence Industry Programme (EDIP) will create the conditions for the EU's defence industry to meet Member States' demand over time and in sufficient scale, through a wide range of tailored measures.

Furthermore, civil-military cooperation and interoperability will be essential in fields such as countering drones, where military and law enforcement actors must closely cooperate to exchange information and develop common capabilities. In this regard, the EU is putting forward several initiatives to support Member States capabilities in countering the threat posed by drones.

Additionally, EU political and diplomatic action can also be exerted to respond to the more frequent hybrid actions in the air domain. Similarly, cooperation programmes can be adapted to support aeronautical capacity building of partners, which in turn could benefit our assets when operating in those regions in case a crisis erupts and the EU is called to act.

Moving forward – towards an EU airspace strategy for security and defence

Looking ahead, the EU is committed to take a more active role in the air domain. Based on the analysis and recommendations made in the strategic reflection and due to the worrisome geostrategic context, Member States have agreed to develop a dedicated airspace strategy for security and defence, to be adopted in 2025, complementing the EU action in securing strategic domains. The EU already has strategies and policies for the other strategic domains (i.e. space, cyber, and maritime), therefore, an airspace strategy will complement the wider EU policy framework, acting as the missing puzzle piece in this framework.

Building on the work carried out within the strategic reflection, the strategy will go one step further. This work will help to provide political overarching direction and guidance to steer ongoing and future initiatives in the air domain, leveraging the wide array of tools at EU disposal – some of them mentioned previously in the text - in a coherent, comprehensive and consistent manner.

The new airspace strategy will help EU and Member States to identify areas of focus, prioritize resources and put forward concrete actions to add real value, without duplicating efforts but looking at its own interests and needs and to fulfil its level of ambition. For that purpose, the EU institutions, tasked to take forward this work, will have to consult closely with EU Member States, key like-minded partners -in particular NATO - and relevant civilian stakeholders throughout the process.

At the end of the process, with the finalization of the airspace strategy for security and defence, the EU will have coherent strategies in all relevant domains that encompass both military and civilian interests and requirements, enhancing its ability to act in all domain, as ambitioned in the Strategic Compass.

about the author

Arturo Arribas
Lieutenant Colonel

Lieutenant Colonel Arturo Arribas was commissioned as an officer of the Spanish Air Force in 2003. During almost 13 years, he took numerous assignments in different Units, flying F-18 and Eurofighter platforms and taking responsibilities as test pilot, weapon's instructor, XO and finally, Squadron Commander.

During his career, LtCol Arribas has been deployed overseas in several occasions, participating in ISAF, NATO Baltic Air Policing and EUTM Somalia Mission. Concerning educational experience, he holds a master degree on international relations, a diploma from the International Studies Society in Madrid and several project-management courses.

HOW CAN WE CREATE THE MINDSET AND THE MEANS FOR MILITARY CAPABILITIES TO SYNCHRONIZE ACROSS DOMAINS TO ACHIEVE THE OPERATIONAL ADVANTAGE?

INTRODUCTION

Ladies and Gentlemen,
In today's rapidly evolving global landscape, achieving operational advantage requires a holistic approach. Our battlespace crosses just boundaries. It is where land forces work with naval units, guided by air force, and protected by cyber defenses.

Our military capabilities must be synchronized across all domains—land, sea, air, space, and cyber. The mindset we cultivate and the means we deploy are key to this attempt.
But the question is; how do we synchronize our military capabilities across domains to achieve operational advantage?

Before getting into details, let us first understand what “Joint” truly means

• Within a country, the term “joint” refers to the combined military forces, including the Army, Navy, Air Force, Marines, and Coast Guard. These forces collaborate to achieve common objectives and ensures national security.

• In a broader context, “joint” can describe cooperation between NATO countries-a coalition of nations committed to mutual defense. For example, NATO member states may engage in joint military exercises, intelligence sharing, or peacekeeping missions to address regional or global challenges.

• "Joint" extends to global partnerships where NATO countries collaborate with non-NATO allied countries, such as the USA/NATO working with the Middle East, USA and Korea, or USA/NATO with Brazil. These alliances bridge different military doctrines to address common security challenges.

“United in Strategy. United in Triumph.
Facing Challenges Side-by-Side.”

SINGLE SERVICE DOCTRINE DEVELOPMENT VS JOINT DOCTRINE DEVELOPMENT

SINGLE SERVICE DOCTRINE DEVELOPMENT

Traditionally, each military branch created its own operational doctrine independently without coordinating with other branches. The Army had its way, the Navy another, and the Air Force yet another.

This approach allowed each branch to focus on and maximize its unique capabilities.
But here's where the problem lies. This siloed mentality brought about several issues.
First, it minimizes inter-service coordination. This means we missed out on comprehensive cross-domain strategies that could make us stronger as a whole.

Second, this stove-piped mentality discourages effective joint operations and reduces overall efficiency. Without a unified doctrine, interoperability between services suffers. This complicates joint missions and lowers our effectiveness on the battlefield.

Lastly, the suboptimal use of combined capabilities means we might underutilize the joint strengths of our military, leading to missed opportunities for operational superiority.
In today's scenario, this fragmented approach no longer suffices. What we need now is synergy, not silos.

JOINT DOCTRINE DEVELOPMENT

Thankfully, we have a choice!
We can adopt a joint doctrine development approach. This approach calls for collaboration across all branches of our armed forces to create unified operational guidelines and strategies.

There are multiple benefits of this approach.
Joint doctrine provides a unified structure for military operations, and increase efficiency and effectiveness.

One of the key advantages is improved interoperability. Enhanced collaboration between services leads to better interoperability, ensuring seamless joint operations.

It also optimizes resources through a joint approach which reduces redundancy and increases operational efficiency. After all, why duplicate efforts when we can achieve more with less?

Moreover, the joint doctrine is based on standardized training and execution. It ensure every service member is well-prepared for any mission, anywhere in the world. This approach strengthens our military's capability to adapt swiftly and effectively to multi-domain operations and diverse threats.

Above all, joint doctrine development gives us the strategic agility we need to facilitate rapid response and keep our nation safe.

However, nothing worthwhile ever came easy, moving beyond the status quo necessitates addressing several critical challenges.

PAST (or STATUS QUO) TECHNOLOGY vs ADVANCED TECHNOLOGY

PAST (OR STATUS QUO) TECHNOLOGY

Our existing capabilities and slow adaptation often leave us vulnerable to modern threats like cyber-attacks and electronic warfare.
Interoperability issues compound our difficulties. They arise from incompatibility across domains and disparate systems, impeding smooth joint operations and coordination.

Operational inefficiencies also plague our forces. Increased maintenance demands and resource waste detract attention from essential training and readiness. As a result, our competitive edge is diminished, which can compromise our position on the global stage. But that's not all!
Our data is a valuable asset, yet poor handling and a lack of real-time analysis limit its effectiveness in decision-making.

ADVANCED TECHNOLOGY

So, what's the solution? To overcome these challenges, we must move past the old technology. The technology of the past served us well, but they belong to a different era and we need invest in advanced technologies and systems.

