Volume No. 1 | December 2022

IAMD—CoE's Annual Conference Journal

Integrated Air & Missile Defence:

Challenges and Threats, Developments and Opportunities in a Rapidly Changing Environment

LETTER FROM THE DIRECTOR

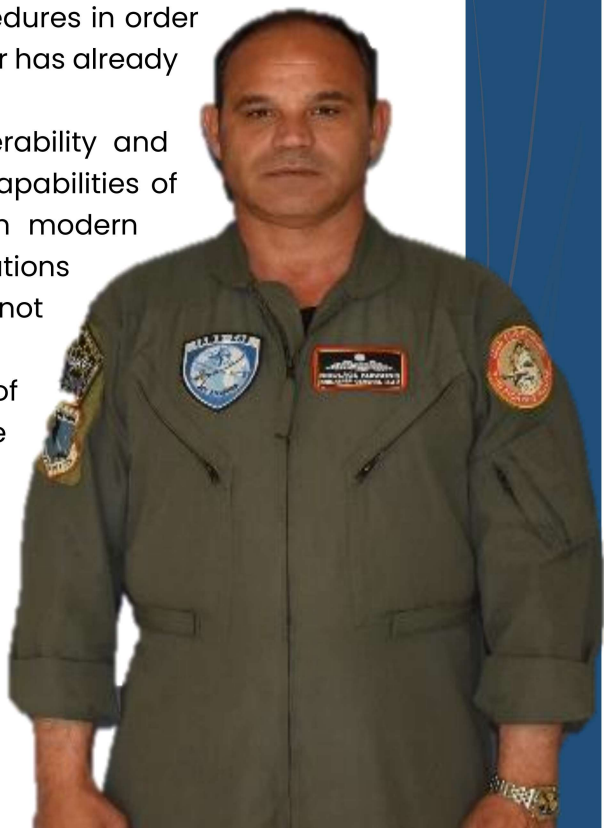
December 2022

Dear reader,

On the 21st of December 2020 and the 25th of January 2021, the Military Committee, and the North Atlantic Council (NAC) respectively endorsed and approved, the IAMD CoE as the 27th in line accredited NATO CoE, it's activation as a NATO Military Body and the granting of international status under Article 14 of the Paris Protocol.

With NAC's approval, Greece offered to the Alliance and its Partners, an accredited multinational Centre, with the vision to act as an internationally recognized focal point for knowledge and expertise in the rather demanding but very timely IAMD domain.

Greece as a Framework Nation (FN) and Bulgaria, Czech Republic, Romania, and the Republic of Türkiye as Sponsoring Nations (SNs), offer to the Alliance, fourteen (14) highly educated, skilled and motivated Subject Matter Experts (SMEs), drawn from Land, Maritime and Air Commands of the respective NATO Nations. Additionally, France has already initiated all the appropriate procedures in order to join IAMD CoE as Sponsor Nation and a French officer has already joined the Center in observer – status.



IAMD COE mission is to enhance the interoperability and support the development and exploitation of IAMD capabilities of the Alliance, NATO Nations and Partners, based on modern requirements and a smart defense multinational solutions mindset, and minimize the gaps identified and not covered by other NATO entities and NATO COEs.

Along with, to provide opportunities of comprehensive research, experimentation, doctrine and concept development and testing, education and training and collateral analysis support in the lessons learned process, with recognized knowledge and expertise.

As it is commonly agreed, sharing of knowledge

and experience among specialists in IAMD, enhancing Air and Missile Defense operations by building common understanding. This particular domain, by definition, deals with all the fields of action of the Alliance (land, sea, air, cyberspace and space) for that, the Centre focuses on the following areas:

- Offensive/Defensive effects in support of IAMD
- Passive Air and Missile Defence
- Surveillance
- Technical and procedural system integration
- Counter – Unmanned Aerial Systems (C-UAS)
- Counter – Rockets, Artillery and Mortars (C-RAM)
- IAMD's role in Anti-Access/Area Denial (A2/AD).

Our vision is to act as internationally recognized focal point for IAMD knowledge and expertise, to support NATO transformation and capability development in a cooperative and cost-efficient way in support of NATO Missions and Tasks, committed to the Alliance key values and principles.

Despite the negative effects of Covid - 19 pandemic, the Centre managed to develop skills in all important fields of IAMD, with active role and dedication to its mission, and to provide, training and best practices, doctrines, analysis and lessons learned in the demanding IAMD Domain.

Sincerely,

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

A NATO HQ policy perspective on Integrated Air and Missile Defence

By Ms Radoslava Stefanova
Head of IAMD Section, NATO IS,
Defence Investment Division,
Armament & Aerospace Capabilities
Directorate

The recent deterioration in the current security environment, in particular, Russia's aggressive war against Ukraine, have prompted a significant adaptation of NATO's deterrence and defence posture. This has also involved the strengthening of NATO's Integrated Air and Missile Defence (IAMD), and all elements of NATO's "appropriate mix" of deterrence and defence capabilities. Furthermore, major state actors, notably China, are in the process of increasing their air and missile capabilities, including using new technologies, such as hypersonic missiles. Iran and its proxies, as well as North Korea have been engaged in similar activities. Additionally, new uses of low-end drone-type capabilities, as well as rapid advancements in the cyber and space domains pose further challenges to NATO IAMD. The proliferation of missile technologies to non-state actors, in the context of an overall weakening of global arms control and non-proliferation regimes adds further complexity to the threats NATO is facing. These developments have had profound effects on NATO IAMD policy, including procedures, decision-making, operational and defense planning, capability requirements, as well as training and exercises. As we continue to strengthen NATO IAMD, we are working to ensure that current concepts and policies are updated at the speed of relevance, while improving coherence within the IAMD missions and ensuring political control at all times. NATO IAMD is in a process of adaptation, with the overall objective of making this core capability more credible, more ready and more responsive, tailored to addressing all air and missile threats, emanating from all strategic directions.

Emerging Threats, Enduring Problems: What the Ukraine Crisis Taught Us About Interoperability

By COL Bruce Bredlow US (A), Commander
52nd Air Defense Artillery Brigade

Introduction

This is a good time to be an air defender, especially in Europe. A lot of positive change has come to the European theater: a new Air Defense Artillery (ADA) Brigade is standing up. Short Range Air Defense (SHORAD) in Europe is modernizing with the more lethal, mobile, and survivable ManeuverSHORAD system. And the new NATO IAMD Center of Excellence is still a new addition to the community. This positive change is well-timed too: the ongoing crisis in Ukraine has helped to remind everyone of the enduring importance of effective air defense capabilities. The deployment of 10th Army Air and Missile Defense Command (AAMDC) subordinate units also provides an opportunity to glean lessons that can inform future improvements to air and missile defense operations throughout the European theater across a wide array of conditions.

10th AAMDC, as the senior ADA headquarters in Europe, has learned a lot of valuable lessons, ranging from the tctical all the way to the strategic level. This paper will focus primarily around policy issues; as such, it is important to begin by acknowledging the insight offered in the conference's first keynote address by Ms. Radoslava. Ensuring a shared understanding of NATO's policy perspective on IAMD is crucial to IAMD success in this theater, and her insight underscores some of the policy-related challenges 10th AAMDC has experienced throughout its IAMD support of operations along the Eastern Flank. One thing will always remain true: we must all work together, including at the NATO policy level, if we want to reach our desired end state. This paper's goal is to describe some of the more urgent challenges we must all confront, which have been realized over the past seven months operating along NATO's Eastern Flank. In doing so this paper will describe how 10th AAMDC and 52nd ADA BDE understand and approach interoperability and some of the things that must be accomplished moving forward in order to achieve full interoperability with all our joint and combined IAMD partners.

Supporting the Eastern Flank

Since the beginning of Russia's invasion of Ukraine, 10th Army Air and Missile Defense Command (AAMDC) has supported efforts to deter further aggression and assure NATO Allies and Partners of U.S. commitment to the Alliance. In fact, 10th AAMDC has been at the tip of the collective security spear. 10th AAMDC Soldiers were among the first to deploy to the Eastern Flank to support NATO and deter Russian aggression, beginning with 5-4 Air Defense Artillery Regiment (ADAR) deploying to Romania to provide Short Range Air Defense (SHORAD) support. This was soon followed by more SHORAD deployments to Latvia, Lithuania, Poland, and Slovakia. 5-7 Air Defense Artillery (ADA) Battalion also deployed multiple Patriot Batteries to Poland and Slovakia. Not only Soldiers from our subordinate battalions have traveled to these countries. Senior leaders at the AAMDC and BDE levels have also traveled to each location to ensure conditions are set for success. Leaders at all echelons, from the Battery level all the way to the

Division level, have traveled and deployed to these locations and conducted key leader engagements with host nation officials.

The wide reach of 10th AAMDC and its subordinate formations during the Ukraine crisis has generated a number of valuable lessons that the organization intends to take into the future as it continues pursuing the strategic priority of developing full interoperability with all air and missile defense counterparts across the European theater. As engagements with senior leaders continue to occur in the countries we deployed to, it is clear that there are no cookie cutter solutions. Every deployment is its own knot to untie. 10th AAMDC deployed forces to five different nations with five different sets of laws, political contexts, airspace management procedures, integration challenges, and joint and combined operating environments (some NATO-led, others not). Seeing this complexity in the operating environment laid the foundation for the most critical lessons being drawn from operational missions, and this complexity underscores the challenge IAMD poses: IAMD operations are tactical in nature but have strategic effects, creating unique challenges.

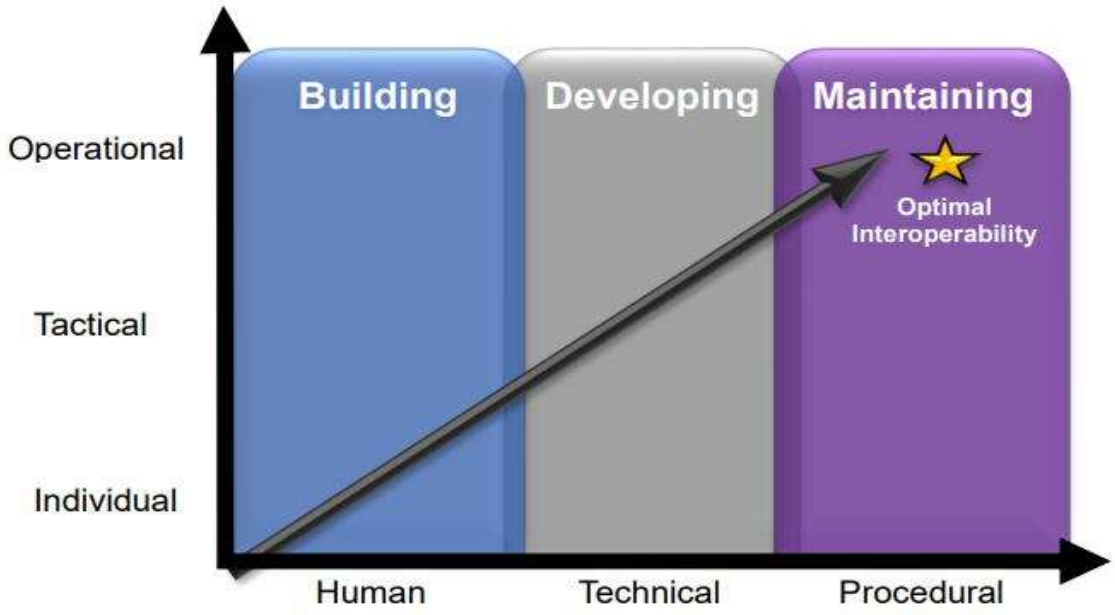
One of the biggest lessons learned for 10th AAMDC is that, despite this complexity, some problems never go away, no matter how much the threats faced, the capabilities on hand, and even the nature of war itself, might change. The most important lessons all have to do with what has been known all along: developing and maintaining adequate interoperability with NATO Allies and Partners is a must to successfully deter Russian aggression and defeat Russian air and missile threats should deterrence fail. Allies and Partners are the center of gravity: without them there is the risk of lacking the capacity required to provide theater-wide defense of critical assets. But what exactly does that mean? What should the IAMD community really be trying to achieve when pursuing interoperability through field exercises, data link fidelity drills, tabletop exercises, and conferences like this one? The biggest lesson 10th AAMDC has learned over the last 7 months is that the most important aspect of interoperability demands more focus moving forward. That aspect is the policy side of procedural interoperability, without which any interoperability to the degree needed to be successful remains out of reach. To be successful in combined air and missile defense operations, this aspect must be right. What this means to 10th AAMDC, the risks associated with failing to achieve it, and some of the things we think must be done to accomplish it are a primary focus for 10th AAMDC.

10th AAMDC's Theory of Interoperability

Interoperability is key to IAMD success in Europe. A lot of people talk about the importance of developing interoperability, but fewer people talk about exactly what interoperability is. 10th AAMDC takes a deliberate approach to developing long-term interoperability. This is done by breaking down interoperability into three different kinds: human, technical, and procedural interoperability. Human interoperability involves building relationships and engaging frequently with partners to build trust and work together toward a common goal. Technical interoperability is the ability to share date and operate successfully from a common operational picture. Procedural interoperability is the ability to operate successfully under a common Command and Control architecture and under common processes and procedures.

These three kinds of interoperability all function at three different levels: the individual level, the tactical level, and the operational level. The individual level is where human interoperability

starts: key leader engagements and unit exchanges where partners get to know each other and begin building the trust necessary to work together under crisis or conflict conditions. The goal is to build off this trust and set the conditions for successful IAMD operations across the theater together. This means progressing from human interoperability to tactical-level technical interoperability where the ability to share data at the bilateral and multilateral levels is validated. This helps build the capacity for a theater-wide network architecture that everyone can plug into and be aware of all IAMD events that happen across the continent. Once these technical solutions are in place, then the holy grail of interoperability becomes achievable: procedural interoperability at the operational level. This entails the ability to operate together, theater-wide, under the same command and control architecture, effectively employing the same tactics, techniques, and procedures to maximize efficiency and shared understanding. But this can only happen after developing the trust with each other to enable this, and implementing the technical solutions that enable the exchange of data necessary to operate effectively under that common command and control architecture. That is why procedural interoperability at the operational level is the holy grail of interoperability: procedural interoperability builds off successful human and technical interoperability, and being at the operational level enables focusing on functioning at the theater level to be effective anywhere on the battlefield, instead of just regionally or bilaterally.



Operational deployments have demonstrated that procedural interoperability is about more than just command and control of subordinate forces. It is primarily about policies and authorities—at least at the operational level. Our biggest challenge in deploying systems across the Eastern Flank has been achieving a shared understanding of what authorities are required to set conditions for successful tactical operations and threat engagement. This is nobody's fault; it is, rather, a challenge that comes naturally with pursuing interoperability with 30 NATO nations and additional partners—but it is a challenge that must receive more attention across the board. Human Technical Procedural Operational Tactical Individual Building Developing Maintaining Optimal Interoperability.

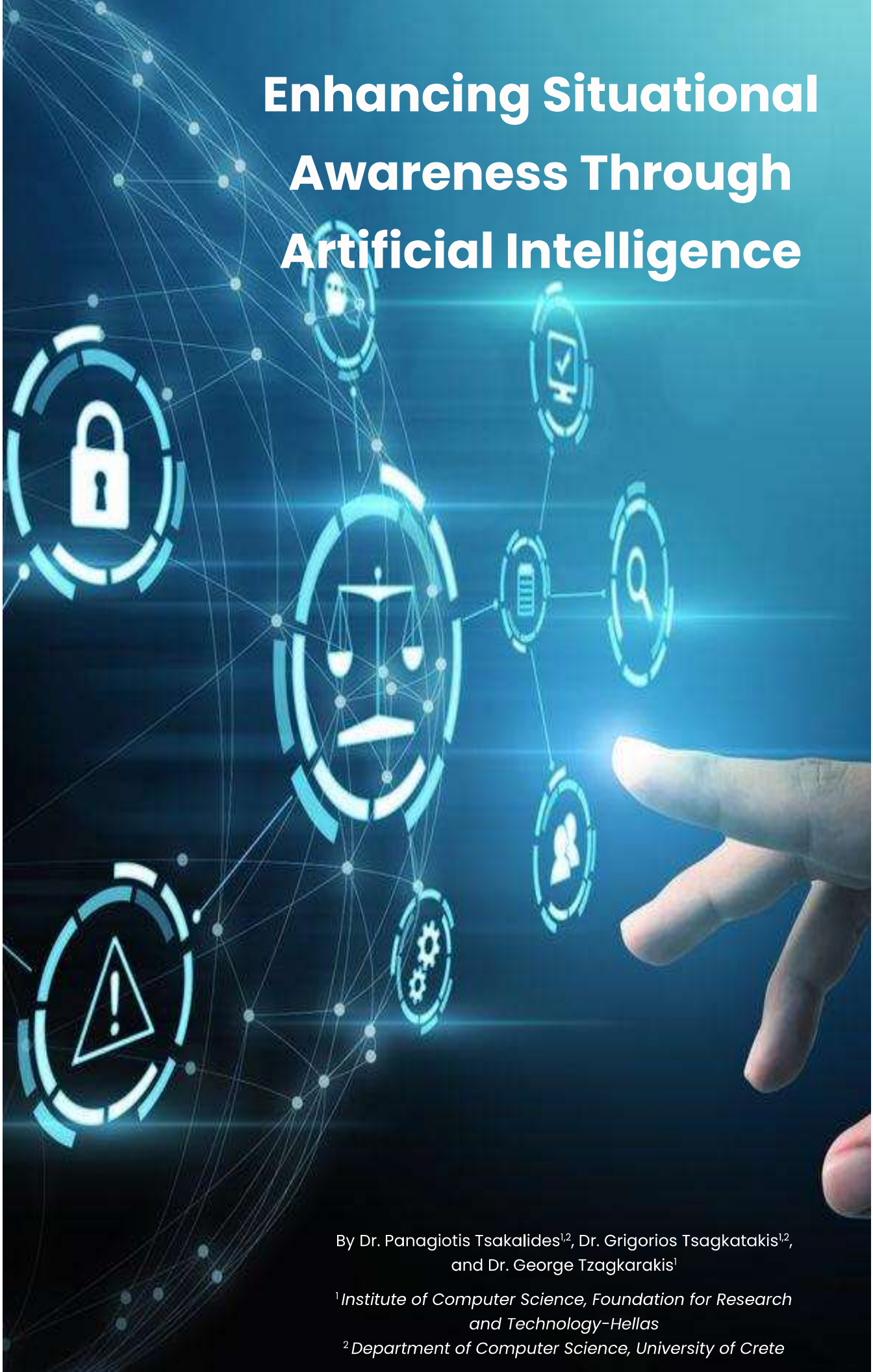
In deploying forces across wide swaths of the Eastern Flank, it is clear that developing procedural interoperability has meant encountering multiple different political contexts, different understandings of the threat environment, different airspace management procedures, and different technical integration challenges. This has made it more difficult to be ready to "fight tonight" if needed, the possibility of which has become more urgent with the Ukraine crisis. Everyone has made significant improvements over the last few years in the ability to demonstrate human, technical, and procedural interoperability at the tactical level. But it is at the operational level, with a focus on integrating forces in crisis environments, rather than just training environments, that should become the main focus. This will require identifying what the ideal authorities and policies will be under a variety of crisis and conflict conditions, demonstrating the importance of those authorities and policies in exercises and tabletop exercises, and then influencing to the extent possible our strategic senior leaders to seek solutions to the authorities and policies problem identified.