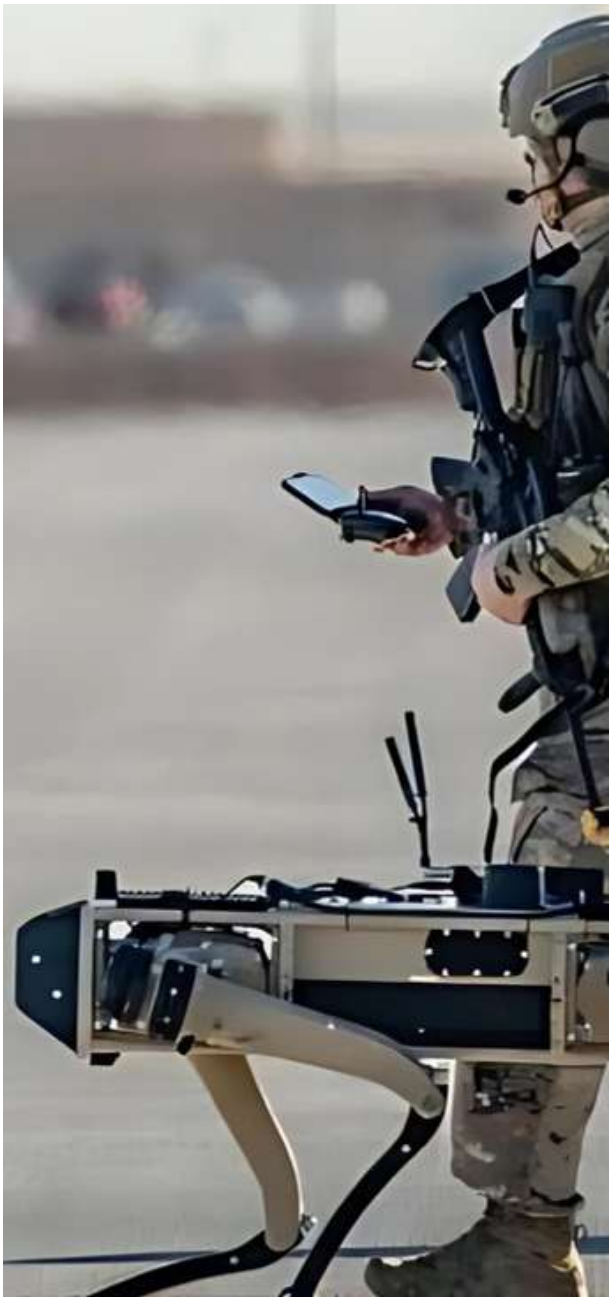
Let's talk about some of these advanced technologies—like artificial intelligence (AI), machine learning (ML), and autonomous systems. They play a pivotal role in modern warfare.

AI and ML turbocharge our data processing and decision-making. Autonomous systems improve coordination by executing complex tasks with pinpoint accuracy and lightning speed. And AI-driven communication and cyber operations ensure our information exchange is both secure and super-efficient.

But to truly harness these innovations, we need to foster an open and forward-thinking mindset among our military personnel. We need to adapt our policies and doctrines to fully integrate these technologies, aligning them with our strategic objectives.

By blending advanced technologies with a progressive mindset, our forces can achieve super synchronization across all domains. Isn't that what we're aiming for? EXCELLENCY?

This isn't just about keeping up; it's about enhancing our operational capabilities and securing our strategic edge in modern warfare.



INCOMPATIBILITY VS INTEROPERABILITY

INCOMPATIBILITY

To truly synchronize military capabilities across domains, it takes more than just new technology.
We need to tackle the root causes of incompatibility between systems, processes, and organizational cultures. Why? Because these disparities can significantly impede the effectiveness of joint operations.
This leads us to explore the disadvantages of incompatibility.
Operating disparate systems incurs unnecessary costs. This approach prevents us from optimally allocating resources due to a lack of shared information.
Think about it—we're spending money on separate systems and maintenance when we could be streamlining these efforts.
Not only that, Incompatibility slows military ability to adapt quickly to battlefield changes. It reduces our flexibility because incompatible systems make it difficult to implement adaptive strategies.

STRATEGIES TO OVERCOME INCOMPATIBILITY

First, we need to standardize technologies and protocols. By implementing common communication standards and data formats, we can ensure smooth and efficient information flow across all units.
Next, we must develop unified training and doctrine. When every soldier, sailor, and airman operates under the same playbook, we create cohesive operations across all domains.
But we can't stop there. We need to step it up with regular joint exercises to address and overcome interoperability issues.
We also need to invest in modular and adaptable technologies. Think of systems that can be easily integrated and scaled. This kind of flexibility allows us to stay ahead, ready to upgrade and adapt to new challenges quickly.
Feedback mechanisms and continuous improvement are key to staying sharp. By establishing feedback loops, we can identify and fix incompatibility issues as they arise.
Lastly, we can't forget about the power of partnerships with strategic alliances. By aligning our technologies and doctrines with international partners, we enhance interoperability with allied forces.

In the fast-paced environment of modern warfare, this compromised agility can be a significant disadvantage.
Additionally, the effectiveness of joint operations also takes a hit. Incompatible systems lead to fragmented efforts, resulting in disjointed actions and compromised mission effectiveness. Communication and decision-making delays caused by these incompatibilities can hinder our responses, which is critical during operations.
Lastly, relying on less secure methods due to system incompatibility heightens cyber threat risks. Miscommunications and misunderstandings are more likely when there's a lack of standardization, leading to errors in combined operations.
To synchronize military capabilities across domains, we must effectively overcome incompatibility. Let's explore how we can achieve this with a few key strategies.

Essential Aspects of Interoperability

Firstly, there's technical interoperability. This involves establishing common standards and protocols to standardize communication and data formats across all branches of our military. It also included compatible technology platforms which ensures that our systems are compatible not only within our own military branches but also with those of our allies.

Procedural interoperability is the next up. This includes developing unified operational procedures through joint doctrines and procedures. It's about integrating our command structures so that decisions are made cohesively, no matter which branch of the military you're in.

The last one is Human Factor. This aspect focuses on conducting regular joint training and exercises to build teamwork and skills.