Of course, a lot of this will be beyond the control of service members like those within 10th AAMDC and its allies and partners, who lack decision authority over authorities and policy questions. But it is the job of military practitioners to ensure the best military advice is provided to the decision makers. Reaching a shared understanding of what right looks like will help provide that best military advice and improve the chances of it gaining traction with the decision makers. The risk of not getting authorities and policies right and being able to "fight tonight" is significant and has strategic implications. For example, it could lead to inefficiencies in the engagement process that decrease the likelihood of successful defense of critical assets. Another example is that gaps in situational awareness could emerge without the policies that enable sharing data appropriately, reducing decision space for air and missile defense forces to defend critical assets.

This is where the interoperability focus should be moving forward. Collectively, lessons learned in ongoing operations should be applied to important exercises like Ramstein Legacy, NATO's new theater-wide IAMD live exercise designed to focus on operational level issues. Ways should also be found to innovate within current constraints to optimize what is achievable. This is where conferences like this one and tabletop exercises can be immensely useful, bringing our collective strength in human interoperability to bear on the need to improve procedural interoperability. And although these challenges are substantial, they are not insurmountable.

Table of Contents

Enhancing Situational Awareness Through Artificial Intelligence



By Dr. Panagiotis Tsakalides[1,2], Dr. Grigorios Tsagkatakis[1,2], and Dr. George Tzagkarakis[1]

[1] *Institute of Computer Science, Foundation for Research and Technology-Hellas*

[2] *Department of Computer Science, University of Crete*

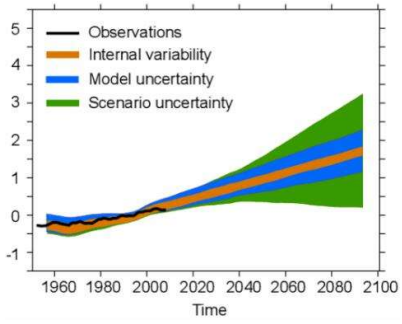
Abstract: Situational awareness (SA) deals with the detection of targets in the environment, the understanding of their nature, and the estimation of their status in the immediate future. From an air-defense perspective, SA refers to the capability to comprehend and project the current and future position of aircraft and surface threats within an airspace. Understanding of geospatial intelligence and information is a key enabler for military SA. As multiple surveillance and reconnaissance platforms and sensors (satellites, synthetic aperture and tracking radars, short and long range UAVs, helmet-mounted displays, microphones, etc.) come online, SA systems face the formidable challenge to collect, analyze and disseminate an ever-increasing volume of rich imagery and multimodal data.

In this paper, we discuss issues related to adaptive SA and dynamic decision-making, which incorporate advanced signal processing, artificial intelligence and data-driven technologies. Big data analytics require innovative high-dimensional, online and robust statistical signal processing and learning methods, as well as scalable, distributed and fault-tolerant systems engineering. These requirements become even more pressing when one considers the heterogeneity of data sources, because of the wide variety of instrumentation, according to which each instrument achieves a different optimal operational point over trade-off curves regarding spatial, spectral, and temporal resolution. The ultimate goal is transforming complex data into meaningful information necessary for informed, mission-critical decision-making.

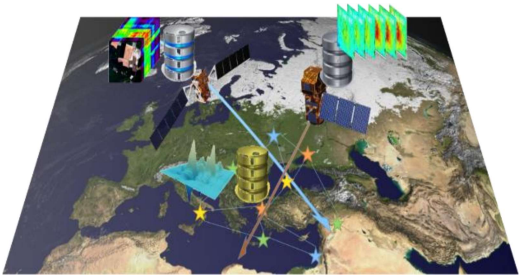
1. Introduction

Situational awareness (SA) constitutes a critical aspect of modern military operations, where the objective is the integration of data from different sources and the delivery of intelligent analysis to operators. Applications of SA include modern battlefields, monitoring of critical infrastructure, homeland security, and defense and disaster response management[1]. In general, three levels of SA have been defined, namely, *Level 1 "Perception"*, which refers to gathering information around the attitudes and dynamics of entities in the surroundings; *Level 2 "Comprehension"*, which refers to the integration of disconnected Level-1 elements and understanding the significance of these elements to specific objectives; and *Level 3 "Projection"*, which refers to forecasting future actions of entities in the environment.

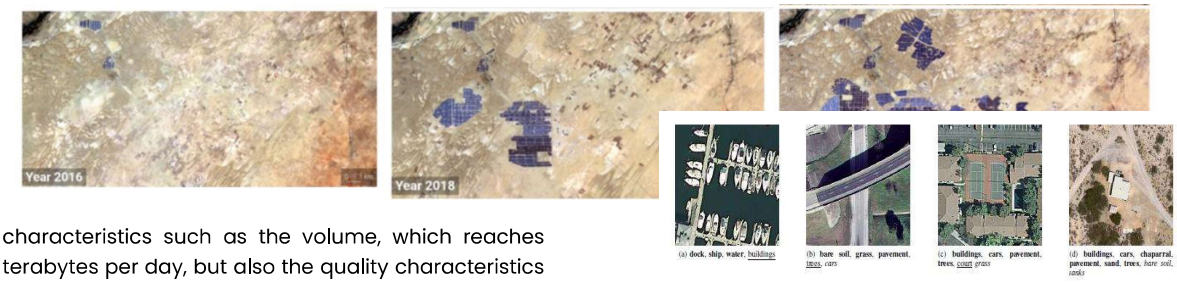
Achieving these goals requires a combination of different data sources, from ground-based sensors to remote sensing platforms like satellites and UAVs. Although the existence of multiple data sources can be beneficial, the characteristics of each must be considered. Ground-based stations have the advantages of measurement accuracy and high sampling frequency. However, measurements of these stations refer to very specific areas. On the other hand, remote sensing technologies achieve global coverage at relatively moderate spatial and temporal resolution.



To achieve the goal of timely and insightful data analysis, a number of key challenges must be addressed. One such class of challenges is related to the different spatiotemporal scales ranging from point measurements to global estimates, as well as the different time scales, from hourly frequency measurements to multi-decadal depth estimates. Another category of challenges has to do with data



[1] *A. Munir, A. Aved, and E. Blasch, "Situational Awareness: Techniques, Challenges, and Prospects," AI, 3(1), pp. 55-77, 2022.*



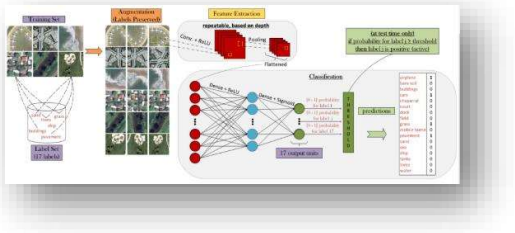
characteristics such as the volume, which reaches terabytes per day, but also the quality characteristics of each system, e.g. its spectral response. Finally, understanding the interactions among different elements is characterized by great uncertainty, both regarding the lack of "objective values" and the uncertainty that characterizes the various forecasts.

2. Artificial Intelligence and Big Data

To address these challenges, the Signal Processing Laboratory (SPL) at FORTH has developed a number of cutting-edge technologies based on artificial intelligence (AI) systems. The training of such models is based on the creation of appropriate datasets that cover as much as possible the diversity of situations that the system will be called upon to deal with[2]. Following the training process, the application of the models can be done with great speed on suitable hardware platforms, offering reliable estimates.

2.1 Remote Sensing Observation Analysis

A major line of research conducted by SPL members is related to the AI-enabled analysis of medium and



high-resolution images from aerial and ESA/NASA satellite platforms. The expertise of SPL includes:

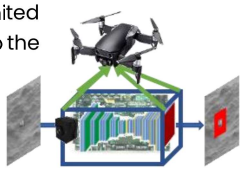
- The fusion of multi-source/multi-modal observations, ranging from active radar to passive imaging.
- The analysis of time series of observations spanning ranges from days to years.
- The integration of space-borne and in-situ observations, focusing on cases of both global-scale in-situ sensing platforms, as well as regional observations.

- The extraction of high value-added satellite-derived products, focusing on high temporal and spatial resolution estimation of critical variables and scene parameters.

We have considered problems such as image classification, where the AI systems we developed can analyze images and provide quantified parameters such as the detection of objects present in an area or the type of land use, and deliver this information in user-friendly formats[3,4]. Our technologies have been validated in the analysis of Synthetic Aperture Radar observations from ESA Sentinel 1, multispectral imaging data from ESA Sentinel 2, and NASA Landsat and MODIS, NASA Global Precipitation Measurement Satellite for rainfall, and ESA Sentinel 5 for high-resolution imagery of cloud parameters.

2.2 Embedded Object Detection and Tracking

We have developed innovative AI technologies based on deep learning for detecting and tracking objects in cluttered scenes, by adapting existing approaches to new imaging modalities (e.g. thermal imaging), under challenging scenarios like limited light, rain, and fog. In addition to the demonstration of these algorithms in ideal scenarios, we have explored how these technologies can be applied in real scenarios including moving platforms, acquiring observations from different viewing points, and motion blur. We have also explored how to deploy AI models "at the edge", where we explored how state-

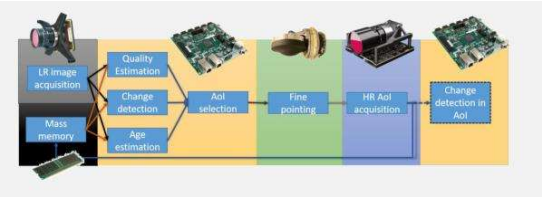


[2] M. Aspri, G. Tsagkatakis, and P. Tsakalides, "Distributed Training and Inference of Deep Learning Models for Multi-Modal Land Cover Classification," *MDPI Remote Sensing, Special Issue on Computer Vision and Deep Learning for Remote Sensing Applications*, 12(17), 2670, 2020.

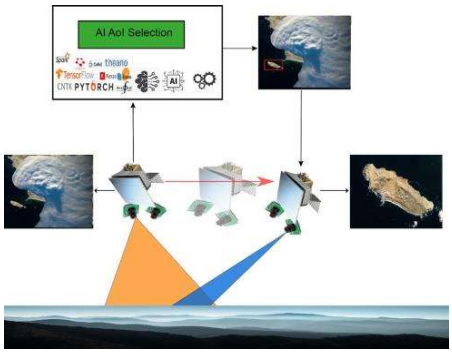
[3] G. Tsagkatakis, M. Moghaddam, and P. Tsakalides, "Deep Multi-Modal Satellite and in-situ Observation Fusion for Soil Moisture Retrieval," in Proc. *IEEE Intl. Geoscience and Remote Sensing Symposium (IGARSS '21)*, Brussels, Belgium, July 12-16, 2021.

[4] M. Giannopoulos, G. Tsagkatakis, and P. Tsakalides, "4D U-Nets for Multi-Temporal Remote Sensing Data Classification," *MDPI Remote Sensing, Special Issue on Computer Vision and Pattern Recognition for the Analysis of 2D/3D Remote Sensing Data in Geoscience*, 14(3), 634, 2022.

of-the-art AI models can be efficiently compressed by employing advanced network design and training techniques like quantization-aware knowledge distillation[5]. Understanding and optimizing with



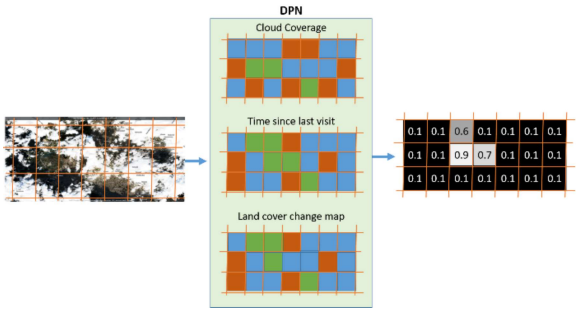
respect to this trade-off is critical when resource constrained devices are employed during the actual



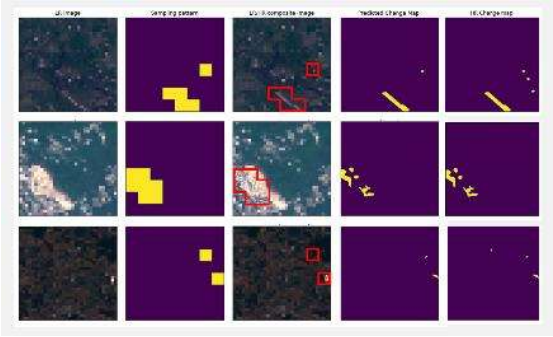
run-time operations.

2.3 AI-enabled Satellite/UAV Tasking

In addition to the analysis of available observations, we have proposed novel classes of missions that can be realized by introducing AI observation analysis on board satellites or UAVs. Moving well beyond existing approaches that focus on the problem of data prioritization (e.g. cloud screening), the developed intelligent observation acquisition aims to maximize different resolution aspects for Areas-of-Interest (AoI). As a representative case study, we consider the implementation of a novel satellite design that envisions platforms equipped with two cameras, one acquiring images over large areas (with low resolution) and a second one focusing on specific areas of interest. In this concept, the decision on which AoI the second camera should select is performed by an intelligent AI-enabled control module that analyses the observations from the first camera in order to provide the necessary signals to the control of the second camera.



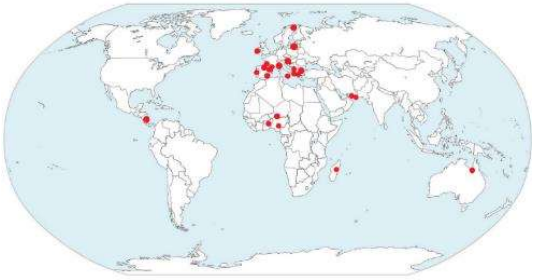
The AI-enabled AoI selection takes the coarse observations from the first camera and executes a process, which assigns a specific value to the different regions. The value is derived from the expected reward associated with taking a specific action, in this case selecting to image at high resolution one or more AoIs. The figure above presents an exemplary set of relevant



data obtained through an initial validation of a proposed scheme on data from the OSCD dataset. Specifically, the top right figure is composed of five columns, where the 1st column shows examples of low-resolution images, the 2nd column the associated analyses, the 3rd column shows a composite of low-high resolution images, column 4 showcases the analysis of the composite images, and column 5 is the actual ground truth.

2.4 Extreme Event Detection and Forecasting

SPL researchers have also developed technologies for the estimation and forecasti

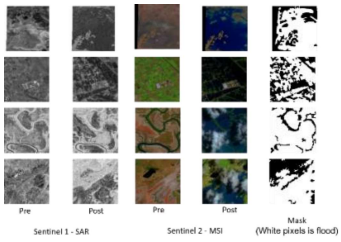


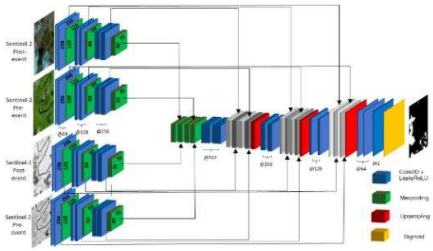
ng of untimely weather phenomena such as the estimation of the extent of flooding events[6]. These technologies have been developed by accepting

[5] *A. Aidini, G. Tsagkatakis, and P. Tsakalides, "Compression of High-Dimensional Multispectral Image Time Series Using Tensor Decomposition Learning," in Proc. 27th European Signal Processing Conference (EUSIPCO '19), A Coruña, Spain, Sept. 2-6, 2019.*

[6] *G. Drakonakis, G. Tsagkatakis, K. Fotiadou, and P. Tsakalides, "OmbriaNet: Supervised Flood Mapping via Convolutional Neural Networks Using Multitemporal Sentinel-1 and Sentinel-2 Data Fusion," IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing, 15, pp. 2341-2356, 2022.*

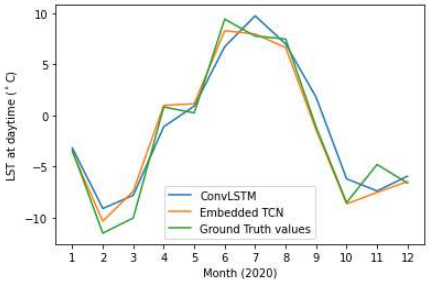
observations f rom areas of interest before and after the occurrence of the phenomena, and estimating their extent. Such models have been trained using data from extreme events that have taken place in many different regions of the planet over different time instances. Specifically, we have compiled a dataset that contains a total number of 2776 examples, which consists of Synthetic Aperture Radar imagery from Sentinel-1, and multispectral imagery from Sentinel-2, accompanied by ground truth binary images produced using data derived from experts and provided by the Emergency Management Service of the Copernicus Program. The dataset covers 20 flood events around the globe, from 2017 to 2020.

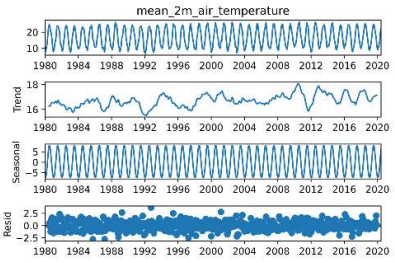




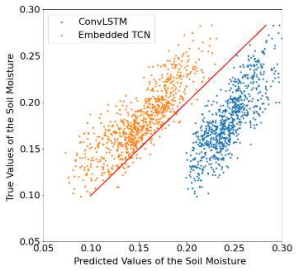
The model can detect changes between land/permanent water and flooded water, exploiting the temporal differences among flood events extracted by different remote sensing platforms. The model achieved 90% accuracy in automatically detecting flooding at 10-meter spatial resolution. These systems are being expanded to be able to offer automated and reliable risk assessment of various phenomena with the aim of early prevention.

2.5 Retrieval of Essential Climate Variables





We have also explored the problem of essential climate variable estimation, where we have developed AI models capable of aggregating different measurements, producing estimations of the uncertainty associated with each estimate, and finally the consistency of the estimates with existing computational models based on physical laws[7]. Such parameters of interest include land surface temperature, surface and subsurface soil moisture, and solar irradiance. The developed model achieves x2 reduction in retrieval error at x9 finer spatial scales compared to gold-standard NASA products for the case of retrieval. Furthermore, the developed AI model surpassed the performance of state-of-the-art methods in this domain by more than 10% prediction error reduction (mean squared error) when evaluated on soil moisture and surface temperature prediction. It is worth mentioning that the technologies are generic and thus they can be employed for the prediction of a large number of different geo-bio-physical parameters.