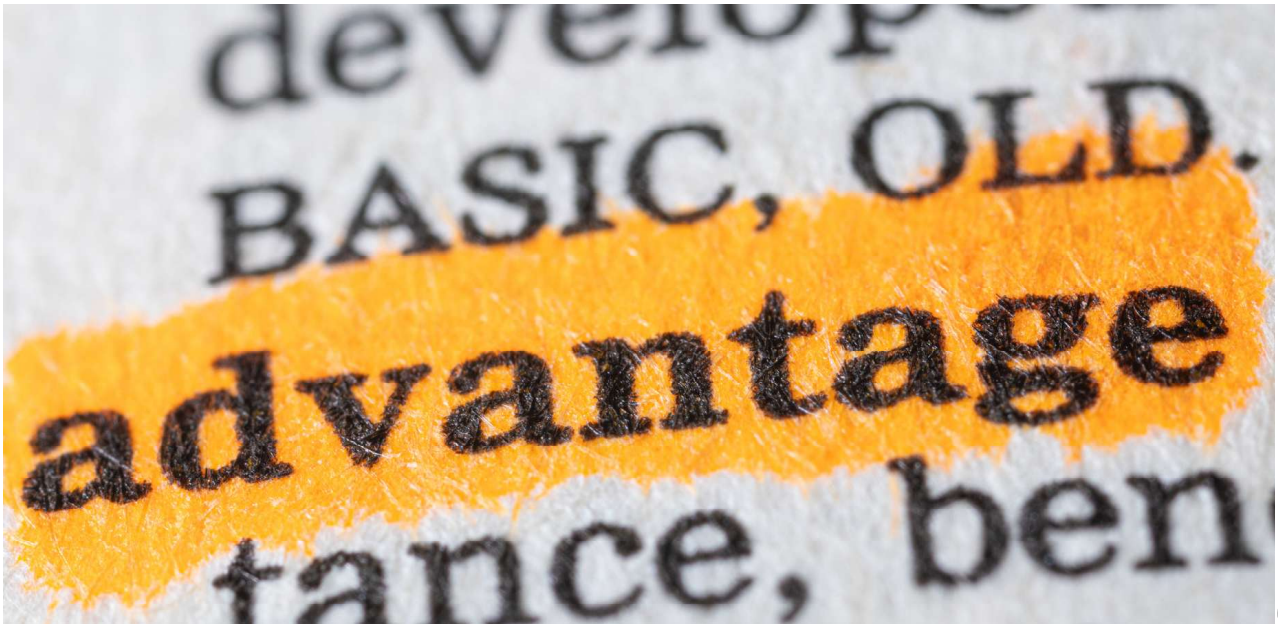
Alongside this, it enhances cultural understanding and language skills through cultural exchange and language training.
As interoperability provide so many advantages for modern military operations, why not leverage it?
Here's how we can do it!

Enhancing Interoperability for Operational Advantage

To enhance interoperability, investing in advanced communication systems is key. These systems create secure channels adaptable to different environments, supporting both legacy and new technologies.
Developing modular systems is another way to boost interoperability. These systems allow for easy integration of components, enabling upgrades without the need to overhaul entire platforms.

Participating in international standardization initiatives is also key. It aligns our military technologies and practices, particularly in critical areas like cybersecurity, UAVs, and networked operations.
Additionally, partnering with allied nations for technology sharing and cooperative development spreads development costs and ensures the creation of interoperable end products. By focusing on shared threats and missions, we strengthen collective defense capabilities and maximize operational effectiveness.

If we aim to enhance interoperability, we must establishing clear policies and agreement frameworks for interoperability, covering intelligence sharing, operational planning, and combined logistics, further solidifies our collaborative efforts.
Lastly, real-world joint operations and feedback loops are where the rubber meets the road. These activities help identify interoperability gaps and establish continuous improvement mechanisms.



INCOMPATIBILITY VS INTEROPERABILITY

STANDARD INTERNAL TRAINING

Lastly, when it comes to synchronizing military capabilities across different domains for operational advantage, basic training isn't enough.

Sure, basic training gives us the essential skills and discipline we need, but modern, integrated multi-domain operations demand more sophisticated preparation.

DISADVANTAGES OF ONLY CONDUCTING STANDARD INTERVAL TRAINING:

LLet's discuss some drawbacks of basic training in preparing military personnel for modern operational challenges.
One big issue is interoperability—it doesn't encourage enough interaction between different military services or domains. This can make it harder for teams to work smoothly together during missions.
I mean, cross domain interaction is not encouraged, and then we expect them to gel perfectly in the field? Not likely.
Additionally, basic training lacks sufficient communication training for the nuanced interactions required in joint operations. This gap can lead to misunderstandings and miscommunications, compromising mission success. That's a recipe for disaster.

Then there's the matter of preparing for modern threats. Basic training tends to focus on reactive posture which may not fully prepare personnel to handle sophisticated threats proactively. This reactive approach lead to limited problem-solving skills and a lack of training needed for dynamic conflict environments.
Additionally, basic training's narrow focus on fundamental skills specific to individual branches leaves personnel underprepared for multi-domain operations. It covers the basics but misses out on advanced skills that can really make a difference in joint operations across various domains.

Lastly, basic training reinforces stove-piped structures within military services, creating operational silos. These silos can lead to disjointed efforts and prevent the full integration of combined capabilities, which are crucial for success in today's interconnected military operations.

STRATEGIES TO OVERCOME THESE DISADVANTAGES

To overcome the disadvantages of incompatibility in military operations, we must adopt several key strategies.

First, implement enhanced joint training programs with simulations and exercises to foster inter-service cooperation and understanding. Encourage a culture of ongoing training and readily available learning opportunities.

The battlefield of the 21st century extends beyond land, sea, and air. It reaches into cyberspace, outer space, and the digital realm. To stay ahead, we must invest in advanced specialized training.

Our adversaries do not fight in isolation, and neither should we. Multi-domain warfare—integrating land, sea, air, space, and cyber—is the new reality. We should conduct exercises involving multiple domains to encourage creative problem-solving and test integrated military capabilities.

EXTENSIVE JOINT TRAINING

While basic training is a good start, it's just that—a start. We need extensive joint training to hone the skills needed for effective multi-domain operations.
So, let's discuss how we can harness this power.

IMPLEMENTATION STRATEGIES

First of all, we need to establish a consistent schedule where different branches of the military come together to simulate realistic and complex operational environments. These exercises should be varied and challenging, designed to push our personnel to adapt and excel in diverse situations.

But it's not enough to just have all the units operating in their own silos. We need to bring planners and units from all relevant domains in the exercise design and execution phases.

By doing this, cross-domain planning ensure that every aspect of joint operations is covered.

We need robust training infrastructure. We need to put resources into developing facilities that support realistic simulations of multi-domain operations. This means creating virtual reality systems and state-of-the-art cyber ranges where our personnel can practice defending against and responding to cyber threats.

Threats don't respect borders. Engaging in multinational exercises helps us enhance interoperability with our international partners. Training alongside forces from other countries prepares our personnel for coalition operations and strengthens our alliances.
It's time to get on board with enhanced joint training programs—they're crucial for our operational success.

BENEFITS OF ENHANCED JOINT TRAINING PROGRAMS

At the heart of these programs lies the development of interoperability skills. With cross-domain cooperation, joint training helps personnel from different branches understand each other's capabilities and techniques. This sets us up to operate as a cohesive force, always ready to act in unison at a moment's notice.

Regular exercises are key for refining Tactics, Techniques, and Procedures (TTPs) across diverse domains. These scenarios help us find where we're falling short and where we can improve, shaping new tactics that boost the effectiveness of our combined operations.

One big benefit of joint training is the cultural shift it sparks. When personnel from different branches collaborate, they build mutual respect and learn to make strategic decisions together, as a cohesive unit.

In the complex environments that characterize modern warfare, decision-making skills are paramount. Multi-domain exercises sharpen the ability of commanders and soldiers alike to make rapid, informed decisions while fully understanding the cross-domain impacts.

Let us not overlook the dynamic arena of technological advancement that these joint exercises offer. As we integrate and master new technologies, we gain operational advantages that were once the realm of fiction.

These exercises are not just about technology; they are also about people. They shine a light on those visionary leaders who excel in multi-domain operations, fostering an environment ripe for professional development and innovation.

But the journey doesn't end there. After-action reviews serve as a platform for continuous improvement. Through candid feedback, it allows us to refine our strategies, technologies, and tactics, ensuring that with each exercise, we emerge stronger, smarter, and more prepared than ever before.

CONCLUSION

In our relentless pursuit of excellence, we face critical choices —choices that will define our ability to achieve operational superiority. Today, we must opt for joint doctrine development over single-service approaches, embrace cutting-edge technology over outdated systems, prioritize interoperability over incompatibility, and invest in extensive joint training rather than standard internal programs.

Synchronization across domains is our advantage; let's not sacrifice it. Together we will be unstoppable! Thank you!

"United in Strategy. United in Triumph.
Facing Challenges Side-by-Side."

about the author

Wendi O. Brown
Lieutenant Colonel (Retired),
United States Army Reserve

Wendi is a retired senior officer from the U.S. Army Reserve who routinely executed duties in the role of a Chief Strategist. Wendi advised at the highest levels of leadership in the U.S. and global governments, including NATO. She has proven leadership experience in risk management, crisis management, strategic and operations planning among NATO multinational teams for cyber operations, and strategic plans to execute supply chain and logistics missions across several European countries, ensuring U.S. Army Forces are equipped to conduct critical military operations in Europe and Africa.

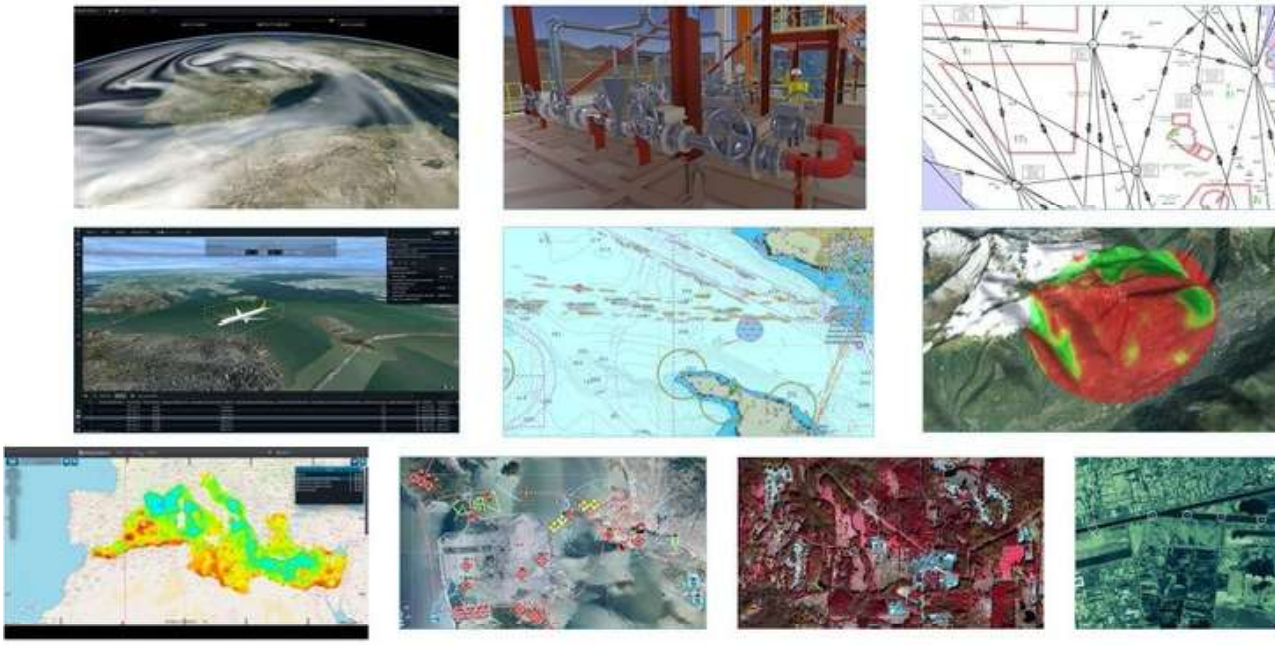

NW
N
NE
SW

Automating geographic content

Underpinning IAMD decisions with AI and data fusion

A modern integrated air and missile defence (IAMD) system is a collection of subsystems made up of sensors, controllers and effectors. NATO said its IAMD "provides highly responsive, robust, time-critical and persistent capabilities in order to achieve a desired level of control of the air." Interoperability of subsystems and ease of data exploitation for the IAMD commander directly affects the IAMD's response speed.

This paper will look at geographic data and software and their uses within IAMD. Examples from recent CUAS exercises, updates on what's possible with commercial off-the-shelf software and customer experience in various air defence systems will be examined.



Examples of data types used in IAMD – including weather, flight paths, terrain, earth observation and tactical movements

The use of geographic data and GIS within IAMD is wellknown; however, data and digital transformation tools for IAMD are relatively underused. Leveraging advances in geographic data automation at various stages of receipt, analysis, exploitation and dissemination can bolster IAMD responsiveness.

Data feeds into IAMD can include radar tracks, acoustic sensors, camera sensors (optical and thermal), terrain models, weather data and aeronautical charts. These data feeds can be analysed via artificial intelligence (AI) or machine learning (ML), which generate outputs and feed into IAMD. To allow the IAMD to fuse together differing data feeds, dynamic and static data, there needs to be interoperability of systems, usually easiest achieved by early adoption of industry standards. Whether it is using defence communication standards, such as Link 16, or geographic data standards such as those set by Open Geospatial Consortium (OGC), system manufacturers need to use standards to allow interoperable systems architecture and ease of technology upgrades.

Cataloguing data

An important first step is cataloguing sensor feeds and any physical data. This stage involves validating data in terms of its relevance to the area of operation for the IAMD and the quality of data, such as ground resolution of terrain. Presuming the data is accepted, it should then be catalogued along with any metadata such as its source, date of capture, resolution and other properties. This metadata can act as the basis for users and automated processes to discover the data later and use it in IAMD. The metadata will assure users of the authenticity of the data and give assurance of its use.

Two more important points for cataloguing data are to give a single place for users to query data and enhanced access control of the data. Through a browser-based portal or via a RESTful API, users and systems have one entry point to search for and discover data. Since catalogues can be federated, this one catalogue search can query across other catalogues, reducing data and information silos. This helps promote the “need to share” concept in a controlled and secure manner.