3. Conclusion

The data collected by a multitude of intelligence, surveillance and reconnaissance sensors enhance SA and help to better understand the environment and its threats. However, a variety of factors, including incompatible data formats, bandwidth limitations, sensor persistence and revisit rates, hinder SA enhancement through the use of big data. AI can help with real-time analysis and prediction, and it can provide actionable intelligence and assistance in decision-making. Furthermore, with the ever-increasing amount of sensor data, AI can identify the most significant pieces of information, fuse that information and present it to the end user in a suitable format. ■

[7] *M. Villia, G. Tsagkatakis, M. Moghaddam, and P. Tsakalides, "Embedded Temporal Convolutional Networks for Essential Climate Variables Forecasting," MDPI Sensors, Special Issue on Machine Learning, Signal, and/or Image Processing Methods to Enhance Environmental Sensors, 22(5), 1851, 2022.*

IAMD and Cyber-Space Threats

If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.
- Sun Tzu, The Art of War

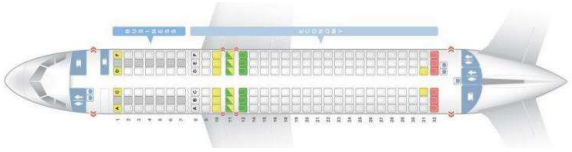
By Mr. Sozon A. LEVENTOPOULOS
CISSP, CASP+, CEH, ISO 27001 LA, NET+, SEC+

Introduction

The importance of information in the military operations, has been recognized from the early years of civilization. Military theorists and strategists, like Thucydides, Sun Tzu, Clausewitz, have outlined and emphasized upon that axiom. While everybody agreed upon that axiom, there was little that could be done in order to achieve what is called as "information dominance", up until a few decades ago. Today, we are not dealing with the lack of information, but on the contrary, the "abundance" of it. Now, we have the ability to collect, manipulate, process, and store far more data that ever before, but as our reliance upon that lifecycle grows, vulnerabilities also grow. Cyberwarfare is a modern term created to describe exactly this reality.

Background

Data can be described as a summary of recorder symbols; therefore, data are meaningless. When I will accompany data with a meaning or a notion, then data are transformed into knowledge. We can say then, that "information is Data in Concept". A typical example is with the seats in an airplane: What do these numbers mean? 2A 2C 6F 9D 12B 18B 18E 20C 21A 22D 25F 26E 31B, without a context it is impossible to tell…



In that view we can describe information security as the quality that keeps valuable and sensitive information protected. It mainly aims in protecting/safeguarding **the Confidentiality, Integrity, and Availability of every bit of information**. On the other hand, **cybersecurity** is the **art** of protecting networks, devices and data from unauthorized access or criminal use. Usually, these two terms will be used interchangeably, and often in the wrong context.

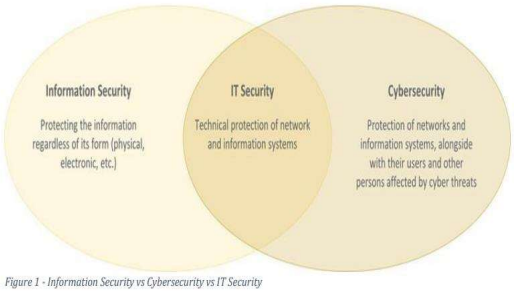


Figure 1 - Information Security vs Cybersecurity vs IT Security

A **hacker** is a person skilled in information technology who uses their technical knowledge to achieve a goal or overcome an obstacle, within a computerized

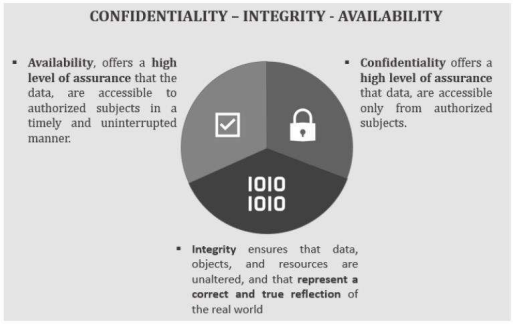


Figure 2 - The CIA triad. Confidentiality - Integrity - Availability

system by non-standard means. Though the term hacker has become associated in popular culture with a security hacker – someone who utilizes their technical know-how of bugs or exploits to break into computer systems and access data which would otherwise be unavailable to them – hacking can also be utilized by legitimate figures in legal situations. There are many types, script-kiddies (the kid refers to their skills, not their age), cyberterrorists, state-sponsored actors, etc.

Cyberwarfare

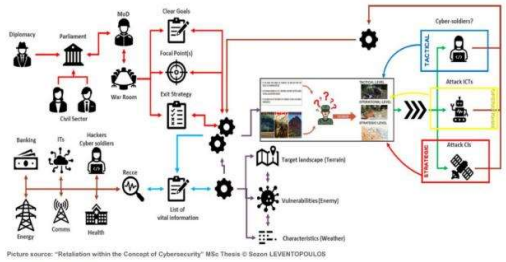
For millennia wars were fought either on land or in the sea. It was in the early 20th century, that a new domain was introduced, that of the air, and after a couple of decades a fourth domain, space has also been identified. Today, a fifth domain, that of the **cyberspace** is emerging prominently as a warfighting domain. While, there are dozens of definitions describing what cyberspace is, Kuehl's definition is considered as the most comprehensive.

> **"a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies"**

It is crucial to understand that cyberspace is a **critical element of current and future military operations**. Among others, cyberspace forms a key operational medium with strategic importance and influence. It is also paramount that we include both **electronics and the electromagnetic spectrum within the realm of cyberspace**.

We can define **cyberwarfare** as the use of digital attacks against a state with the possibility to cause comparable harm to traditional kinetic warfare by the disruption of vital information, communication systems, and infrastructure.

While **cyberwarfare as a concept is still debatable**, most countries have developed active cyber units capable of both offensive and defensive cyber operations. Furthermore, there is debate as to whether cyberwarfare is distinct or not from the term cyber war. It is implied that cyber war typically refers to a long period of time, where multiple offensive and defensive operations or cyberwarfare-related operations are taking place.
Having said that, we need to also clarify that cyberspace is *non sine qua* for cyberwarfare. An insider threat, a spy with physical access to the server, or a kinetic attack, can still be identified as cyberwarfare.



Picture source: "Retaliation within the Concept of Cybersecurity" MSc Thesis © Sozon LEVENTOPOULOS
Figure 3 - At cyberwar!

Information Warfare (a "new" form of war?)

In November 2, 1988 the oldest worm in internet history was unleashed. Its creator, Robert Tappan Morris[1], who was the first person convicted under the then-new Computer Fraud and Abuse Act, said that he created the worm simply to see if it could be done. During the same period the concept of a "revolution in military affairs" emerged in the then Soviet Union, which described a "military technical revolution" which could dramatically improve lethality as well as the capabilities of conventions weapons. Within the same scope and a decade earlier it has been identified in the U.S. Military that "data links, computer assisted intelligence evaluation, and automated fire control…[2]" will be used in the future to search for, lock, and engage enemy forces. It is worth to say that the microprocessor (the core of modern computers) was invented two years after this declaration.

Today, information and communication technology as a whole, are considered a key enabler. Current command structures (C4I, ISTAR, etc.) together with the integration of all weapon-delivery platforms have created the "**all-domain approach**". A new approach in the form of **Hybrid Warfare** was also introduced, which extends the concept of cyberwarfare. In that view, different ways of warfare including conventional and, irregular tactics and formations, terrorist acts, and criminal disorder conducted by both sides along with a variety of nonstate actors. **In such a form of warfare all efforts, including conventional military operation are subordinate to an information campaign.**

Legal Considerations

From a legal point of view, cyberspace is similar to international waters. No entity or country can claim ownership or dominion upon cyberspace, but the physical infrastructure installed in any given country falls within its jurisdiction (the sovereignty principal applies to both the physical infrastructure and the data stored/processed/collected within or with the aid of said infrastructure).

The sources of international law are clearly defined in Article 38(1) of the Statute of the International Court of Justice. Four sources are identified:

i. international conventions/treaties;
ii. International custom;
iii. General principles recognized by civilized nations;
iv. Judicial decisions and the teachings of the most highly qualified publicists.

United Nations Security Council (UNSC) is one of the principal organs of the United Nations. Its main mission is to **ensure international peace and security. It is one of the most powerful organs within the United Nation's ecosystem, since it the only part of the UN ecosystem with the authority to issue binding resolutions to its member states.** In that view, it can direct the establishment of peacekeeping operations, enact international sanctions, and **authorize military action.**

The International Court of Justice (ICJ) is one of the principal organs of the United Nations. Its primary mission is to settle disputes between states, with its decisions being based upon international law principles. It supports the work done by the United Nations, by providing advisory opinion. In that view, **ICJ's professional opinions are one of the primary sources of international law.**

The Law of Armed Conflict

The United Nations general assembly resolution 3314 (XXIX) defined and adopted by consensus the definition of aggression, which is described as the use of armed force by a state against the sovereignty, territorial integrity, or political independence of

[1] *Interestingly, Morris' father, Robert Morris, was a computer scientist at Bell Labs and later chief scientist at the National Computer Security Center of the National Security Agency.*

[2] *This quote comes from General William Westmoreland testifying in a Congressional hearing in 1970.*

another State. In 2010, the Rome Statute of the ICC has used this definition in the relevant elements comprising the crime of aggression. Article 2 of the United Nations Chapter, forbids the use of force, and asks states to refrain from the threat of use or actual use of force in their international relations, with some notable exceptions (e.g., authorized by the UN's Security Council, as an act of individual or collective self-defense, etc.)

Jus in Bello (or International Humanitarian Law - IHL), is the part of international law, that governs how warfare is (or should) be conducted (Corn and Al, 2012). Its main purpose is to limit the suffering caused by war. To achieve that, it provides protection and assistance to the victims of war, as far as possible. Jus in Bello recognizes the reality of a conflict and regulates only those aspects that are of humanitarian concern.

Jus ad Bellum, is Latin for "right to war". It has been identified early in the history of International Law, that while war is an unwanted situation, there are times when States, need to respond with force. In that view, Article 51 (Kunz, 1947) of the UN Charter clearly states that:

"*Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations until the Security Council has taken measures necessary to maintain international peace and security*"

Jus ad Bellum defines the criteria that need to be considered before the State is engaged in war. Nevertheless, there are four basic principles, that need to be taken into account: proper authority and public declaration, just cause, probability of success, and last resort.

Key Considerations

- **State Responsibility**: The requirements for retaliatory actions are described extensively in the Articles on State Responsibility by the International Law Commission. The key requirement is that the offended State shall apply such measures, as to convince the "responsible" State to refrain from its unlawful actions.

- **Armed Attack:** Articles 2(4) and 51 of the United Nations Charter are applicable only in the case of an armed attack. As a general rule we can argue that for a cyberattack to be identified as an "armed attack" or as a "use of force", its consequences should resemble that of a conventional one.

- **Non-intervention**: The principle of non-intervention prohibits States from coercively intervening in affairs reserved to another State.

- **Sovereignty**: Arguably, a cyber operation will breach the rule of State sovereignty under two conditions. If it causes damage to the cyber infrastructure in that State or if it will permanently interfere with its functionality. Secondly, if the cyber operation will interfere with the State's exclusive right to exercise the functions of a State within its own territory.

- **Proportionality**: Any action taken that is not proportionate to the original action that triggered the retaliation, would automatically be identified as unlawful, thus be considered as revenge. As a rule of thumb, a retaliatory action of the same nature, or similar in nature to the unlawful act against which is directed will be most likely identified as proportionate.

- **Attribution**: As the example of the "Olympic Destroyer" malware showed, attribution in cyber-space can be an extremely difficult or even impossible act. Attribution, is a critical element of deterrence, and failure to do so will either be seen as a failure to punish the guilty, or – if accusing the innocent – as erosion of the legitimacy of the actions. Further, in the case the retaliation action will be publicly announced (as to enhance deterrence) 3rd parties and the international community, together with the State's population need to be convince regarding the legitimacy of the actions. Olympic Destroyer is malware that was used by Sandworm Team against the 2018 Winter Olympics, held in Pyeongchang, South Korea. The main purpose of the malware was to render infected computer systems inoperable. The malware leverages various native Windows utilities and API calls to carry out its destructive tasks. Olympic Destroyer has worm-like features to spread itself across a computer network in order to maximize its destructive impact.

Take Aways

In 2007, Estonia was hit by a DDoS attack on a massive scale. This attack is considered now, as **Web War I**. In 2008, Russia implemented a cyber-campaign alongside conventional military operations in Georgia (S. Ossetia). This is now known as **Hybrid War I**. In 2010, STUXNET malware managed to crimple Iran's nuclear weapon program. Today, STUXNET is considered as **CYBER WEAPON I**. Today, Russia had launched a massive offensive against Ukraine. The first targets were Data Centers, ISPs, and relevant CII, which were hit by a combination of cyber and kinetic attacks. Misinformation and disinformation actions/campaigns are still ongoing. Perhaps, this will be known as **INFORMATION WAR I**.

Key considerations:

▪ The required technology and knowledge are already in place and can support a FULL SCALE CYBERWAR.

▪ The introduction of space and cyberspace as the 4th and 5th domain of operations, have drastically changed how we perceive military operations.

▪ Cyber-attacks can be very targeted (no collateral damage), non-lethal, proportionate, etc., thus fulfilling most (if not all) of International Law provisions (attribution can be a challenge). Therefore, they can be considered as the "weapon of choice" in a number of scenarios.

▪ Cyberspace IS NOT ISOLATED from the rest of the domains. Therefore, a new term, that of the **INFOSPHERE** has been introduced.

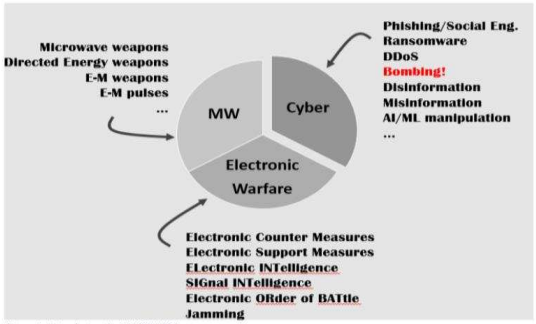


Figure 4 - Introducing the INFOSPHERE

▪ Cyber-warfare can be seen as the **nuclear deterrence of the 21st century**. For decades the Mutual Assured Destruction, or MAD had dominated global peace and security. The importance of information in everyday social, private, and economic life, had paved the ground for cyber-attacks and cyber-warfare to rise to prominence. Therefore, cyber-warfare is a reality, that will continue to evolve in the next years. As such, no one is safe, and no one is too big to fail.

▪ Cyber-warfare provides a number of advantages when triggered. Attribution should be considered as a key principle as seen from the scope of international law, and can be from extremely difficult, to impossible to be validated. Cyberwarfare can create significant damages (even in the physical domain), but not the destruction created from conventional warfare. Finally, cyber-warfare can be very targeted and very specific, minimized collateral damages to both physical and digital infrastructures. Furthermore, cyberwarfare can reduce human casualties to zero. Consequently, resorting to cyber-attacks can be proved as the only appropriate solution.

▪ While most of the scholars would agree that the International Law (and consequently, the Law of Armed Conflict) are applicable to the cyberspace (the most notable example here is the Tallin Manual 2.0), there is no single piece of legislation from either the UN Security Council or the International Court of Justice directly related to cyberspace. Tallin Manual, provides only an opinion and could and should not be considered as a source for international law. The only, closely related decision, comes from the International Court of Justice, which had ruled that anything can be categorized as a "weapon", provided that a number of prerequisites are fulfilled.

▪ **Cyberspace in general, lacks standardization**. Even the correct spelling (with hyphen or not) is still debatable. ENISA has launched in 2015 a relevant initiative to provide certain frameworks and standardization in cyberspace. Still, no tangible results can be identified, and in order to facilitate standardization in the cyberspace, a global initiative is needed.

▪ **Attribution**: As the example of the "Olympic Destroyer" malware showed, attribution in cyber-space can be an extremely difficult or even impossible act. Attribution, is a critical element of deterrence, and failure to do so will either be seen as a failure to punish the guilty, or – if accusing the innocent – as erosion of the legitimacy of the actions. Further, in the case the retaliation action will be publicly announced (as to enhance deterrence) 3rd parties and the international community, together with the State's population need to be convince regarding the legitimacy of the actions.

▪ **Weapon of choice**: Can be extremely targeted and focused. Can be tailored in such a way to inflict limited to no, collateral damage. Can be either "loud" or "stealth" as to either promote deterrence, or limit further escalation or counter-retaliation. ■

Further Reading

Libicki, M.C. (2021). Cyberspace in peace and war. Annapolis, Maryland: Naval Institute Press

Schmitt, M.N. and NATO Cooperative Cyber Defense Centre Of Excellence (2017). Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge, United Kingdom; New York, Ny, USA: Cambridge University Press.

Greenberg, A. (2020). SANDWORM: a new era of cyberwar and the hunt for the kremlin's most dangerous hackers. S.L.: Anchor.