Conversely, rigid access control for users and systems is needed to enhance data security. This can determine which datasets users can discover and view, and if they can discover data from different geographic areas (e.g., not revealing all high-resolution data of sensitive sites to allies). IAMD users and systems need to have knowledge of what data is available and if it’s suitable for use. Without this, the value of the data is lost, and the decisions made may lack crucial information. ERDAS APOLLO, as an end user product, and LuciadFusion, as an SDK for integration into systems, both offer cataloguing and data provision.

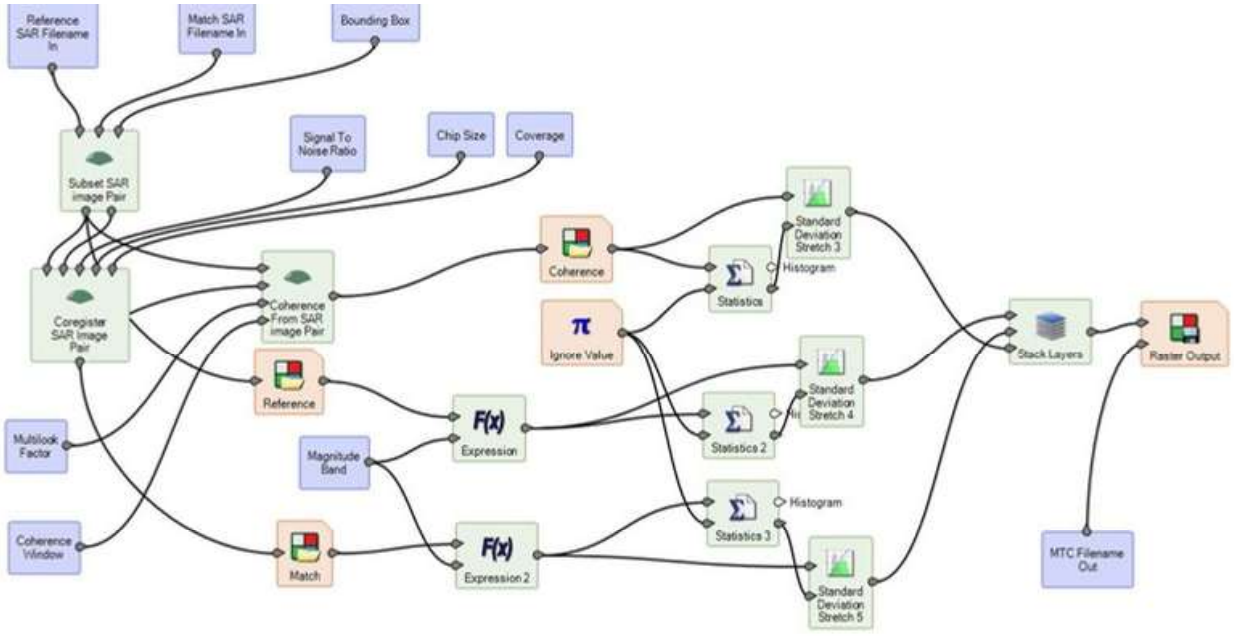
Analysing data

Once a user or system has discovered relevant data, they usually want to analyse that data in some way. This could include using terrain data to determine a good location for a radar system or using optical imagery to determine the best route for vehicles to that location. Information can be delivered to users via automatic analysis of data, using ML, AI and processing workflows. When data is processed and analysed, IAMD users can extract valuable information to gain knowledge.

Processing and analysing geographic data require certain skills and background knowledge of the data, software and desired end result. While geographic technicians may be deployed with IAMD to perform this analysis, having the analysis captured as a digital data workflow means any user or system can run the analysis. The data workflow can be created at headquarters and shared among users either as a physical file or as a web API service. End users do not need to know how to perform the analysis; they simply need to know which relevant data workflow to run and analyse the latest data available to them. The use of data workflows increases analysis capacity and reduces variability and inaccuracies introduced by individual users running analysis by hand.

Data can be analysed in real time with real-time data feeds, such as tracking UAVs, and real-time interaction between users and data visualisation. The former can be as simple as visually highlighting the airspaces in which a UAV is active or performing spatial calculations on trajectories and intercepts using bounding boxes. The latter can be a calculated line of sight drawn over terrain data as the user moves around the observer position on screen. This is a quick way to check a route for blind spots. Spatial Modeler, which is delivered as a graphical editor and an SDK, is used to create these data workflows.

Modern IAMD can incorporate simulation and prediction routines and algorithms to help commanders validate decisions and alternatives more quickly. In a digital data environment, running "what if" analyses are also possible, both in a training environment and when operational. This can also feed back lessons learned to aid continuous improvement of processes and procedures for future deployments.



An example data workflow, in a graphical editor

Visualisation of missile trajectory and interception

Visualising data

Most of the data and derived information will eventually need to be delivered to users and other systems – users need the correct information in the correct format at the time of relevance. Through automation of dissemination and ease of retrieval, decision-making is faster because users and systems don't have to search for information.

The delivery medium can be visualised on a screen, showing a 3D view of the terrain, sites of interest, airspaces above them and the predicted or tracked locations of missiles.

Alternatively, the delivery medium can be a simple notification to users via email of new, relevant data in an area of interest, which allows them to access the data and view or analyse it as needed. If the data and information are delivered to another system, even a subsystem within the IAMD, it will be delivered as a standard data format or web API service.

These are publicly documented and used by multiple vendors to allow data sharing. There can be an authorisation façade on the services so only intended users can access the data.

The visualisation of information and data can help users interpret and understand a situation quickly, whereas a 3D view of real-time data and analytics depicts thousands of sentences. And by utilising advanced browser technology, the IAMD C2 delivers timely information to commanders.

The view can be made up of real-time tracks, predicted tracks, weather information, background geographic data and ad-hoc analysis results. Automated highlighting of certain data or objects in the view helps users discern relevant information. For instance, airspaces can be represented as volumes (e.g., 3D shapes) in the visualisation, and each airspace highlighted as air traffic (e.g., drones, missiles, etc.) passes through it.