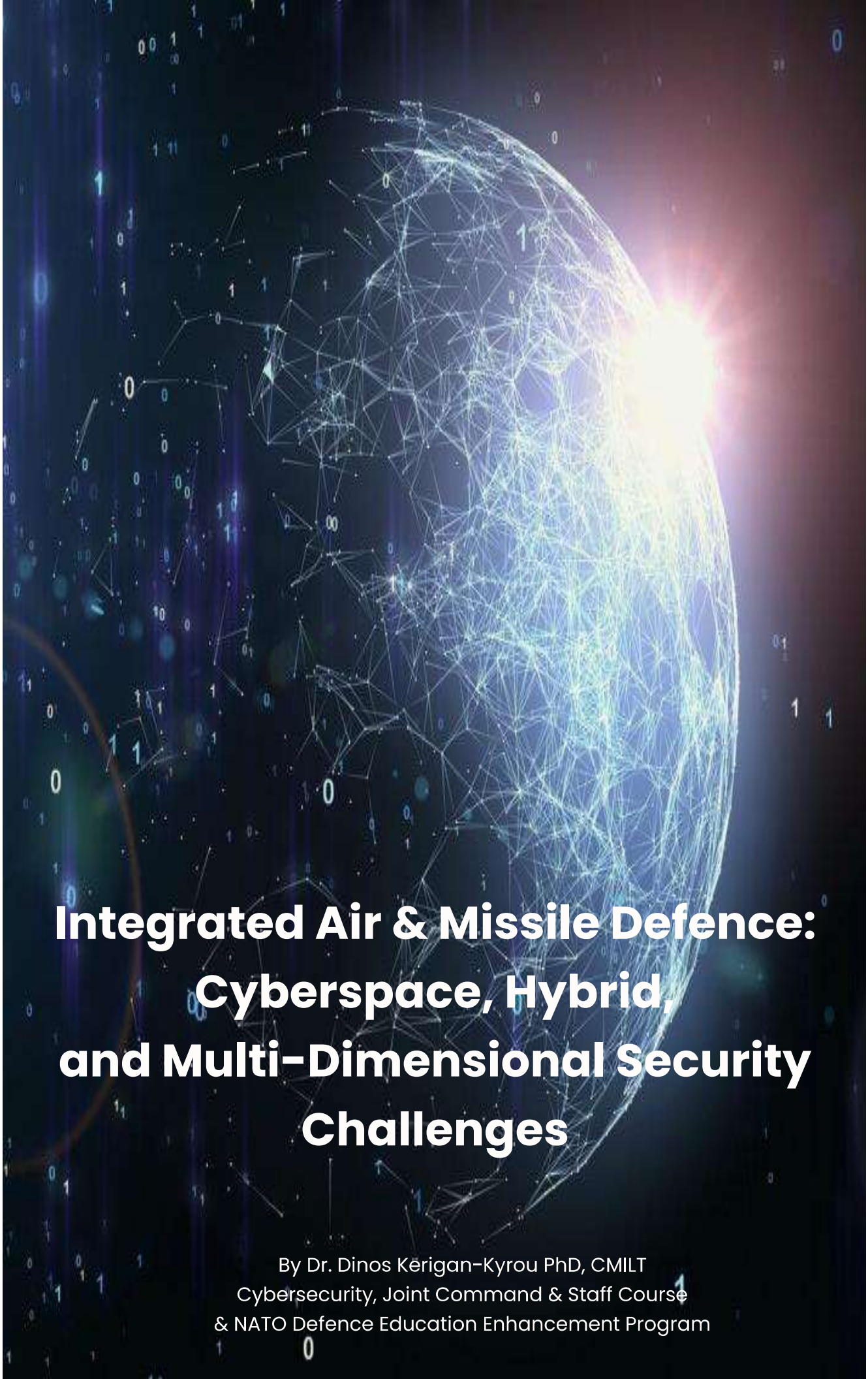
Perlroth, N. (2022). THIS IS HOW THEY TELL ME THE WORLD ENDS: the cyberweapons arms race. S.L.: Bloomsbury.

Mitnick, K.D. (2019). The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data. New York: Little, Brown & Company.

Mitnick, K.D. (2003). The art of deception: controlling the human element of security. New York; Chichester: Wiley.

Hacking : the Art of Exploitation. (2007). Erscheinungsort Nicht Ermittelbar: No Starch Press, Us.

Cunningham, C. (2020). Cyber warfare - truth, tactics, and strategies: Strategic concepts and truths to help you and your organization survive on the battleground of cyber warfare. Birmingham: Packt Publishing.



Integrated Air & Missile Defence: Cyberspace, Hybrid, and Multi-Dimensional Security Challenges

By Dr. Dinos Kerigan-Kyrou PhD, CMILT
Cybersecurity, Joint Command & Staff Course
& NATO Defence Education Enhancement Program

The paper is going to focus on broad aspects of cybersecurity regarding NATO Integrated Air and Missile Defense.

I'll start first with an explanation of hybrid threats and how they are shaping everything that ishappening in security.

Next we will look at what cybersecurity is. (And it's not about computers, software, and antivirus). And we'll look at how our whole approach to cyberspace - the online environment in which we all live andwork - shapes the security of everyone and everything, including all that happens at NATO.

We will then look at specific challenges we face - particularly how individuals are being targeted by nefarious actors across NATO, the EU, Partner Nations, and those within the supply chains on which Integrated Air and Missile Defense depend.

We will then conclude by looking at some ideas on how we address these challenges

At this conference there are many outstanding presentations and discussions concerning NATO's Integrated Air and Missile Defence Systems. So I'm not going to try and replicate any of these presentations. What I'm aiming to do is to look broadly at new and emerging threats that we are facing -particular in cyberspace - and how these directly affect our missile systems. (Please note: The footnotes are crucial to reference in order to properly understand this paper).

The terms 'cyberspace', 'cybersecurity' and 'hybrid threats', 'hybrid challenges and hybrid warfare'' are used regularly but understood rarely.

A very good definition of exactly what 'hybrid' means was given by former US Sec of State Madeleine Albright in her report for NATO over 10 years ago, *NATO 2020: Assured Security; Dynamic Engagement*.[1] Sec Albright highlights new and emerging threats as a 'blurring', of threats which are military, and those which were not traditionally seen as concerning the military. The distinction between the two, she argued, is becoming less and less clear. Such threats include, but are not limited to: energy security, threats from terrorism, changing health challenges (including pandemics), climate change and associated security problems arising from changes in our environment.[2]

Cybersecurity is a term which is repeatedly used and yet rarely explained properly. But cybersecurity is interlinked with hybrid / new and emerging threats because it is central to all of them.

Repeatedly we hear that cybersecurity concerns computers, computer networks, and software. This is explanation is both wrong and dangerous. For while computers and their networks are indeed a crucialcompetent of cybersecurity, this explanation is like saying that the engines are the only component of an aircraft. The engines are critical - but there are a multitude of other factors that create a safe aviation environment. And yet, when it comes to cybersecurity it's like we only focus on the engines without thinking about air traffic control, pilot training, meteorology, airports, runways, landing systems and the hundreds of other factors which comprise safe aviation. And this general assumption that cybersecurity is only about computers and software creates huge dangers for us across NATO, our Partners, the EU, and within our nation states - at every possible level.

This 'narrow' and ill-defined explanation of what

[1] Madeleine Albright, *NATO 2020: Assured Security; Dynamic Engagement: Analysis and Recommendations ofthe Group of Experts on a New Strategic Concept for NATO* (Brussels: NATO, 2010), www.nato.int/cps/en/natolive/official_texts_63654.htm?selectedLocale=en

[2] For a complete and comprehensive overview of all hybrid threats we face, see the NATO / European UnionHybrid Centre of Excellence, Helsinki, at: https://www.hybridcoe.fi/hybrid-threats/ and www.hybridcoe.fi/publications-and-readings/

See also: Dinos A. Kerigan-Kyrou, "Protecting Cyberspace: A Hybrid Threat Requires a Hybrid Response" AnCosantóir - Irish Defence Forces 79, no.4 (May 2019): 18-19, www.dfmagazine.ie/2011-2/
Yuriy Danyk, Tamara Maliarchuk, and Chad Briggs, "Hybrid War: High-tech, Information and CyberConflicts," Connections: The Quarterly Journal 16, no. 2 (2017): 5-24.
Office of the Director, National Intelligence, Annual Threat Assessment of the U.S. Intelligence Community,February 2022 (Washington: Office of the DNI, 2022), www.intelligence.gov/ic-annual-threat-assessment

cybersecurity is avoids the main issue affecting allof us in this room today and those we work with; and that is: Cybersecurity is about the security of cyberspace – the online environment in which *everyone* lives and works.[3]

Cyberspace is utilized by nefarious actors for a wide range of reasons and motivations.

These nefarious actors include criminals who want to steal money from you, your family, your business or organisation. They include those that want to harm children and other vulnerable people. Nefarious actors in cyberspace include criminals and terrorists who use cyberspace for the funding of illicit activity - whether it's drug smuggling, human trafficking and modern slavery, piracy, historicalartifact and wildlife trafficking.

The communications apps used by criminals and terrorists in cyberspace are as secure - sometimes more secure - than anything we use in the military; the military and law enforcement often have no idea whatsoever what nefarious actors are doing or planning. And unlike our military communications systems which cost millions (and take years to tender for and buy), the apps and communications systems used by terrorists and criminals cost nothing whatsoever and are available right now on any smartphone.

Terrorists use cyberspace for disinformation, recruitment, 'advice' and planning of atrocities. Hostile states use cyberspace for propaganda, disinformation and gaining access to both military networks and - increasingly - the personal devices of military personnel; our phones, smartwatches, and the multitude of devices we all have at home, in our cars and on our wrists, so that they can hear and seeall that we are doing.

Cyberspace enables nefarious actors to access weapons and the means to cause harm which were unthinkable just a few years ago. Cheap off-the-shelf drones are increasingly used by terrorists - andhostile states - for transport and logistics, reconnaissance, and the actual execution of atrocities.

Indeed, a modern smartphone contains GPS navigation, accelerometers, gyroscopes, and motion detectors; all of which can be used to weaponize an IED, or a UAV, or to produce an improvised missile. Terrorists can now obtain the latest technology for just hundreds of dollars. In other words, terrorists and other criminals now have access to many of the technologies we have at NATO and theEU - all available via and enabled by cyberspace.

Cyberspace is *the* platform via which all these threats manifest themselves; the 'weaponization ofeverything' as described Dr Mark Galeotti.[4]

As well as enabling new methods of weaponization, cyberspace also links everything we do as individuals. Our smartphones, smartwatches, alarms, door locks, door cams and home security, even our refrigerators, are all connected online. And it's not only devices we individually use; our nations' critical infrastructures,[5] industrial control systems, and NATO weapons systems including drones, radar, navigation and logistics systems, vehicles, and integrated air and misled defence are all increasingly controlled and operated online.

NATO's Network, Communications, and Information Agency - NCI - does a superb job protecting NATO's computing, Information Technology, and Operating Technology networks for our Air and Missile Defense. NCI provides this support though NATO Air Command and Control (AirC2) and Ballistic Missile Defence (BMD) operations. This critical NCI capability supports and enables NATO to plan, execute and monitor all air operations, including those defending the Alliance against a missile attacks.[6]

[3] For the broad range of threats we face in cyberspace, see: John P. Carlin, Dawn of the Code War (New York: Public Affairs, 2019). Also see: Dinos A. Kerigan-Kyrou, "Defining Our Approach to Cybersecurity." An Cosantóir - Irish Defence Forces 78, no.1 (January 2018): 18-19, www.dfmagazine.ie/2011-2/
For continually updated crucial cybersecurity information, including national strategies and the latestpublications, see the NATO Cooperative Cyber Defence Centre of Excellence, at: www.ccdcoe.org

[4] Mark Galeotti, The Weaponisation of Everything: A Field Guide to the New Way of War (New Haven: YaleUniversity Press, 2022).

[5] Critical infrastructure includes - but is not limited to - supply and distribution of energy, health systems and emergency response, transport, food and clean water supply, and communications including cyberspace. See:Cybersecurity & Infrastructure Security Agency (CISA), list of Critical Infrastructures, at: www.cisa.gov/critical-infrastructure-sectors

[6] See; NCI 'Air and Missile Defence Command and Control' at: https://www.ncia.nato.int/what-we-do/air-missile-defence.html

But despite this outstanding work done by NCI there are further security challenges facing thesecurity of our Missle Defence Systems - all of which occur via cyberspace.

Weapons and support systems such as transport, energy, logistics, heating and air conditioning, supplies, etc are increasingly operated online. The Operating Technology underpinning these systems operates via the internet. The computers and software within these systems known as SCADA Systems, are used everywhere and in every environment.[7] Contrary to popular option there is no separate, 'secure' internet for 'critical' operations – it's the same internet that everyone uses for watching Netflix and posting on Facebook. The internet is - essentially - one giant computer system to which everyone in the world is connected. And this system was not built with security in mind. We are continually having to add cyber defence to make cyberspace as secure as possible. And all of thesesystems are part of the supply chain for air and missile defence. If a nefarious actor targets a supply chain they enter a 'ring of trust', in the words of the US NSA. Thus, to target air and missile defence aterrorist or hostile state need not target the *actual* system, but need only target an operator within the supply chain.[8]

Second, the vast majority of cybersecurity breaches occur via individuals - not some sophisticated 'hack' involving complex code.[9] Individuals within our trust network are targeted, normally by a spear-phishing email pretending to be from a person in a superior position, such as a commanding officer. And who is not going to open an email they really think is from their CO? It takes just one cleverly targeted email and the nefarious actor is in your system. And the idea that it is only the unwary and the clumsy that will click on a fake link or accidently open a file from a terrorist or hostilestate is total nonsense. As UK based ethical hacker Mike Godfrey correctly states: the right spear- phishing email, targeted at the right person at the right time works **every** time. Current 'phishing training' - of the type we all have to endure - is outdated, based on fear, counterproductive, and essentially worse than useless.

A third problem are the devices we use every day at home at work, in our cars, on our ships, planes, vehicles, and indeed all the places we work in our military environments - often called IoT - the Internet of Things. The security on these devices, in general, is abysmal. We allow apps on our devices to record and monitor all we do. Our phones, smartwatches, the devices we use to listen to music, TVs....all have camera and microphone access. These devices are targeted directly by nefarious actors. Moreover, miliary personnel are increasingly being targeted online with social engineering, where our adversaries - be they terrorists, hostile states, criminals (or combinations of all three) - gain our trust and confidence, allowing them access to our lives at home and at work.

Extortion and blackmail, especially 'sextortion', where a fake profile on a dating site blackmails thevictim, is becoming an increasingly common way for nefarious actors to gain access to our systems and all we do.

In short, they - the bad guys - don't need to 'hack' our missile systems in order to gain access. Why try and go through a securely locked door when they can just hop over a tiny little fence?

So we should give up? Not at all. The answer is to re-shape and re-think how we approach security. Essentially, the solution is **to enable each and every person in our NATO and Partner organisations to become part of the defence**. This means that everyone – regardless of rank or 'status'- needs be able to report problems and security concerns in a **wholly no blame environment -** even (and especially), where someone has made an error. We all make cybersecurity errors. Anyone who says that they or

See also, EU European Defence Agency (EDA), "Future Capabilities", at: https://eda.europa.eu/docs/default-source/eda-publications/futurecapabilities_cdp_brochure
EU Permanent Structured Cooperation, at: www.pesco.europa.eu

[7] See: Robert M. Lee, SCADA and Me: A Book for Children and Management (Scotts Valley: CreateSpace,2013).
See also: Stefan Lüders, CERN, Geneva "Why Control System Cyber-Security Sucks...", Presentation at the Black Hat Conference, Las Vegas, USA, 2014, at: www.youtube.com/c/BlackHatOfficialYT

[8] For a discussion of supply chain security see: Rob Joyce, NSA, "View from the National Security Agency," interview by Suzanne Kelly, Cyber Initiatives Group Spring Summit, May 25, 2022, (Official Cyber InitiativesYouTube Channel), video, 30:09, www.youtube.com/watch?v=e-Sko0Kersc

[9] For an excellent analysis and explanation see Dr Jessica Barker, Cygenta, "Fear and Loathing in Cybersecurity: An Analysis of the Psychology of Fear", RSA Conference, San Francisco, 2020, at: www.youtube.com/c/RSAConference

their organisation has never been breached, or that they never make any cybersecurity errors, is either a liar or totally deluded.

We must take cybersecurity lessons from aviation, especially what Comdt Frank Byrne, Irish Defence Forces Air Corps, calls the 'Just Safety Culture', where the reporting of errors is encouraged and honest mistakes are never punished, thereby allowing everyone to learn.[10] It is the *organizational* approach which needs to rapidly adapt and change, if we're to develop cybersecurity for our air and missile systems - and all military systems across NATO.[11]

By doing this we create a complete defence against our adversaries by utilizing all our people - ratherthan presenting multiple opportunities for hostile actors to gain access to our systems, networks, and people.

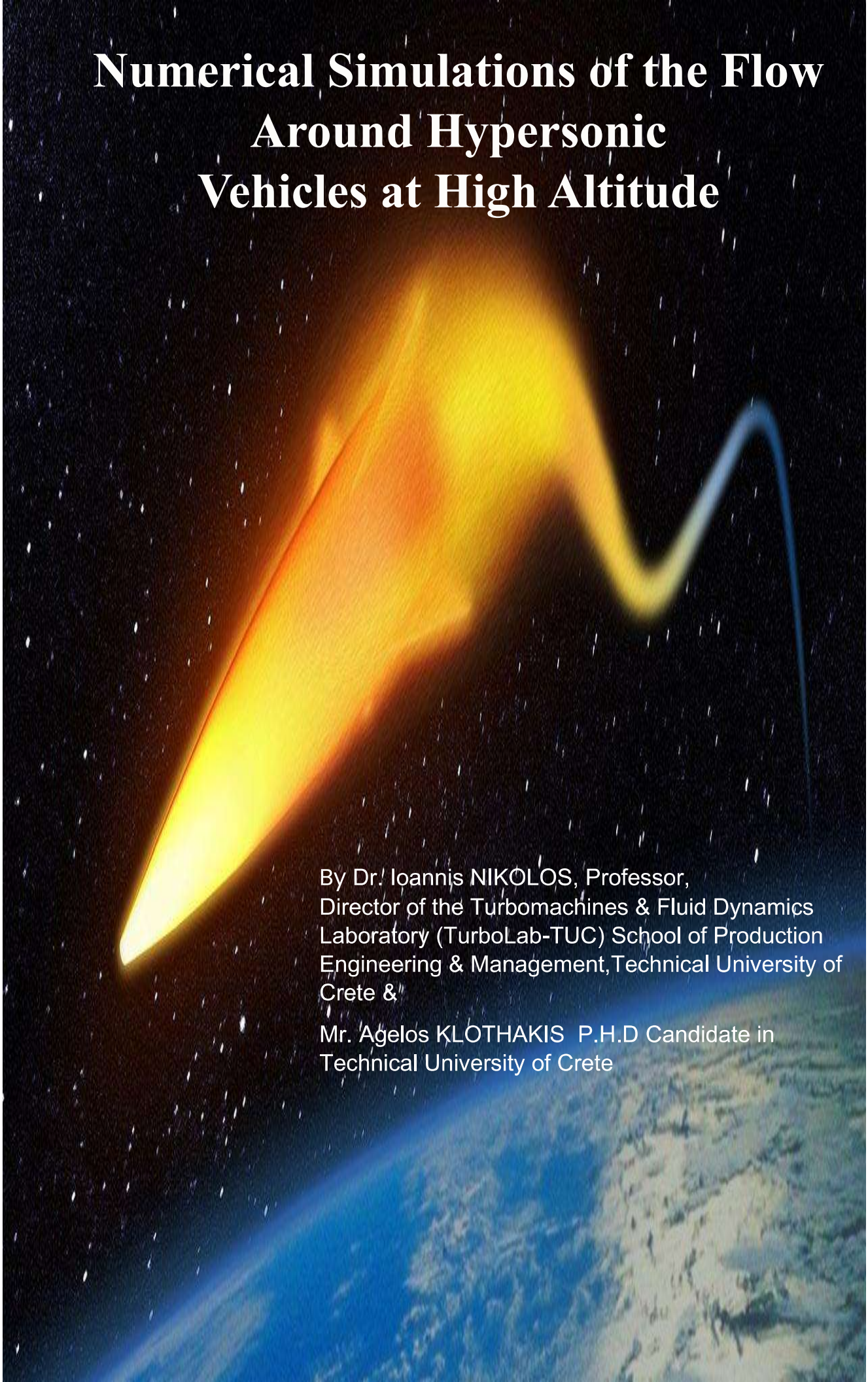
Summary

The horrendous and illegal invasions of Ukraine have further highlighted the new and emerging security challenges we face across the NATO Alliance, our Partner Nations, and the European Union. Integrated Air & Missile Defense is a key component of our security. But Air and Missile Defense is essentially a form of critical infrastructure, operated by the same technology and with the same vulnerabilities online - in cyberspace - as a power station, an Air Traffic Control facility, or a logistics network. Computer security is - and will remain - critical to securing these networks. But computer security is not enough. What's needed is a holistic approach to cybersecurity where the entire security of cyberspace - for our systems *and* our people - is placed at the heart of our defence. And that's the only way to defend ourselves from the bad guys - whether it's protecting us from disinformation and hate speech, online abuse, protecting people from internet banking scams and online fraud, or protecting our critical Integrated Air and Missile Defense Systems. ■

[10] *Frank Byrne, "Trust Me, Trust Me, I'm A Pilot. The Journey Towards a Just Culture in the Irish Air Corps," Irish Defence Forces – Defence Forces Review (2017).*

[11] *See: Emma Ryttare, "Change Management: A Key in Achieving Successful Cyber Security. A Multiple Case Study of Organizations in Sweden" (Masters diss., Luleå University of Technology, 2019), https://ltu.diva-portal.org/smash/get/diva2: 1327887/fulltext01.pdf -EU ENISA, Cyber Security Culture in Organisations (Athens: European Union Agency for Cybersecurity, 2017), www.enisa.europa.eu/publications/cyber-security-culture-in-organisations*

Numerical Simulations of the Flow Around Hypersonic Vehicles at High Altitude



By Dr. Ioannis NIKOLOS, Professor,
Director of the Turbomachines & Fluid Dynamics Laboratory (TurboLab-TUC) School of Production Engineering & Management,Technical University of Crete &

Mr. Agelos KLOTHAKIS P.H.D Candidate in Technical University of Crete

1. Introduction

The design and flight of hypersonic vehicles is a challenging and multi-dimensional effort due to complex aerodynamics, steep flow gradients, and non-equilibrium phenomena. Because of the high flight altitude such vehicles are exposed to high velocity rarefied gas flows [1-3]. Such flows are significantly different compared to those at the continuum regime. Thus, the Navier-Stokes equations fail to simulate such phenomena without further adaptions and modifications.

Despite the development of special velocity slip and temperature jump boundary conditions, which allow the Navier-Stokes solvers to extend their area of application, the latter seems to be inadequate to analyze flows with Knudsen numbers greater than 0.1. This observation, along with the enormous computational cost required to solve the Boltzmann equation, created the need for the development of the DSMC (Direct Simulation Monte Carlo) method, introduced by Bird during the late 60's [4]. As with all computational methods, a trade-off arises between the desired accuracy and the available computational resources; the DSMC method requires excessive computational resources in cases involving high-pressure and large computational domains. However, it is a valuable tool for simulating flows at high altitudes and high Mach numbers.

In this work the open source DSMC code SPARTA [5], developed in Sandia National Laboratories, will be used for the simulation of two hypersonic test cases. The first test case is a Mach 15 flow over a 2d axisymmetric 25/55 double cone, whereas the second case is a 3d Mach 10 flow over a cone with a swept fin. Both cases involve complex shock interactions resulting from the hypersonic flow around these configurations, which resemble to typical configurations of hypersonic vehicles. Therefore, the outcome of such simulations can be used to draw useful conclusions, regarding the corresponding physical phenomena induced from the flight of such vehicles.

2. The numerical method

DSMC is a particle method based on the kinetic theory for the simulation of rarefied gases. The method models the gas by using many simulator particles, each representing a large number of real particles [4]. In the DSMC method the time step (Δt) is chosen to be small enough so that the movement and collisions of the particles can be decoupled. During a DSMC simulation the flow field is discretized into computational cells, which provide geometric boundaries and volumes required to sample macroscopic properties. The algorithm has four main steps.

1. Movement of particles;
2. Indexing particles into cells;
3. Performing intermolecular collisions;
4. Sampling particles properties.

In order to locate the particles and track their movements, the whole computational domain is divided into a number of cells, which contain sub-cells in a predefined structure. Initially, a set of particles is randomly distributed in each cell. Each of the particles is assigned a position, velocity components and energy. Subsequently, the aforementioned steps are repeated in each time step in order to simulate the flow evolution in time. The macroscopic quantities of the flow (such as velocity, pressure, density, temperature and so on), are computed on each cell, obtained from simple weighting averages of microscopic properties.

3. Results

As mentioned before, two hypersonic test cases will be studied in this work. The first is a 25/55-degree axisymmetric biconic and the second is a 7-degree cone with a swept fin. The first geometry has been developed by the NATO Research Technology Organization in collaboration with the Working Group 10 [6-7]. The geometry is shown in Figure 1.

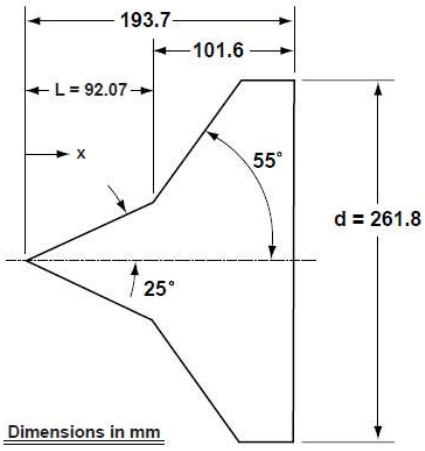


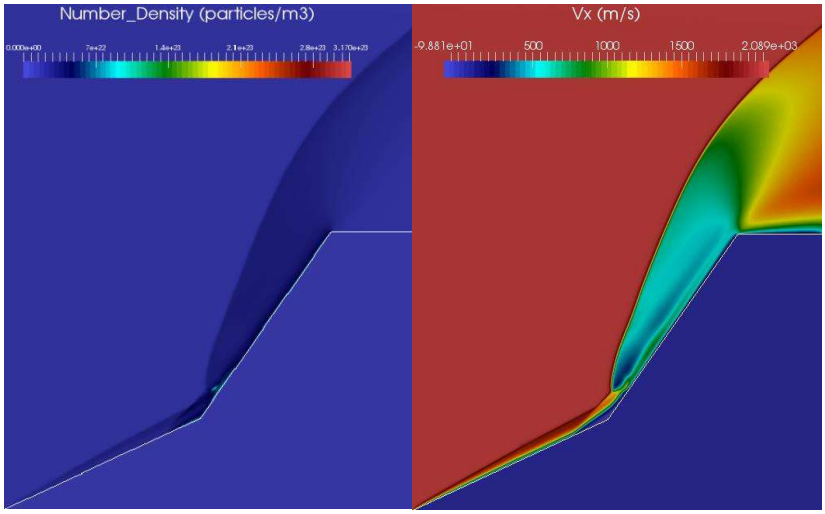
Figure 1. Double cone geometry [8].

This specific geometry produces very strong shock interactions, due to the attached leading-edge shock coming from the first cone, which interacts with the detached shock from the second cone. Furthermore, the outer shocks are influenced by the separation and reattachment shocks. The flow conditions are summarized in Table 1.

Flow Velocity (m/s)	Flow temperature (K)	Number Density, part/m^3	Surface Temperature (K)	Time step (s)	Fnum
2072.6	95.6	3.78×10^{21}	297.2	4.0×10^{-8}	3.0×10^{18}

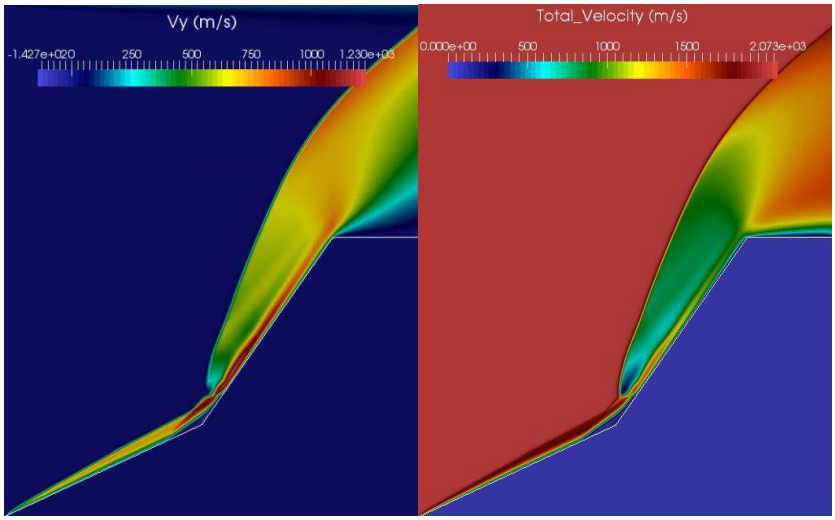
Table 1. Biconic case flow conditions.

In Figure 2a we can see the shocks interaction area, where the density rises up to 40 times the freestream density. Figures 2b and 3a contain the velocity along x and y axis respectively. From Figure 2b a small counter-rotating vortex can be evidenced in the junction area of the two cones. Furthermore, the leading-edge shock interacts and intersects the bow shock, generated from the second cone. Due to this interaction a transmitted shock is generated and reflects off the surface of the biconic. Figures 4 and 5 contain comparisons between the experimental and the computed heat flux and pressure on the surface of the biconic. As it can be demonstrated, very good agreement is obtained throughout the surface of the examined geometry.



(a) (b)

Figure 2. a) Number Density field; b) Axial velocity component.



(a) (b)

Figure 3. a) Radial velocity component; b) Total velocity.

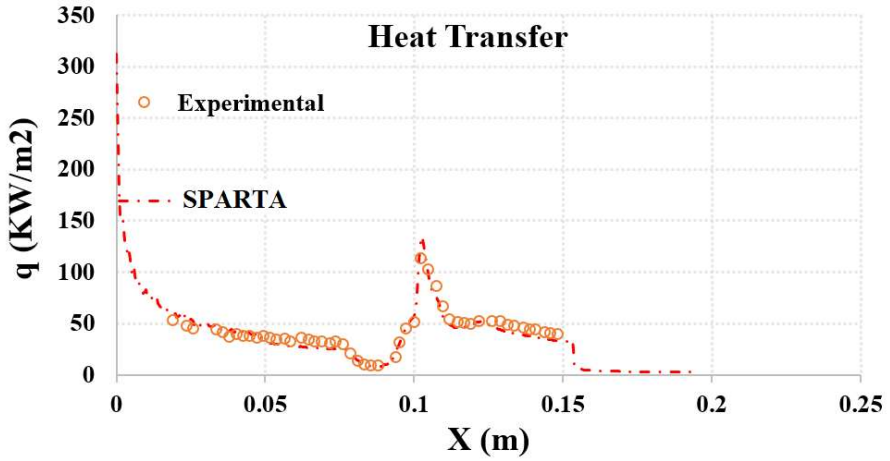


Figure 4. Heat transfer on the surface of the biconic case (comparison between experimental data and DSMC simulation results).

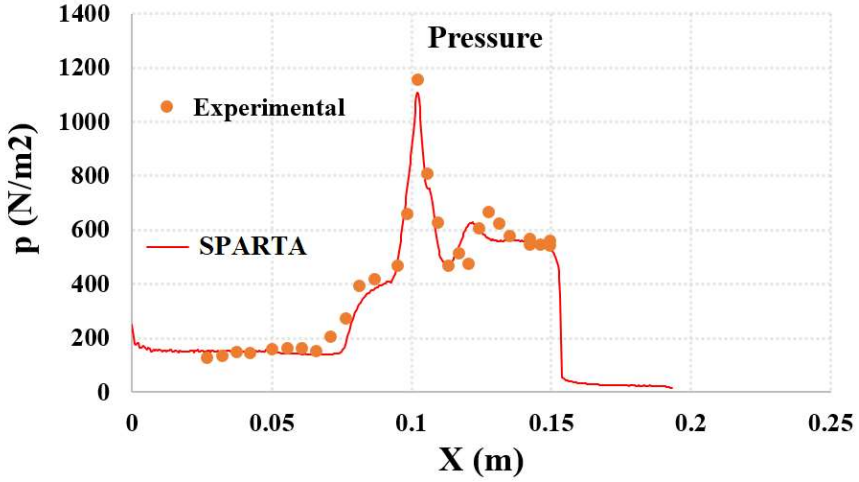


Figure 5. Pressure on the surface of the biconic case (comparison between experimental data and DSMC simulation results).

The second test case was based on a geometry with 7-degree cone with a swept fin. This geometry was developed in the PURDUE University, and has been extensively used to examine boundary layer transition on the surface of the cone and the fin [9-11]. An overview of the corresponding geometry can be seen in Figure 6. The cone is 40 cm long and the highest point of the fin is 4.45 cm high. The presence of the fin generates a complex shock system, resulting in large pressure gradients. In this work this geometry is simulated in flow conditions existing at ~65 km altitude and at a cruise speed of Mach 11. The flow conditions can be seen in Table 2. In order to ensure an accurate representation of the flow field, a refined grid was employed around the surface. The configuration of the grid is depicted in Figure 7.

Flow Velocity (m/s)	Flow temperature (K)	Number Density, part/m^3	Surface Temperature (K)	Time step (s)	Fnum
3721.08	231	3.75×10^{21}	300	2.0×10^{-8}	8.0×10^{11}

Table 2. Fin cone case flow conditions.

In Figure 8 the velocity gradient of the flow field is presented. As demonstrated in Figure 8, apart from the leading-edge shock, another shock exists due to the presence of the fin. The second shock starts from the junction point between the fin and the cone surface and then merges with the leading-edge shock downstream, creating a complex and interacting system of shocks. Figure 9 shows the computed temperature of the flow around the vehicle. As demonstrated, the stagnation temperature is as high as 1200 K and occurs at the tip of the leading-edge. In Figure 10 the heat flux on the surface is depicted. The maximum amount of heat flux is 50 kW/m^2 and is observed around the leading-edge area. Furthermore, on the top surface of the fin there is a significant amount of heat flux exerted on the top part. The heat flux absorption in that area is expected to be significantly high, due to the fact that the shock generated from the fin stands very close to the fin's surface, thus resulting in high amount of heat energy exchange between the shock, the boundary layer and the surface. This effect leads to high amounts of heat flux directed towards the surface of the vehicle.

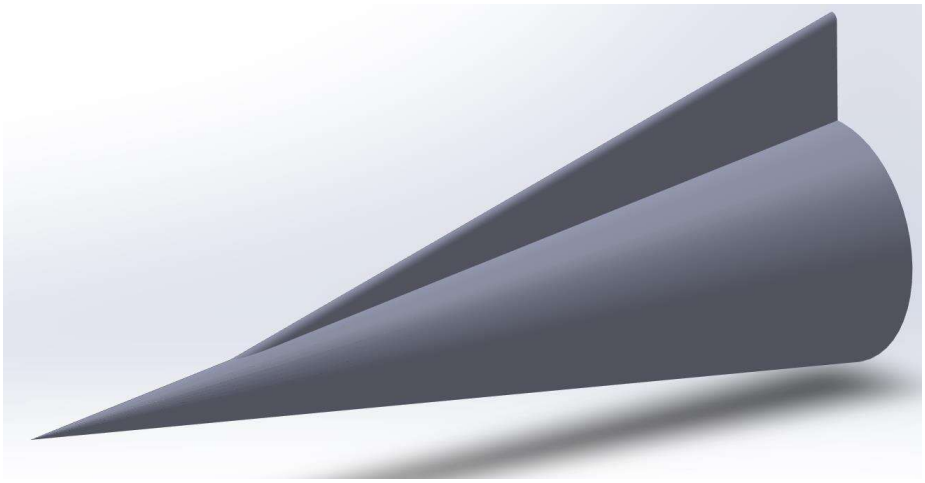


Figure 6. Overview of the fin cone geometry (test case 2).

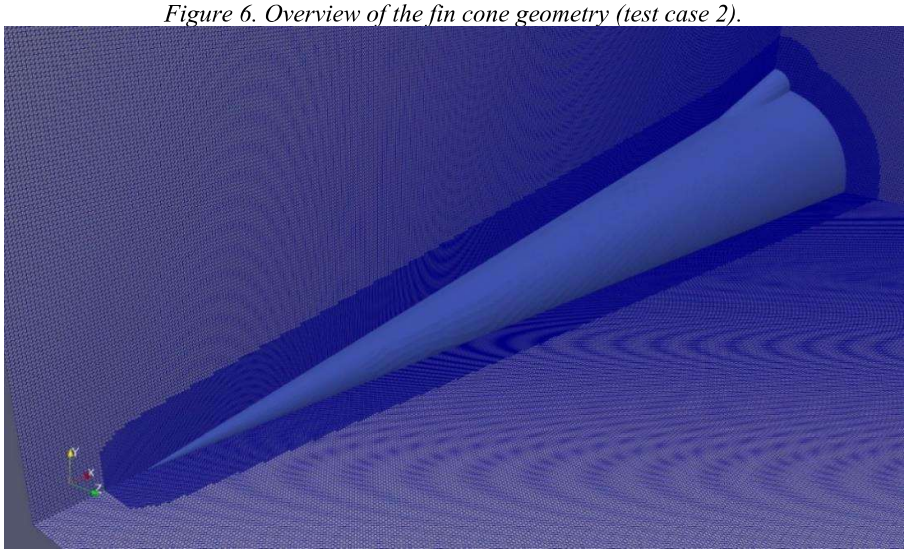


Figure 7. The computational grid used for test case 2.

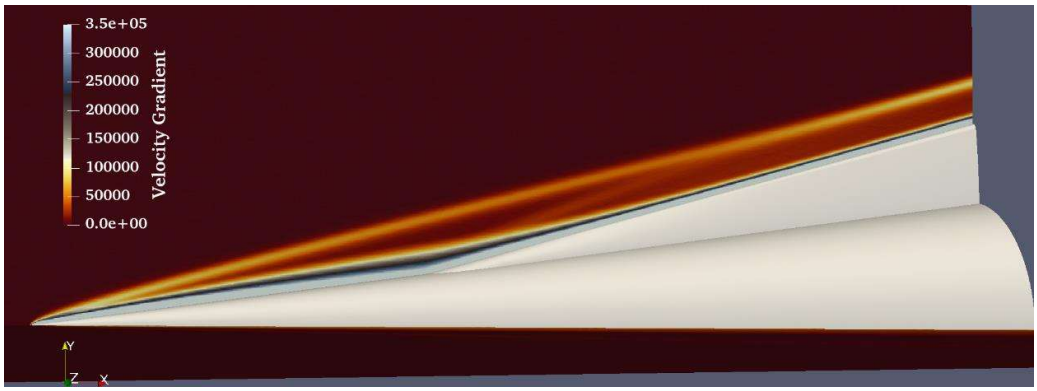


Figure 8. Velocity gradient.