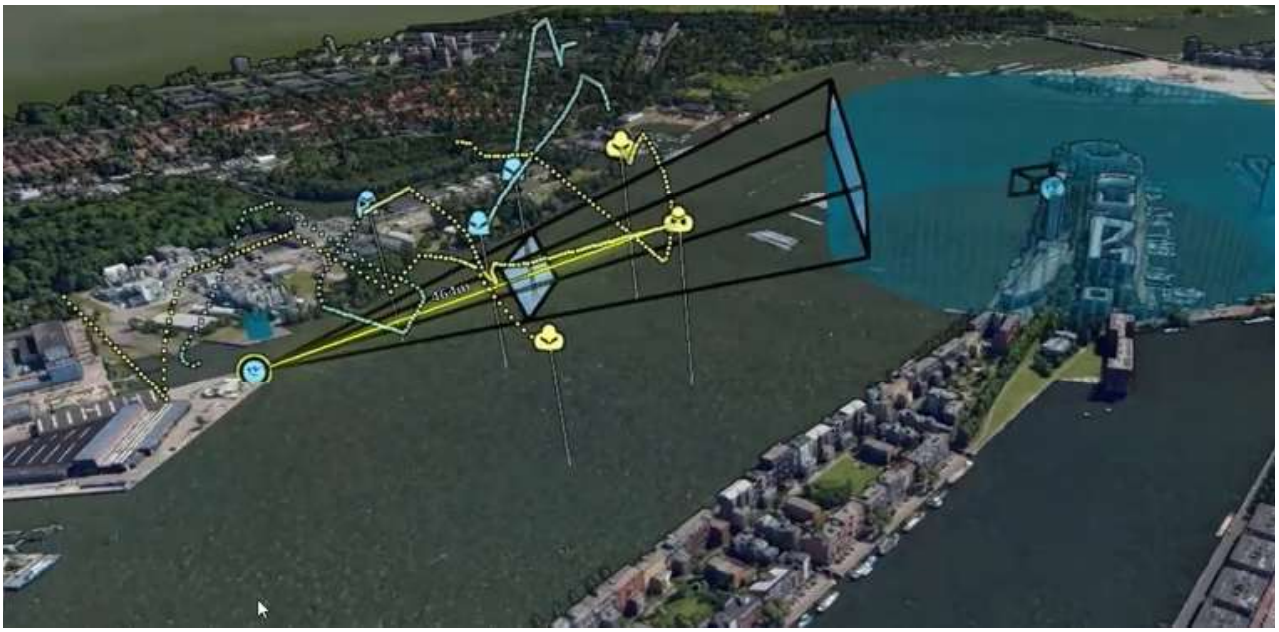
This gives operators easy to see and easy to interpret situational awareness. The SDK LuciadCPillar is one product for C++/C# developers that supports IAMD development.

Gaining trust in AI and ML

AI and ML are used throughout the various processes described above, whether to identify suspect UAVs from a video feed or locate suitable anti-missile battery locations. As AI grows in adoption and is more widely utilised, users will begin to gain trust in it as well.

However, IAMD systems still have human-in the-loop (HITL) processes to decide when to deploy an effector, whether lethal or not. To add confidence in AI, data fusion can be used in outputs of various sources. Sensors can have their own AI onboard and can, for example, classify objects in a video feed such as birds, UAVs or planes.

If the AI is processed on the edge (e.g., on the sensing device), alerts, such as for a suspect UAV, can be transmitted back to the IAMD C2 instead of all raw data.
Data fusion will then use AI to ascertain if the alerts reported by the sensors are of the same rogue UAV or separate ones. At the C2, the operator has a lower cognitive burden since only significant alerts are displayed.
Through C2-based AI, and in correlation with data fusion, alerts from different sensors can be confirmed against third-party sensors including other nations' assets.



In closing

As with many systems of systems, the output of an IAMD can be greater than the sum of its parts.
Using interoperable data formats, communication services and automation of data receipt, analysis and distribution, the modern IAMD can reduce reaction and decision times for commanders.
Hexagon has proven its product and technical expertise during NATO interoperability exercises. Discover how Hexagon's solutions can help defence organisations and systems providers integrate, visualise and analyse missioncritical data in dynamic common operational pictures that support better situational awareness and faster, more informed decision-making.

Hexagon is the global leader in digital reality solutions, combining sensor, software and autonomous technologies. We are putting data to work to boost efficiency, productivity, quality and safety across industrial, manufacturing, infrastructure, public sector and mobility applications. Our technologies are shaping production and people-related ecosystems to become increasingly connected and autonomous – ensuring a scalable, sustainable future.

Hexagon's Safety, Infrastructure & Geospatial division improves the resilience and sustainability of the world's critical services and infrastructure. Our solutions turn complex data about people, places and assets into meaningful information and capabilities for better, faster decision-making in public safety, utilities, defense, transportation and government. Learn more at hexagon.com and follow us @HexagonAB.

about the author

RICHARD GOODMAN
Geography Specialist

Richard GOODMAN is a geography graduate with a background in geographic data production, software support and presales. His current role involves business development for Hexagon around defence, setting strategy, gaining market recognition within defence agencies and supporting the wider sales team and partners.

Initially working in photogrammetry and with early digital cameras for aerial survey, Richard led a department capturing mapping data, telecoms data, & creating ortho images and elevation data from aerial images.


RELOADING


An-26B
2.6km
102

TRAIN AS YOU FIGHT REINVENTED.

SYNTHETIC ENVIRONMENT EXPLOITATION TO ENHANCE NATO IAMD CAPABILITIES.

ABSTRACT

NATO Integrated Air and Missile Defense (IAMD) is essential for credible deterrence and defense in an era of increasingly complex air and missile threats, from UAVs to hypersonic missiles. To enhance IAMD capabilities, there is a critical need to integrate these efforts into Multi-Domain Operations.

This integration should leverage emerging and disruptive technologies to adapt to a future operational environment characterized by multi-region and multi-dimensional challenges—physical, virtual, and cognitive. Cultivating a military culture within NATO that promotes excellence in these areas is paramount.

INTRODUCTION

Persistent preparation in today's military landscape requires a Synthetic Environment, utilizing advanced modelling and simulation (M&S) to pinpoint improvement areas, foster trust in new capabilities, and support leadership development through wargaming and experimentation. Frequent, realistic training through live, virtual, and constructive (LVC) venues is crucial for conserving resources while enhancing combat realism and multi-domain readiness and to facilitate the development of innovative and collaborative solutions.

The IAMD Center of Excellence (COE) has explored relevant M&S initiatives across NATO nations, identifying modern training methods, including Serious Games and advanced extended reality (XR) technologies.

The COE aims to serve as a knowledge hub, fostering the development of a NATO IAMD simulated battle network while highlighting associated risks and opportunities for stakeholders, including in NATO HQs, NATO Command Structure (NCS), NATO Force Structure (NFS), scientific organizations,

and other COEs. This collaborative approach is essential for advancing digitalization in line with the Warfare Development Agenda.

The envisioned transformation of NATO IAMD capabilities is central to the IAMD COE's Power of Work (POW) 25, as approved recently by its Steering Committee. By fully exploiting M&S capabilities across its transformational pillars, the COE seeks to engage with operational and tactical units to utilize the synthetic environment regularly, thereby reinventing NATO's IAMD, training, capabilities development, interoperability, and overall effectiveness.

ANALYSIS

On Going NATO Nations M&S Programs (FASF/HAF/RAF/USAF)

The transition of NATO Air Forces from fourth to fifth-generation fighter aircraft reflects the increasing complexity and cost of modern air combat. As these advanced aircraft become scarce high-value assets, maximizing their sortie effectiveness and training value has become a pressing challenge. This situation is exacerbated by the rising costs of operational flight hours, making it crucial for air forces to manage their resources effectively.

To address the need for Air-to-Air (A2A) and Air-to-Ground (A2G) training, many air forces are increasingly turning to private Red Air services and enhancing their simulation capabilities. The evolution towards a more integrated training environment involves utilizing "common synthetic environments" that allow for non-proprietary and interchangeable training systems. These developments enable aircrews to engage in mission rehearsals and test new weapons in a LVC multi-domain framework.