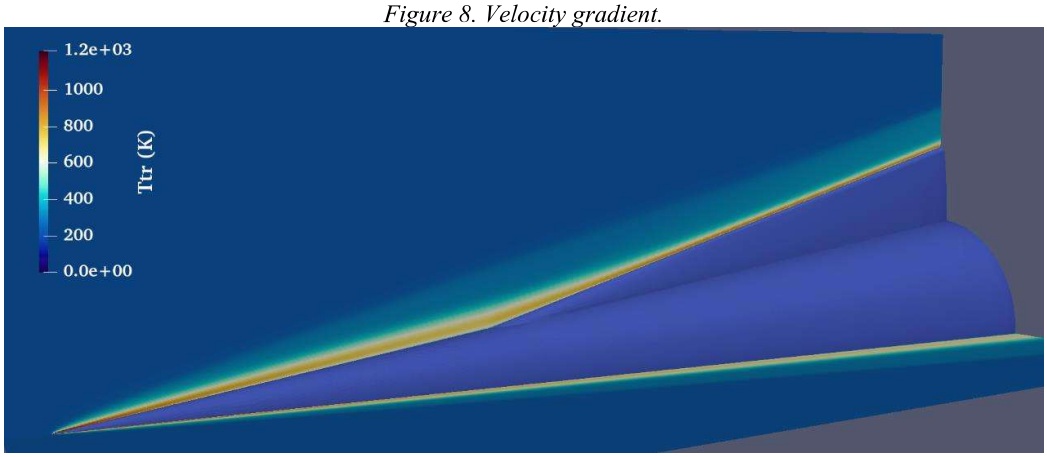


Figure 9. Translational temperature.

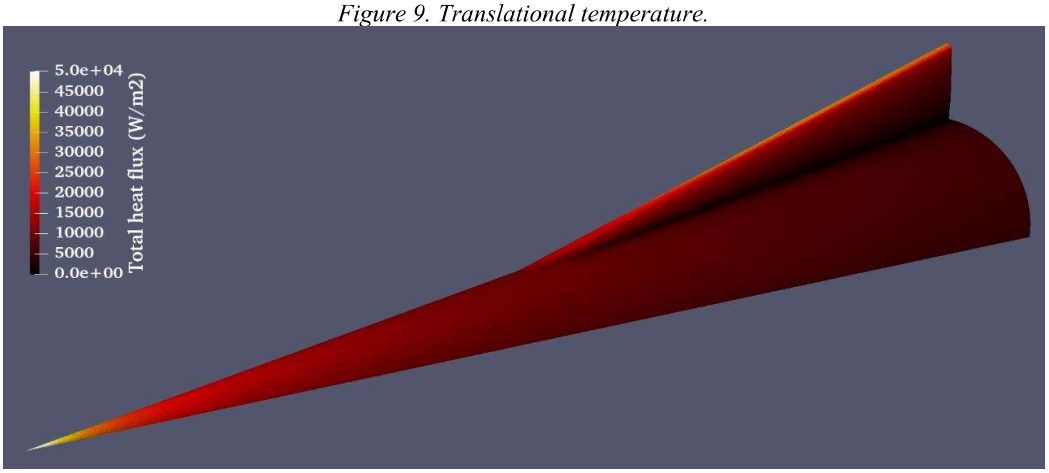


Figure 10. Heat flux on the surface of the cone.

4. Conclusions

Two test cases of hypersonic flows around complex geometries were studies in this work. The first geometry was a 2D axisymmetric biconic, with very strong shock-shock interactions and steep flow gradients. The flow conditions were set to be identical to the experimental values. As shown, the SPARTA DSMC solver managed to capture very accurately the surface properties, as well as the complicated flow effects. The second test case investigated a flow around a 7-degree cone with a swept fin. The flow properties and vehicle velocity were set to match the conditions that occur at ~65 km altitude. This complex geometry generated interacting shocks that, due to the high velocity, rest very close to the surface. This generates enormous amounts of heat flux to arrive on the surface. In future work the same flow will be examined with the inclusion of chemical reactions between the nitrogen and oxygen molecules, so as to study how these reactions influence the shock interactions and flow properties.

As it was demonstrated, the SPARTA DSMC solver is capable to provide very accurate simulation results of the complicated flow fields around hypersonic vehicles, including the heat transfer characteristics

and surface temperature fields. The latter are of paramount importance for the investigation of possible methods for the identification and tracking of similar types of hypersonic vehicles. ■

5. References

[1] Zhang, W.M., Meng, G. and Wei, X. (2012), "A review on slip models for gas microflows," Microfluidics and Nanofluidics, Vol. 13, pp. 845-882.

[2] Ho, C.M. and Tai, Y.C. (1998), "Micro-electro-mechanical-systems (MEMS) and fluid flows," Annual Review of Fluid Mechanics, Vol. 30, pp. 579-612.

[3] Gad-el-Hak, M. (1999), "The fluid mechanics of microdevices," ASME Journal of Fluids Engineering, Vol. 121, pp. 5-33.

[4] Bird, G.A. (1994), Molecular gas dynamics and the direct simulation of gas flows, Clarendon Press, Oxford.

[5] Gallis, M.A. Torczynski, J.R., Plimpton, S.J., Rader, D.J., and Koehler, T. (2014), "Direct Simulation Monte Carlo: The quest for speed," in Proceedings of the 29th Rarefied Gas Dynamics (RGD) Symposium, Xi'an, China.

[6] Knight, D. (2002), "RTO WG 10 - Test cases for CFD validation of hypersonic flight," in 40th AIAA Aerospace Sciences Meeting & Exhibit, American Institute of Aeronautics and Astronautics, AIAA Paper 2002-0433.

[7] Walker, S. and Schmisseur, J.D. (2006), "CFD validation of shock-shock interaction flow fields," DTIC Document.

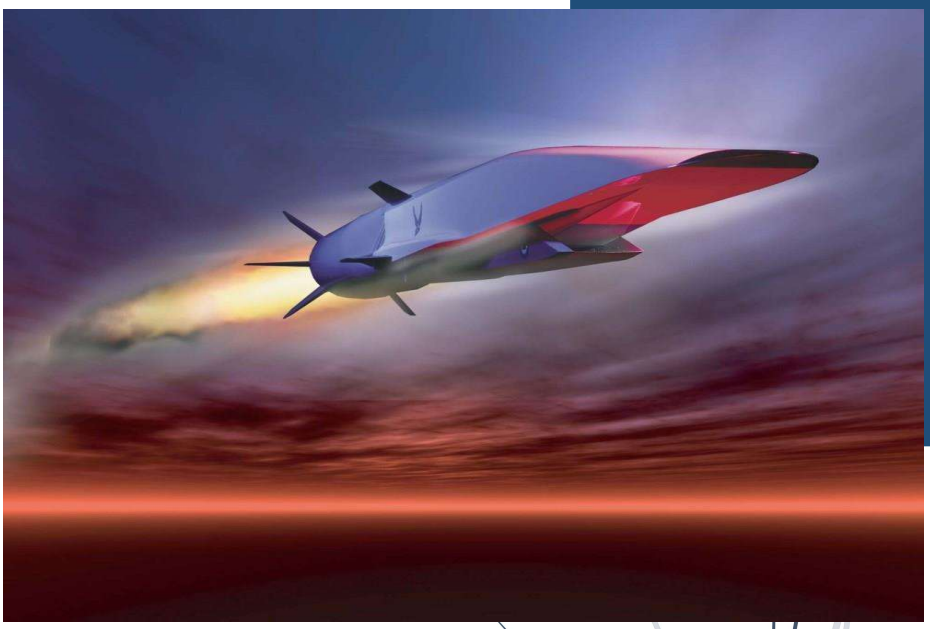
[8] Allègre, J., Raffin, M., Chpoun, A., Gottesdiener, L. (1992), "Rarefied Hypersonic Flow over a Flat Plate with Tuncated Leading Edge", Progress in Astronautics and Aeronautics, pp. 285-295.

[9] Turbeville, F. D., and Schneider, S. P. (2018), "Boundary-layer instability on a slender cone with highly swept fins," in 2018 AIAA Fluid Dynamics Conference, AIAA Paper 2018-3070.

[10] Turbeville, F. D., and Schneider, S. P. (2019), "Transition on a cone with a highly-swept fin at Mach 6," in AIAA Aviation 2019 Forum, AIAA Paper 2019-3217.

[11] Mullen, C. D., Turbeville, F. D., Reed, H. L., and Schneider, S. P. (2019), "Computational and experimental boundary-layer stability analysis on a hypersonic finned cone," in AIAA SciTech 2019 Forum, AIAA Paper 2019-1381.

Hypersonic



By Mr. Sozon A. LEVENTOPOULOS
CISSP, CASP+, CEH, ISO 27001 LA, NET+, SEC+

Introduction

Since almost the beginning of human history, mankind always tried to go faster, even when that was not a requirement or cost effective. Only, a couple of years after Flyer. I made that historical hop into the air, engineers and researchers were trying to push the speed limit forward. Both Word War were a catalyst for a number of technologies, including the jet engine. The latter is a reaction-type internal combustion engine, and was developed in both UK and Germany during the 1930s and 1940s. Jet engines thought had a number of limitations and research for ramjets soon followed. A ramjet is a form of airbreathing jet engine that uses the forward motion of the engine to produce thrust. Since it produces no thrust when stationary (no ram air) ramjet-powered vehicles require an assisted take-off like a rocket assist to accelerate it to a speed where it begins to produce thrust. Ramjets work most efficiently at supersonic speeds around Mach 3 (2,300 mph; 3,700 km/h) and can operate up to speeds of Mach 6 (4,600 mph; 7,400 km/h). The first prototype to successfully use a ramjet was the Leduc 0.10 of 1949. In late 1930s, Eugen Sager and Irene Bredt proposed a liquid-propellant rocket-power sub-orbital bomber, known as Silber Vogel (Silver Bird). The design was way ahead of its time, and incorporated new rocket technology and the principle of a lifting body (paving the way for X-20 Dyna-Soar of 1960s and the design of the Space Shuttle of the 1970s) Flying at speeds between the speed of sound had other challenges. During WW2 the then high-performance aircraft had experienced (usually in dives) strange phenomena when approach certain speeds. For some, it was their last flight, since the forces applied to their structure were overwhelming. Similar challenges were identified when the first airplanes reach supersonic speeds. For example, the SR-71 had to be specifically designed in order to withstand extensive heat and air pressure for prolonged flight times. These challenges were intensified when approaching the hypersonic layer. NASA's X-15 was one of the first examples to explore hypersonic flights. The results proved the theoretical and mathematical assumptions regarding the dangers and problems that needed to be addressed. While research efforts continued for a couple of decades, it soon became clear that the technology was not mature enough for a successful example. Everything changed on March 10, 2018 when Russia demonstrated the first operational hypersonic cruise missile.

Background

In aerodynamics, a hypersonic speed is the one that exceeds Mach 5 and up at about Mach 10. It should be stated that the precise Mach number can vary, since factors like atmospheric density, conversion of kinetic energy to heat, etc., can heavily affect those boundaries. Hypersonic flight, on the other hand refers to a flight occurring below 90km and at speeds greater than Mach 5. In this environment dissociation of air starts becoming significant, resulting in high heat loads. A number of physical phenomena are observed in these flights:

PHENOMENON	DESCRIPTION
Thin shock layer	The shrinking distance between the vehicle surface and shockwave at hypersonic speeds can induce additional stress.
Entropy layer	The layer of high entropy vorticity near the vehicle's leading edges can cause unusual aerodynamic effects, leading to dynamic instability.
Viscous interaction	The boundary layer—airflow around the vehicle body—thickens, interacts with the shockwave, and can increase heat and turbulence
Shock-shock interaction	The interaction between shockwaves of various vehicle features can complicate aerodynamic predictions.
Boundary layer	This thin layer of air directly interacts with the surface of a hypersonic vehicle.
Boundary layer transition	Hypersonic vehicles are engineered to maximize laminar boundary layer flows, where air travels in an ordered path over the vehicle surface. Changes in vehicle speed, surrounding air temperature, and others can cause laminar boundary layer flows to become turbulent, where air follows a chaotic path over the vehicle. This phenomenon is known as boundary layer transition. Turbulent boundary layer flows can impose significantly higher heat and vibration loads on the vehicle's surface.
High-temperature effects	Dissociation of air molecules, plasma formation, internal changes to thermodynamic properties of air molecules, and off-gassing from heat shield materials complicates design of thermal protection systems and can induce electromagnetic interference and other challenges.
Low-density flow	At high altitudes approaching 100 km, the physical characteristics of the atmosphere change considerably, resembling a series of discrete particles instead of continuous airflow. At the edge of space, air molecules striking a vehicle may never interact with other air molecules striking its surface.

To put things into perspective, the fastest bullet can travel at around Mach 2 (~1800 mph). A hypersonic weapon is design to travel from 2,5 to almost 12 times the speed of the fastest bullet. It should be noted also, that a set of physical phenomena and not a specific speed is what defines the hypersonic flight (therefore there is no meaning to refer to speed when a vehicle is in the vacuum of space). By definition a hypersonic flight is an atmospheric flight. As a result, hypersonic weapons need to address aerodynamic and thermal conditions that can stretch materials, and the navigation and control systems to their limits and beyond. A high-hypersonic weapon will need to sustain for considerable amount of time, extreme pressure and temperatures that reaches thousands of degrees Celsius. At these temperatures even the structure of the materials is changed. New and exotic materials, internal airframe structural design and avionics, need to be used in order for the hypersonic weapon to be able to survive is such a harsh environment.

Taxonomy of Hypersonic Weapons

There are two primary categories of hypersonic weapons:

· Hypersonic glide vehicles (HGV), which are launched on top of a rocket (usually, an obsolete or old ballistic missile), before gliding to their target. These types would follow boost-glide trajectories, in order to extend their range (usually the range will be doubled)

· Hypersonic cruise missiles (HCM), which are powered by air-breathing engines (usually scramjets)

Regime	Velocity			
	Mach No	mph	Km/h	m/s
Subsonic	< 0.8	< 614	< 988	< 274
Transonic	0.8-1.2	614-921	988-1482	274-412
Supersonic	1.2-5	921-3836	1482-6164	412-1715
Hypersonic	5-10	3836-7673	6174-12350	1715-3430
High Hypersonic	10-25	7673-19810	12350-30870	3430-8570
Re-entry	>25	>19030	>30870	>8575

Figure 1 - Speed Regimes

While HCMs and HGVs can be equipped with both conventional and nuclear warheads, in case of unhardened or soft targets their momentum should be enough (for example, the Kh-47M2 Kinzhal has a kinetic energy of 16,9 gigajoules, which equals 4 tons of TNT!).

Challenges for the Air Defense

The introduction of hypersonic weapons has created a number of unique challenges for the air defenses. While the HGVs are launched on top of a ballistic missile, its initial trajectory is much steeper and at a lower altitude. Their speed, maneuverability, and low altitude of flight challenges detection and defense (see Figure.3). Furthermore, HCMs can be launched from aircrafts and ships, thus making their initial detection even more challenging. That delayed detection can compress available decision time, which can result to a single intercept attempt. Finally, additional measures (like ASAT missiles) can deny the early warning capabilities..

Additionally, it would be extremely difficult to identify the actual target of the hypersonic weapon. This could further challenge defenses, since their alert time would be minimum (considered that it would take only 8 minutes for the Kinzhal missile to travel its full range of 2000 (MiG-31K). It is also interesting, that at these speeds a plasma cloud will form (at least around missile cone) due to the intense air pressure and heat. Plasma cloud is known to absorb and interfere with electromagnetic radiation (e.g., loss of communication between ground control and command module during the re-entry phase of the Apollo mission flights), and can significantly reduce target's RCS (Plasma STEALTH). Today, a growing number of countries are investing in hypersonic weapons. Russia and China seem to lead the race, since they have already demonstrated operational capability of various weapons, launched from a number of platforms[1].

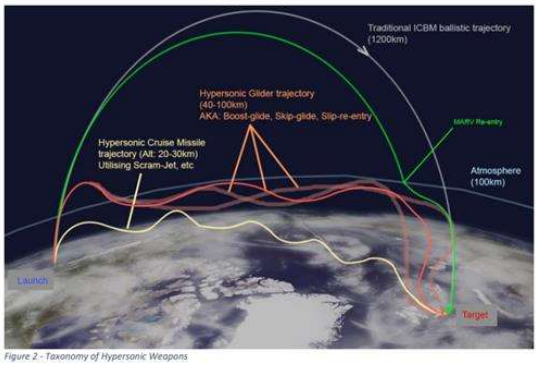


Figure 2 - Taxonomy of Hypersonic Weapons

[1] *Various sources claim that hypersonic weapons have been used by the Russian forces during the invasion in Ukraine. The validity of the sources, and the type of the weapon used can not be verified.*

Country	Variant	Remarks
USA	AGM-183 ARRW	Under development for use by the U.S. Air Force. Estimated range 1600+ km.
	LRHW	Under development. Joint program between the U.S. Army and U.S. Navy
	SCIFiRE	Under development. The Southern Cross Integrated Flight Research Experiment (SCIFiRE) is a joint program between the US Department of Defense and the Australian Department of Defence for a Mach 5 scramjet powered missile
RUSSIA	3M22 Zircon	A scramjet powered maneuvering anti-ship hypersonic cruise missile. It has a maximum speed of Mach 9 and an operational range of more than 1000 km. It is tailored for use by submarines and surface ships.
	Avangard	Also known as Objekt 4202, Yu-71 and Yu-74. It is a Russian HGV that can be carried as a MIRV payload by the UR-100UTTKh,[7][8] R-36M2 and RS-28 Sarmat heavy ICBMs. It can deliver both nuclear and conventional payloads. It has a maximum speed of Mach 20 – 27
	Kh-47M2 Kinzhal	The Kh-47M2 Kinzhal (in Russian: Х-47М2 Кинжал, "dagger", NATO reporting name Killjoy) is a Russian nuclear-capable hypersonic aero-ballistic air-tosurface missile. It has a claimed range of more than 2,000 km (1,200 mi), Mach 12 speed (2.5 mi/s), and an ability to perform evasive maneuvers at every stage of its flight
CHINA	DF-ZF	Is a Chinese HGV. It is mounted on a DF-17 which is a two-stage, solid-fuel rocket, single-warhead medium-range ballistic missile (MRBM) in the Dong Feng series. It is estimated that a smaller and lighter version has been development for use from Chinese Type 055 Destroyers

Defense Against Hypersonic Hypersonic weapons pose an elevated threat for missile defense efforts, introducing new challenges. Their main characteristics are:

- Speed,
- Trajectory
- Maneuverability,
- Low altitude, and
- Destructive force

By exploiting these characteristics, hypersonic weapons can be used as the "silver bullet" for surprise attacks against small targets (e.g., a carrier, or a remote base). In that view, they are extending the range and capabilities of the A2/AD concept. When combined with AD systems that will potential engage the interceptors, or with ASAT weapons that will deny the early warning capabilities, they create a very dangerous environment.

In order to address the challenge of hypersonic weapon we need a holistic approach. A new "system of systems" should be created in order to address detection, tracking, and interception efforts. Legacy systems (like the Aegis and THAAD) can and should be tailored as to address the new threat. But this would not be enough.

A **common Integrated Command and Control System** should be established that will extend to all domains (land, sea, air, space, and cyberspace).

New information technologies, like edge computing, big data analysis, AI/ML and cloud computing should be incorporated and exploited as to create and/or extend the needed decision space, thus providing the decision makers with credible options.

Multiple, redundant, and diverse systems should be

introduced in every part of the kill chain. It is safe to assume that the adversary will try to eliminate or diminish the effectiveness of our systems (ASAT missiles or directed energy weapons, electronic warfare/cyber-attacks, etc.).

New interceptor(s) should be developed tailored for the middle layer of the threat environment.

Deterrence efforts (dogma of "the best defense is a good offence"), meaning that research and development efforts should intensify.

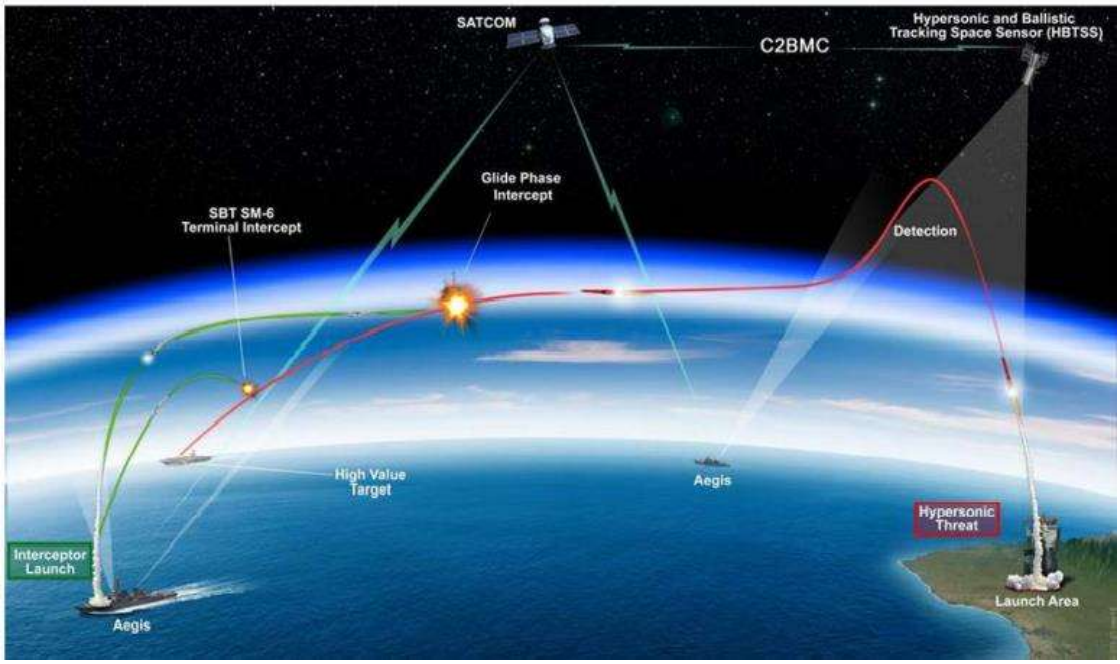
Out-of-the-box approaches also need to be considered. For example, incorporate methods and effectors that will force the weapon to bleed its energy, or tailor the early warning systems to detect and track the atmospheric disturbances (e.g., Schlieren photography) caused by the hypersonic weapons during their flight.

Key Take Aways

✓ Hypersonic weapons are now a clear threat and not a design approach or an experiment
✓ They can be used in surprise attacks, as "weapons of choice", to extend/hardened an A2/AD environment, or a combination of the above.
✓ While defending against such weapons would be challenging, it is not impossible. Novel strategies and approaches should be explored, and system's capabilities needs to be verified. The versatility and mobility of hypersonic weapons may prove overwhelming for space-based detectors.
✓ Out-of-the-box approaches also need to be considered ■

References

[1] Zhang, W.M., Meng, G. and Wei, X. (2012), "A review on slip models for gas microflows," Microfluidics and Nanofluidics, Vol. 13, pp. 845-882.
[2] Ho, C.M. and Tai, Y.C. (1998), "Micro-electro-mechanical-systems (MEMS) and fluid flows," Annual Review of Fluid Mechanics, Vol. 30, pp. 579-612.
[3] Gad-el-Hak, M. (1999), "The fluid mechanics of microdevices," ASME Journal of Fluids Engineering, Vol. 121, pp. 5-33.
[4] Bird, G.A. (1994), Molecular gas dynamics and the direct simulation of gas flows, Clarendon Press, Oxford.
[5] Gallis, M.A. Torczynski, J.R., Plimpton, S.J., Rader, D.J., and Koehler, T. (2014), "Direct Simulation Monte Carlo: The quest for speed," in Proceedings of the 29th Rarefied Gas Dynamics (RGD) Symposium, Xi'an, China.
[6] Knight, D. (2002), "RTO WG 10 - Test cases for CFD validation of hypersonic flight," in 40th AIAA Aerospace Sciences Meeting & Exhibit, American Institute of Aeronautics and Astronautics, AIAA Paper 2002-0433.
[7] Walker, S. and Schmisseur, J.D. (2006), "CFD validation of shock-shock interaction flow fields," DTIC Document.
[8] Allègre, J., Raffin, M., Chpoun, A., Gottesdiener, L. (1992), "Rarefied Hypersonic Flow over a Flat Plate with Tuncated Leading Edge", Progress in Astronautics and Aeronautics, pp. 285-295.
[9] Turbeville, F. D., and Schneider, S. P. (2018), "Boundary-layer instability on a slender cone with highly swept fins," in 2018 AIAA Fluid Dynamics Conference, AIAA Paper 2018-3070.
[10] Turbeville, F. D., and Schneider, S. P. (2019), "Transition on a cone with a highly-swept fin at Mach 6," in AIAA Aviation 2019 Forum, AIAA Paper 2019-3217.
[11] Mullen, C. D., Turbeville, F. D., Reed, H. L., and Schneider, S. P. (2019), "Computational and experimental boundary-layer stability analysis on a hypersonic finned cone," in AIAA SciTech 2019 Forum, AIAA Paper 2019-1381.



By LT. Col. Panormitis - Nikolaos Demertzis GRC (AF)
Hellenic National Defence General Staff

INTRODUCTION

During the last 73 years since NATO's formation in 1949[1], the Alliance has witnessed an ever-changing geopolitical and geostrategic environment, where multi-polarity alternates with bi-polarity and constantly new balances are created between old and new, state and non-state actors, struggling to consolidate their position on the international chessboard. At the same time, threats to the maintenance of peace and sovereignty of states worldwide, evolved in type and number in all domains, taking advantage of the new technological developments.

NATO has been responding to the challenge by developing collective military and political structures, while utilizing concepts such as common interest, collaboration, constructive dialogue, coherency, volunteering, etc, Among these concepts, there is one that is almost identical to the NATO itself. The concept of integration in NATO constitutes one of the core elements on which the Alliance was built upon, taking into account the next two common definitions of the term[2]:

· The action or process of combining two or more things in an effective way.

· The process of becoming part of a group of people.

It is imperative to have always in mind, that integration in NATO is not only about combined military forces, weapons and firepower but most importantly about people, coordinating and working together, towards the common goal of peace, security and ultimately survival.

Is NATO IAMD integration a reality?

The need for integration in NATO became apparent right from the start, especially in the domain of the Air Defence, resulting to the creation of the contemporary NATO IAMD[3]. The IAMD has been created by the cooperation and the contributions of the NATO members, as a countermeasure to the constantly evolving threats environment for peace and stability in the Alliance's member - states territories and in the broader NATO interest's region. The integration in NATO IAMD became a reality in the forms of Councils, Committees, Working Groups, Operational Plans, Crisis Management Mechanisms, Command & Control Structures, Joint Operations, Exercises, Facilities, Sensors, Weapon systems and various other projects and programs. Undisputable facts of IAMD's integration are the development of capabilities for planning, executing, monitoring and evaluating, the Alliance's air and missile defence operations.

These capabilities have been achieved not only by utilizing and integrating NATO's personnel, funds, means and assets, but mainly by the will of the member-states and their actual support in every aspect, to achieve the success of the IAMD venture.

Prime examples of the above mentioned capabilities are the NATO AirC2[4] and the NATO BMD[5], leading to execution of peacetime missions such as the NATO Air Policing over Albania, Republic of North Macedonia and Montenegro[6] which is executed jointly by the Greek and the Italian Air Force, under the Alliance's BMC3I[7] system's operational and tactical control. Correspondingly, for the permanent defence against missile threats to the Alliance territory, a wide net of integrated sensors and SBAD[8] systems has been established, commonly funded by the Allies in combination with voluntary contributions by some of them, such as the AEGIS ashore systems in Poland and Romania, the TPY RADAR in Türkiye[9], the Patriot and SAMP/T systems of several member states.

Although, the IAMD integration is also clearly depicted in the development of programs as the NATO ACCS[10], the NATO BMD ACCS, and in a wide variety of common evolving armaments programs directed by the CNAD[11], the common and realistic training and exercises for the evolved personnel and the various means, remains a key factor for the success of IAMD integration and its effectiveness. The successful execution of exercises as Optic Wind Mill, Steadfast Armour, Formidable Shield, Ramstein Legacy, IAMD TTX[12] and many more, enhances the IAMD integration by identifying any deficiencies and shortcomings in order to be eliminated, while at the same time promotes and strengthens the critical cooperation, coordination and understanding between people of different military, academic and national background, as well as and the combined utilization of a highly diverse variety of systems.

Is NATO IAMD integration adequate and complete?

Taking in mind all the above, we could say as a response to the question, whether the NATO IAMD integration is a reality, that it is.

[1] *12 countries signed originally the North Atlantic Treaty in Washington D.C. at the Departmental Auditorium on the 4th of April 1949. Today the NATO member – states are 30, soon to be risen to 32.*
[2] *https://dictionary.cambridge.org*
[3] *Integrated Air and Missile Defence*
[4] *Air Command and Control*
[5] *Ballistic Missile Defence*
[6] *Since they lack the appropriate means to perform air policing on their own*
[7] *Battle Management, Command, Control, Communications and Intelligence*
[8] *Surface Based Air Defence*
[9] *As parts of the US European Phased Adaptive Approach for regional missile defense*
[10] *Air Command and Control System*
[11] *Conference of National Armaments Directors*
[12] *Table Top Exercise*

But if we pose the question to whether NATO IAMD integration is adequate and complete, the response could be quite different, since several factors in national and alliance level, affect constantly the IAMD integration's course such as:

· Geopolitical environment
· Threats
· Policies
· Economy/Budgets
· Technology
· Available means
· Contributions

So, in order to form an answer to the last question, it is essential to take a closer look at each one of the above factors.

The effect of geopolitical environment on IAMD integration

Starting with the geopolitical environment, NATO had initially developed the IAMD while a bi-polar geopolitical competition was in motion, focused on a single main peer adversary. After undergoing a series of transformations and a relative peaceful short era, the competition has now evolved to a multi – polar one, with Russia and China becoming prominent players, while many other states are constantly upgrading their geopolitical status using political, economic and mostly military means. The international geopolitical and strategic balance that was based on the principal of threat of force has been irreparably disturbed and aggressive military operations are already executed even between sovereign states, aiming in changes of the status quo. The threat for the Alliance is becoming a reality, especially for the smaller member – states that lack the capability to defend them self's, the states of the outer regions of the Alliance and even for the states that wish to join the Alliance and become part of NATO's expansion. Therefore, NATO IAMD has to evolve and adapt its integration, in order to be able to face successfully the upcoming challenge of defending the Alliance against a growing number of potential adversaries, which possess an even faster growing arsenal of missiles and airborne threats with the intention to use them, anywhere and everywhere, regardless the geopolitical cost.

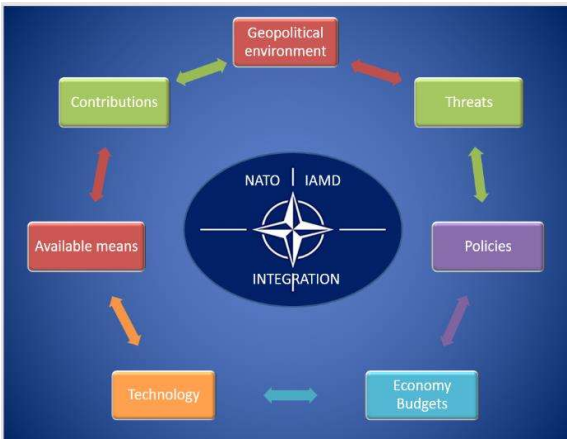
IAMD threats versus integration

These missile and airborne threats constitute the core of another factor that also affect's NATO's IAMD integration, the factor of threats. As the IAMD threats constantly evolve in number, type, destructiveness and efficiency, the Alliance's counter measures risk to gradually become insufficient and obsolete. Recent examples of air and missile defence operations worldwide have demonstrated that the threats are based on the combined and often simultaneous use of numerous weapon systems as aircrafts, UAVs, missiles, loitering munitions and many others, with the objective to suppress the enemy air and missile defence and hit not only high value and strategic targets, but also the backbone of the opponents fighting capability.

We must always have in mind that the IAMD threats are even more enhanced with hybrid warfare through combined operations in other domains as cyber and definitely never forget that the epitome of the IAMD threats, the nuclear, still exists and is getting bigger, since more states have acquired the capability to launch nukes and in greater distances. As a result, the NATO IAMD's evolving threats create a necessity for its integration to be constantly if not more at least equal evolved, not only in means and weapon systems, but also in capabilities and most important in tactics and courses of action.

Alliance's policies on IAMD integration

But since courses of actions derive from policies, the next factor to be examined in accordance with IAMD integration is exactly them. This specific factor is based mainly in two derivatives, the NATO policies and the national policies of the member states, that must be mutual supportive although that's not always the case. NATO IAMD policies form the Alliance's answers to questions as to who, where, when and how regarding IAMD capabilities and operations, allies, adversaries and threats and the appropriate treatments. National IAMD policies depict the attitude of the members - states towards the Alliance, the other member – states and also towards other non NATO states and non – state actors according their national interests. All the above mentioned policies are reconfigured constantly since national interests are reconfigured also constantly and furthermore, since the posture of third states towards the Alliance fluctuates from friend to foe and from moderate to extreme. The reconfiguration of both the policies of the Alliance and the member – states, affect the NATO IAMD integration in a positive way only when they



converge, otherwise they bring about the opposite results.

Economy and Alliance's budgets a crucial IAMD integration factor

It is common knowledge that the formation of policies rely in a significant degree on funding, which leads us to the next IAMD integration factor the economy and the budgets. The NATO IAMD personnel, capabilities and means are funded by the NATO budget and by the members – states budgets. Therefore an increase or a decrease of them affects directly the NATO IAMD in total and furthermore its integration.

Although NATO budget is relatively stable and continuous, the decisions of its use in IAMD are affected by the Alliance's economic environment and status at every given moment, affecting in turn the relevant operations and programs. In an even greater degree the economic environment and the economic status of every member – state affects its IAMD decisions, armaments, voluntary contributions and participations in operations. In the recent past years the global economic depression left its mark in NATO IAMD by decreasing and postponing developments of IAMD capabilities and means of the Alliance and especially those of the members – states, affecting accordingly the IAMD integration. At the moment the recovery of the global economic environment, is slow and full of obstacles as the pandemic Covid -19, and the economic predictions are not optimistic. Never the less, some member – states have commenced large scale IAMD armaments and capabilities upgrade programs, as an urgent necessity, due to the Russian invasion in Ukraine and the relative global implications. As it seems there may be an opportunity for the NATO IAMD integration to be further enhanced, before the fragile global economic environment slows it down again.

IAMD technology a wish or a curse?

The direct or indirect funding of the NATO IAMD integration enhancement is used partially in the acquirement of advanced military technology, which represents another IAMD integration factor. The rapid advance of military technology has given to the NATO IAMD integration the opportunity and the means to be further enhanced and become more efficient, but at the same time it has widened the gap between Alliance's edge technology systems and legacy ones that still exists at the members – states arsenals, making their use in the NATO IAMD impossible. Furthermore the advanced military technology is also used for the enhancement of the threats against the IAMD. Therefore advanced technology is a wish and course for the IAMD integration since it provides solutions and problems simultaneously. Never the less the future of IAMD integration is undoubtedly based on the faster and larger exploitation of the most advanced military technology, with the condition that at least most of the member – states can keep up and the rest will follow up. Consequently technology plays a key part in the presence of available IAMD means which in turn form the next IAMD integration factor.

Member - states voluntary contributions to IAMD integration

Although NATO has funded and developed an IAMD net of sensors, BMC3I systems and various relevant capabilities, the NATO IAMD relies mainly to the member - states voluntary contributions, which as the previous mentioned availability of means, it's also self evident that affect directly the NATO IAMD integration. The US has the leading part in voluntary IAMD contributions amongst the allies, followed by many others according to their military strength and policies. Recently the Russian invasion in Ukraine made crystal clear that there is an urgent need for many more voluntary contributions to NATO IAMD in order to be able to meet the upcoming challenges, initializing a new stream of contributions and as a result an increased need for integration not only of these systems, but also of the NATO IAMD in total.

Final remarks - Suggestions

As has already been stated the implications of all the above factors have constantly reshaped the path of the IAMD and will continue to shape its future. Therefore in accordance with those factors the following suggestions could further improve the NATO IAMD integration:

· Simplification of IAMD related procedures.
· Increase of available IAMD means.
· Development of IAMD common logistics support.
· Development of IAMD strategic "express" transportations.
· Increase of common experiences in IAMD integration through larger scale integrated training.
· Decrease of IAMD systems diversity through increased common IAMD systems development.
· Development of a NATO-COMPLIANT standardization for new IAMD systems.
· Research, development and evaluation of IAMD integration best practices and approaches, utilizing the combination of the Alliance's IAMD CoE[13] and its neighboring NAMFI[14] in Crete.

[13] *Center of Excellence*
[14] *NATO Missile Firing Installation*

Conclusion

It is well known that throughout the global military history and especially after the WWII, the achievement of Integration was always considered the "Holy Grail" for the Air and Missile Defence domain as it still is and probable will continue to be in the future, relying on systems interoperability and on common understanding of procedures and doctrines, development of common concepts of operation and common use of tactics.