FASF – AIR WARFARE CENTER/Distributive Mission Operations Center (DMOC)

In this context, the French Air Warfare Center (AWC) and its Distributed Mission Operations Center (DMOC) in Mont De Marsan are at the forefront of these innovations.
Their L-16 LVC system, known as "Jeannette1", has been operational since 2018, providing a range of valuable services that enhance mission training and operational readiness. The DMOC facilitates everything from simple missions to complex Combined Air Operations (COMAO) and international exercises, such as VOLFA.

Moreover, the ongoing "Massive Network Simulation" program aims to develop in serious games software advanced part-task trainers for various fixed-wing and rotary platforms, all interconnected with the Jeannette system. This initiative not only supports national training needs but also promotes interoperability with established networks like CFBL NET2 and emerging multinational training environments in Europe and across the Atlantic.

Picture 1. French AWC/DMOC – LVC - MNS

In the DMOC, SYNAPSE3's experienced reservist weapons instructors collaborate to enhance training effectiveness. Their roles range from mission planning and airboss duties to running flight animations and conducting thorough debriefings. A key focus is on capturing performance data and statistics, leveraging the expertise of data scientists to provide actionable insights that support the operational requirements of the French Air Force.

HAF - Hellenic Air Tactics Center (HATC)/ Synthetic Training SQN (STS)

The Hellenic Air Force (HAF) has made significant strides in synthetic training through its Hellenic Air Tactics Center (HATC). A dedicated team has successfully developed ten F-16 tactical simulators, eight part-task trainers4, and a Joint Terminal Attack Controller (JTAC) simulator, all designed to enhance tactical training mainly for Airmen. These systems operate within a cohesive tactical environment and are actively utilized during HATC courses and the annual INIOCHOS live exercise.

Picture 2. HAF HATC/STS M&S Capabilities

By collaborating with allied capabilities (UAWC/ABTC & FASF), HATC has enhanced its synthetic training environment, ensuring << day 1>> interoperability with NATO systems and allowing for efficient coordination with other synthetic environments5.

Participation in NATO's RAFL 24-Virtual exercise (Jun 24), the first NATO Virtual rehearsal, marked a significant milestone in digital transformation for the alliance, preparing for future live exercises (OCT 24 in Greece).

HATC is also expanding its synthetic training capabilities with the development of an electronic warfare (EW) training environment and a Live-Virtual-Constructive (LVC) operations center. This center will integrate live platforms via Link-166, facilitating a more comprehensive and adaptable training approach.

Plans include extending synthetic training capabilities to HAF combat wings and other branches of the Hellenic Armed Forces, driven by advancements in virtual reality technology and compatible software. These initiatives aim to continually improve training outcomes and operational readiness.

Picture 3. VR/MR devices exploitation in Military/Civilian AVIATORS Training.

RAF - GLADIATOR, UK, Air Battlespace Training Centre (ABTC)

The new Gladiator training capability at ABTC - RAF Waddington - represents a significant advancement in synthetic training systems. This world-leading facility connects various synthetic training devices to a central hub, enabling collaborative training across Land, Maritime, and Air domains in a safe and secure environment.

The scale and security of this training are unprecedented in Europe, and future expansions will integrate Space and Cyber capabilities, enhancing connectivity with Allies and Partners. Air Chief Marshal Sir Mike Wigston highlighted the importance of Gladiator in preparing the next generation of warfighters across all domains.

Picture 4. Gladiator - ABTC

Importantly, Gladiator complements live training rather than replacing it, ensuring that training activities are conducted in the most effective settings. The UK Ministry of Defence has invested over £220 million in BAE Systems to deliver high-fidelity simulators7 specifically for Typhoon pilots, further solidifying Gladiator's role in advanced synthetic training.

USAF – USN /VVTC & JSE

The Air Force Warfare Center at Nellis Air Force Base is advancing its Virtual Test and Training Center8 (VTTC), which provides a sophisticated platform for pilots and crews to train together using a variety of simulators in a controlled environment. This initiative not only enhances pilot training but also explores the integration of synthetic scenarios with live flying operations at the Nevada Test and Training Range. The "vision" is for all the Air Force's latest-generation aircraft to have a device that connects to the VTTC campus, and moreover to connect the newest platforms to the Joint Simulation Environment (JSE), a government-owned, non-proprietary modeling and simulation environment.

The JSE, initially established at the Naval Air Warfare Center Aircraft Division features a network of simulators, including eight F-35 and four F-22 cockpits, all designed to replicate actual aircraft systems precisely. This facility supports the simulation of complex mission scenarios with thousands of threats sourced from the latest intelligence models. It allows for the integration of various adversarial elements, such as enemy aircraft and advanced weaponry, along with electromagnetic, infrared, and cyber threats.

The JSE serves as a critical training tool, having already trained over 1,000 F-359 pilots, incorporated as well into the formal curriculum for weapons schools. This training environment is seen as vital for preparing pilots for real-world combat situations against peer adversaries. Department of Defense plans are in place to extend this high-fidelity simulation capability to additional Navy and Air Force facilities, with a fully operational JSE, complete with F-35 and F-22 cockpits, expected at Nellis AFB by 2028.

Picture 5. AWC/VTTC - JSE

Comprehensive NATO IAMD Training Environment

Considering that NATO IAMD must be multi-national by design, not aspiration, such integration demands a comprehensive multi-national training environment, including an open architecture network, command and control, tactical data links, shared doctrine and operating procedures. The baseline must remain "train as you fight" being as close as possible to the real operational environment. To that end, innovative ways of training are to be further developed, to complement live training in multi-domain operations, with most of the participants being in their operating environment-almost everyone besides the pilots10 who will mainly connect through a simulated cockpit.

Proprietary simulators, however, each created by the manufacturer of the platform itself with inherent modeling, security, and latency limitations, make it expensive and time-consuming to link together multiple platforms and test new threat paradigms. A tangible solution is to develop simulators with open architecture, or/and following an unconventional defence planning process, to exploit ad hoc relevant software and extended reality commercial of the self-devices.

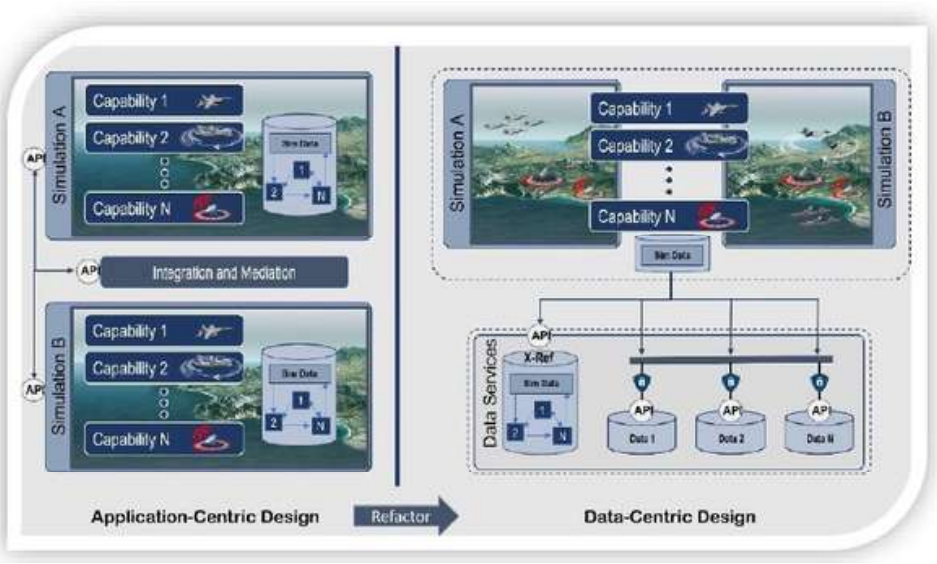
By doing so, part task trainers can be produced/procured able to be connected to existing and under development distributed synthetic environments through established networks (e.g CFBL NET) in a fraction of the cost of full fidelity simulators.

Integrated LVC training solutions could be developed and through standardized distributed simulation protocols to enable realistic tactical mission training, both at national and multinational levels, with a higher impact on the multinational coalition operations.

The urgency of the shift to the synthetic environment is multifaceted, including adversary observation capabilities, current range limits, the need to integrate multiple platforms with high operating cost, airspace capacity including environmental considerations, and that some training and test aspects cannot be efficiently taken place in a live environment. Adversary observation means everything from weapons testing to new tactics, techniques, and procedures (TTPs) can now be seen, particularly by opponents' satellites passing overhead. Current ranges are also too limited for modern air warfare, as rehearsals needed require multiple aircraft and standoff distances in hundreds of miles, making it almost impossible to put all those assets together in one piece of sky, considering the cost of such setups as well. Moreover, the increased use of synthetic training will help with more efficient airspace exploitation13 in addition to reducing the current carbon footprint14 of live training. Finally, and more importantly, modern 5th gen platforms cannot be efficiently exploited15 faced with poorly simulated Red Air adversaries (e.g F-16, and threat emulators), restricting needed Fighter Pilots advanced and realistic training, consequently undermining the pilots' Fighting Spirit.

When you pair all of those together, to enable effectiveness and performance you're almost left with no choice but to start executing some of this high-end, advanced test, training, and tactics development concerning IAMD effects in the synthetic environment, delivering cost16, time, enhanced realism17 and sustainability benefits over live training, enabling IAMD fighters, including fifth generation pilots, to acquire the skills they need to exploit the IAMD capabilities in the multi domain operation context to the maximum extent.

Easier said than done, to achieve such effectiveness, in a NATO environment several parameters should be faced; among others, various levels of security and interoperability (as the need for correlated terrain/targets), the integration of other domain M&S effects including cyber and space, intellectual proprietary rights and conflicting interests by industry, national procurement procedures, lack of the needed workforce to efficiently run suggested capabilities in parallel with live ops, and critically, the institutionalization of the synthetic training, maybe the most difficult task at hand, as the transition to synthetic training will likely face resistance due to organizational inertia, necessitating strategic change management approaches.



Picture 6. US shifting to a data-centric enterprise

Moreover M&S data should be treated as Strategic Asset19, as a data-centric enterprise not only will provide shorter integration times and more readily available training opportunities to conduct Joint training exercises and mission rehearsals, but in addition will fuse research and experimentation to support capabilities development, and wargaming to enhance decision making from the political to the tactical level.

IAMD COE Supporting Role

The IAMD COE is strategically positioned to transform IAMD training within NATO, aligning with the Alliance Warfare Development Agenda, addressing ongoing challenges and enhancing cooperation among allies, by supporting the development of a NATO Synthetic Training Network across multiple services and domains to facilitate joint training, research, experimentation, and wargaming, thereby strengthening IAMD capabilities.

As a central hub, the IAMD COE will share insights on existing solutions and promote research and analysis while engaging with relevant stakeholders. A critical aspect of this transformation involves enhancing Modeling and Simulation (M&S) capabilities, with a new facility set to open in 2025. This facility will enable remote connectivity to various LVC environments through the CFBL Net and VoIP.

Building robust relationships with the Operational and Training Community in locations like Souda Bay and leveraging the Synthetic Environment will further enhance collaborative training efforts. Support from NCIA and engagement with the M&S COE and the NATO DST WG will help streamline wargaming initiatives, minimizing duplication of efforts, while fostering innovation in experimentation within synthetic environments. This includes exploring concepts related to Unmanned Aerial Systems (UAS) and Hypersonic threats, which are vital for developing effective IAMD capabilities.

An operational state-of-the-art VR Tactical Simulator will provide interoperability with existing LVCs and serve as a Part Task Trainer for both Blue and Red Air scenarios. This initiative will enable valuable data capture for mission analysis and rehearsal, and support studies on the application of VR/MR devices in IAMD missions, particularly for fighter pilot training, in response to NATO Requests for Support. Through these efforts, the IAMD COE aims to significantly enhance NATO's defensive posture in the evolving threat landscape.

Picture 7. IAMD COE envisioned IAMD M&S Ecosystem

CONCLUSION

The evolving landscape of Integrated Air and Missile Defense (IAMD) necessitates a transformative approach to capabilities, leveraging advanced technologies and fostering a culture of innovation within military alliances. The integration of LVC environments is essential for preparing forces to meet modern multi-domain challenges effectively.

Key elements for this transformation include:

- Digital Transformation: Embracing modern technologies, including commercial off-the-shelf solutions, to enhance training efficiency and realism in IAMD operations.
- Collaboration and Networking: Building trust and cooperation among allied forces through persistent engagement in LVC environments, facilitating shared experiences and learning opportunities.
- Human Capital Investment: Developing expertise and training personnel who can manage complex synthetic exercises, ensuring effective planning and execution.
- Operational Requirements: Addressing the challenges in defining clear operational needs within the rapidly changing military landscape, where traditional approaches may not suffice.
- Innovative Solutions: Encouraging creative problem-solving and collaborative initiatives to adapt to emerging threats and technologies, thus enhancing overall readiness.
- Stakeholder Engagement: Involving various levels of military and political stakeholders to drive a unified approach to capability development and operational integration.

The IAMD Center of Excellence aims to be a pivotal hub for these efforts, promoting the transformation of IAMD capabilities while navigating relevant complexities. The transition to a more integrated, synthetic training environment is not just a logistical or technological challenge but a strategic imperative for NATO. It requires a concerted effort to align policies, overcome institutional resistance, and prioritize interoperability and security to fully realize the benefits of multi-national training initiatives.

The potential for improved operational effectiveness, cost efficiency, and environmental sustainability makes this shift essential for future readiness in complex multi-domain operations. By focusing on these areas, NATO can position itself to capitalize on significant projected benefits, reinforcing its defensive posture in an increasingly complex global security environment.

IAMD CoE

iamd-coe.org