This pursue for integration is constantly affected by various factors, as was analyzed in the case of the NATO IAMD integration which was examined in this paper. Based on the above analysis and as a conclusion, the answers to the paper's core questions about integration are the following: Is IAMD integration a reality? Definitely. Is IAMD integration adequate and complete? Not yet. Will IAMD integration ever be adequate and complete? It can be achieved on a temporary basis but its pursuit is doomed to be continuous. ■

References

https://www.nato.int
NATO Integrated Air and Missile Defence
https://www.nato.int/cps/en/natohq/topics_8206.htm
(Accessed 29 August 2022)
NATO Air Policing: securing NATO airspace
https://www.nato.int/cps/en/natohq/topics_132685.htm
(Accessed 29 August 2022)
Ballistic Missile Defence
https://www.nato.int/cps/en/natohq/topics_49635.htm
(Accessed 29 August 2022)
Conference of National Armaments Directors (CNAD)
https://www.nato.int/cps/en/natolive/topics_49160.htm
(Accessed 29 August 2022)
NATO members countries
https://www.nato.int/cps/en/natohq/topics_52044.htm
(Accessed 29 August 2022)
https://www.ncia.nato.int
Air and Missile Defence Command and Control
https://www.ncia.nato.int/what-we-do/air-missile-defence.html (Accessed 29 August 2022)
https://ac.nato.int
Air policing over the western Balkans
https://ac.nato.int/missions/air-policing/western-balkans
(Accessed 29 August 2022)
Allied forces conduct successful integrated air and missile defence exercise
https://ac.nato.int/archive/2022/RALY22
(Accessed 29 August 2022)
https://www.natomultimedia.tv
NATO deploys Patriot missile defence system to Slovakia (B-ROLL)
https://www.natomultimedia.tv/app/asset/665113
(Accessed 29 August 2022)
https://www.oecd.org/economic-outlook/ (Accessed 29 August 2022)
https://www.defense.gov/News/Releases/Release/Article/3078056/fact-sheet-us-defense-contributions-to-europe/
(Accessed 29 August 2022)
https://iamd-coe.org/about-us/iamd/ (Accessed 29 August 2022)
https://www.japcc.org
https://www.japcc.org/articles/the-importance-of-integrated-air-and-missile-defence-training/ (Accessed 29 August 2022)
https://www.japcc.org/articles/25-years-of-integrated-air-and-missile-defence-training/ (Accessed 29 August 2022)
https://rusi.org/explore-our-research/publications/occasional-papers/future-nato-air-and-missile-defence (Accessed 29 August 2022)
https://www.belfercenter.org/publication/nato-seventy-alliance-crisis (Accessed 29 August 2022)
NATO at 70 peace in a changing security environment
https://www.jstor.org/stable/48668552#metadata_info_tab_contents
(Accessed 29 August 2022)
Return to realism? NATO and global competition
https://www.tandfonline.com/doi/full/10.1080/14702436.2022.2082958
(Accessed 29 August 2022)
https://www.mda.mil/system/aegis_bmd.html (Accessed 29 August 2022)
https://www.edrmagazine.eu/tag/nato-iamd (Accessed 29 August 2022)
https://ukdefencejournal.org.uk/finland-and-sweden-train-with-nato-air-defence-forces/ (Accessed 29 August 2022)
https://defbrief.com/2022/06/06/nato-tests-integrated-air-and-missile-defense-in-the-baltics/ (Accessed 29 August 2022)
https://missiledefenseadvocacy.org/alert/all-for-one-the-nato-missile-defense-team/ (Accessed 29 August 2022)
https://portal.ieu-monitoring.com/editorial/ramstein-legacy-fighters-and-sbamd-units-in-large-scale-exercise/379401?utm_source=ieu-portal (Accessed 29 August 2022)

C - RAM Systems Beyond the Conventional Ways of Employment – Utilizing the Highly Reactive Capability in a Multi-Dimensional Environment

C-RAM Choices

Introduction

The C-RAM, as a capability, refers to a system of systems, like sensors, interceptors, and warning systems, and not only a weapon. It is used to detect and/or destroy incoming rockets, artillery, and mortar rounds in the air before they hit their ground targets, or simply provide early warning. This capability was initially designed to offer protection to the deployed forces and infrastructure without the provision, to hit the point of origin. Nonetheless, this tends to be a desired capability either as an inherent system characteristic or, as a result of integration between deployed forces. Currently, C-RAM is considered one of the areas that comprise IAMD and thus becoming an area of interest for the Centre. The IAMD COE monitors the latest tendencies concerning this capability through its participation in relative working groups.

By Maj Merkourios KATSAMAKAS GRC (A)
IAMD CoE SME

History

Iraq Freedom Operations revealed the need for the development of a system, that would be able to protect both ground forces and forward operating bases from insurgents' firings.

While the development of this project, began in 2004 and was tested in 2005, the initial idea came from the US Navy in late 1960, as the terminal Naval defence against anti-ship missiles. The main difference between the two versions concerns the rounds. While both systems use 20mm rounds, the ones fired from the Naval Version at sea, are by far more effective at destroying inbound RAM, compared with the Land Version. The reason is that the Land Version rounds are equipped with a self-destructing technology, which is activated approximately after 2km, in order to avoid causing friendly losses.

As mentioned previously, during the Iraq Freedom Operations, the US forces and their coalition were facing serious damage due to insurgents' firings. The number of losses both from military personnel and civilians was increasing. There were some methods, of initial countering those firings prior to their launch, such as aggressive patrolling, establishing ambushes, and counter firings on suspected or confirmed enemy

Initial Countering Methods (Ambushes & Patrolling)

locations, but each of these methods posed risks to friendly soldiers and civilians. So, it was vital to develop a system with quick reaction ability, effectiveness, and precision.

Use

The system uses sensors, like radars and UAVs, and computing systems, to update itself with information about the location of friendly air platforms. This information is updated almost continuously. At the same time, the system detects incoming RAM and calculates the optimal time to engage the target and the needed duration of firing, with extended use of Artificial Intelligence (AI).

The outcome is a system that works as intended. It provides early warning to the deployed personnel and destroys incoming RAM at the same time. Although the system cannot prevent all casualties, having C-RAM is certainly more effective that the status quo prior to it.

Pillars

The C-RAM capability was made up, of a variety of systems that provide it with the ability to Command and Control, Sense, Warn, Intercept, Respond, Shape and Protect.
The abovementioned abilities are considered the C-RAM's Pillars. Only four of them, constitute "active defence".

Active Defence	Non-Active Defence
Command and Control	Warn
Sense	Shape
Respond	Protect
Intercept	

Command and Control – Sense

The C-RAM Command and Control is implemented in the Engagement Operation Centre, where the Integration of sensors, weapons, and warning systems takes place, and uses target acquisition sensors, to detect and track fired incoming rounds.

Warn

Once a threat is detected, a subsystem, predicts the incoming round path, prioritizes targets, and provides data to defeat the incoming cell while it's still in the air. Finally, the "**incoming**", broadcast gives valuable seconds to the deployed forces, to take cover.

Dissemination of information between deployed forces is considered vital. For example, friendly air platforms (aircrafts, helicopters, UAVs) need to know that an enemy projectile is incoming and the fact that the C-RAM is about to engage, so they will not fly into the trajectory of either.

Intercept

Currently, the highest available firing rate, according to open internet sources, is 4,500 rounds per minute, offering very high percentages of successful interceptions. Since the available time between detection and interception is just a few seconds, we need quick and valid decisions. There is no time to decide which available system or interceptor should be used, or which threat should be engaged first. So, Artificial Intelligence should be and is used in an extended way.

Insurgents' firings from Urban Areas

Challenges & Solutions

In case, an insurgent, for example, launches a mortar cell from close to the deployed forces distance, the C-RAM faces challenges that arise from the shell's high speed and small signature.

To overcome this difficulty, when the countermeasures against RAM must be carried out within a few seconds, the industry has developed laser-powered interceptors, that offer interception in just one hit.

But lasers pose a few technical challenges themselves as well, such as duration in use, the minimum time needed for repetition of a strike, swarm attack response, etc. Although the interception of a few drones, let's say 10, is feasible, a greater number, let's say 100, might be challenging.

Command & Control Sense Warn

C-RAM vs Counter Battery / Counter Artillery

This paragraph aims to note some differences between C-RAM and Counter Battery/Artillery in order to avoid any possible misunderstanding.

"Counter Battery/Artillery" systems, track a shell back to its point of origin, using data derived mostly from the flight trajectories of incoming shells, and issue real-time targeting for its own weapons. Those weapons' mission is to prevent the next attack: by launching fire on the enemy point of origin, attempting to destroy the enemy's weapons.

C-RAM, instead, is an active defence: it intercepts and destroys the rocket, artillery, or mortar shell, in the air, prior it hits the ground.

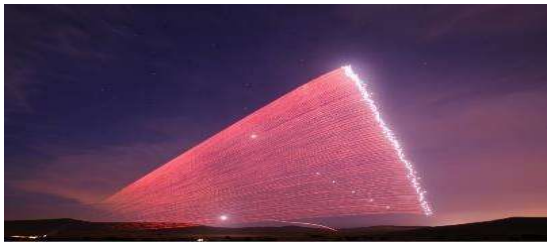
The C-RAM capability, as we mentioned previously, was not initially designed to attack the point of origin. But there is no system that can operate continuously, and it would be more effective, and/or cost-effective, to destroy the forces that launch those incoming RAM.

So, the integration between the C-RAM forces, Counter Battery/Counter Artillery, friendly air platforms and why not, and SOF, is considered desirable.

Another perspective could be, to give the C-RAM systems, in principle, the ability to locate and destroy the point of origin, themselves.

Even if the C-RAM capability, had those inherent or integrated C-B / C-A capabilities, there could be many cases where the destruction of the point of origin would be inappropriate. For example, the cases where those RAM are fired from urban areas were causing unacceptable civilian casualties, would be possible.

Apart from that, since rockets, can be launched from single-use launchers or fired by a timer, there would be no equipment or personnel to destroy. So, this exactly is the advantage of the C-RAM capability. It offers protection under all circumstances.



Dissemination of information interception

C-RAM Beyond its Conventional Use

Even though the C-RAM capability was initially developed to work as a standalone system with a very more than that. For example, it can be used to intercept Class I UAVs and Drones, or even to provide Short-Range Air Defence. The point is that C-RAM capability can undertake more than one mission, even secondary ones.

Another point of interest could be to give more flexibility to the C-RAM capability's architecture. It might be interesting, for example, to see the C-RAM Capability's components as independently deployable elements that can be swapped in and out of one main system, with no delay and no degradation of performance, offering tailored to our needs services with its sensors, or its interceptors

This architecture could be likened to the very well-known game, LEGO, the game that gives you the capability to make many-different constructions, using the same items.
This similitude's aim is to uphold the theory that C-RAM can and has to be used in more than one way.

So, could the C-RAM capability, be used against Helicopters, or UAVs? Maybe yes. And why not, the C-RAM could also be used to protect HVA or Air Defence Systems, which are vulnerable to RAM, and other threats that may occur in the future, contributing that way, to the development of a more effective AD umbrella.

Of course, there are many technical challenges, but cooperative work between Armed Forces, Academia and Industry might give the required solutions.

Summary

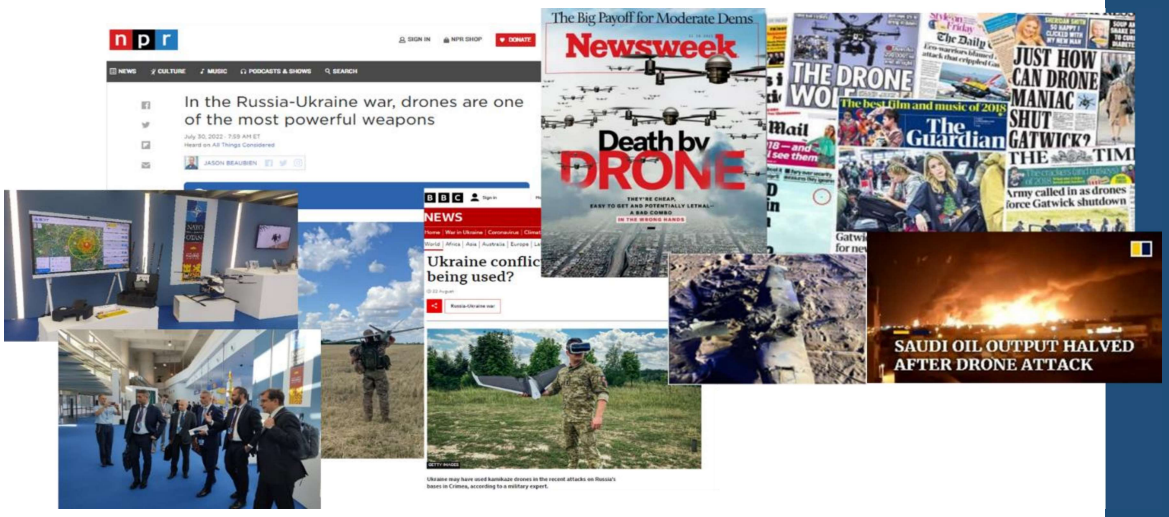
The C-RAM is a system of systems and not only a weapon, which is designed to protect both personnel and infrastructure from rockets, artillery shells, and mortars. The C-RAM system was not initially designed to attack the point of origin, because its primary mission is to destroy the incoming shell in the air. But nowadays, this is considered a desirable capability provided that the defending forces want to fully utilize their capabilities.

The C-RAM is a multitool. It can operate as a standalone system offering protection from incoming RAM, but also It can be a part of a greater system/node, contributing to the development of a more effective AD umbrella, offering mission-tailored defence. ■

Sources:

1. https://en.citizendium.org/wiki/Counter-rocket,_artillery_and_mortar
2. https://www.mbda-systems.com/press-releases/mbda-germany-prepares-the-way-for-c-ram-laser-weapon-system/
3. https://geneva.usmission.gov/2018/04/13/ccw-gge-u-s-slide-presentation-counter-rocket-artillery-and-mortar-system-c-ram/

NATO Counter Unmanned Aircraft Systems (C-UAS) effort



The widespread proliferation of Unmanned Aircraft Systems (UAS) poses a clear risk to civilian and military infrastructure, assets and people. The use of UAS capabilities by adversaries, both conventional forces and non-state actors, is rapidly increasing and evolving. Class I UASs are growing increasingly sophisticated, offering autonomous flight, high-end Intelligence, Surveillance and Reconnaissance (ISR) capabilities, and ever-expanding payload capacity, range, and endurance. They are widely accessible to potentially disruptive actors and could be assembled using components without identifiable markings, thus increasing the difficulty of attribution if used in an attack. For this reason, NATO has been pursuing a dedicated Counter UAS (C-UAS) effort since 2019, led by the NATO C-UAS Working Group, the single forum that includes the required expertise from different communities within all Allied nations. The Group is looking holistically through the DOTMPLFI (Doctrine, Organization, Training, Material, Leadership, Personnel, Facilities, Interoperability) spectrum to support Allies in developing solutions in this domain. The presentation will highlight the new efforts under developments in the fields of doctrine, threat scanning, standardization, development of capabilities, research, innovation, tests and exercises. ■

By Dr. Claudio Palestini
Emerging Security Challenges Division
NATO HQ

NATO Military UTM Project

By Mr. Roy Bookham
Senior Principal Consultant, Counter-UAS Platforms Systems Division, UK MoD
rpbookham@dstl.gov.uk

Aim

The Military UTM project aims to pull through findings from the earlier NATO Drone Single Local Air Picture (Drone SLAP) project and to outline NATO options for: "A "Military Uncrewed Traffic Management (UTM)" system that harmonizes/optimizes the output of emerging UTM initiatives with advanced C-sUAS DTI systems".

The DroneSLAP project identified a number of reasons (civil as well as military) why harmonization was likely to be useful to NATO and to member states. The "Military UTM" project is taking this work to the next stage. It will explore options and priorities and will address, demonstrate and publish how the harmonization benefits identified in the DroneSLAP findings could be realized for the benefit of NATO nations.

Background

The earlier Drone single local air picture (DroneSLAP) project identified a number of reasons **why** harmonization was likely to be useful, demonstrated that AI and ML could enhance UAS identification and potentially enhance the effectiveness of automated C-UAS surveillance systems, presented its UTM/C-UAS Integration Recommendations to NEASCOG and supported TIE 21. Circulation of the DroneSLAP findings generated dialogue about the level to which integration/harmonization should occur and how best to achieve it whilst identifying that member states have different harmonization priorities.

The "Military UTM" project commenced Apr 22 and will take this work to the next stage. It will explore options and priorities and will address **how** the harmonization benefits identified in the DroneSLAP findings could be realised for the benefit of NATO nations.

DroneSLAP recommendations include:

- Both C-UAS and UTM systems would benefit from integration
- Systems should be integrated early in development
- Remote ID should not be considered a silver bullet, particularly for rogue drones
- We should recognize that the roles of C-UAS and UTM will increasingly merge
- We should endorse effective automation of UTM and C-UAS DTI systems
- We need to assess cyber vulnerabilities introduced by integrated systems

Anticipated Benefits for NATO

We anticipate that NATO and member states will benefit from this study from an understanding of the potential for improved detection of rogue and hostile drones through the harmonisation of UTM/C-UAS, how UTM/C-UAS harmonisation can underpin the seamless management of all drones in a crowded military airspace, the technical/operational/legal issues involved in harmonising UTM and C-UAS systems, real world options for harmonising UTM and C-UAS and the use of Remote-ID within a Military context and direction and guidance on generation after next (GAN) R&D for harmonised C-UAS and UTM systems

Programme Deliverables:

Project will deliver a demonstration of a practical harmonised UTM/C-UAS system; early 23. A harmonised UTM/C-UAS system digital twin in the margins of TIE 22, a "Wider Options report" comparing

and contrasting demo outcome and other potential UTM/C-UAS options in March 2023. The programme will include Mil UTM "best practice" recommendations and recommendations for further work. Possible refined demonstration in late 2023.

The demonstration plans to address a number of Use Cases;

1. **UC1: General situational awareness**

The system will use cooperative and independent (ie non-cooperative) surveillance sources to demonstrate a live digital view of the airspace surrounding the infrastructure of interest.

2. **UC2: Separate own aircraft from other aircraft**

The system will enable clear separation of cooperative aircraft/UAS in the same airspace

3. **UC3: Identify and track non-cooperative aircraft**

The system will leverage the fused C-UAS system to identify non-cooperative UAS and underpin the separation of cooperative aircraft from them

4. **UC4: Predict threats of airspace infringements**

.

Fused C-UAS detections and both network and broadcast RID will be used to predict threats to vulnerable infrastructure in the area of interest.

5. **UC5: Predict conflicts between own and other aircraft**

The system will integrate radar and ADS-B to produce consistent surveillance information in a common operating air picture with a 30-second prediction to the correlated target's flight path

Demonstration;

A digital twin was deployed in the margins of TIE 22 in September in the Netherlands to illustrate the principle behind the demonstration and what we hope to achieve. UTM System demonstration contract let with contractor. Target for demonstration is for early 2023. Laydown, demonstration plan, location and associated C-UAS system agreed.

Wider Options;

Current investigation covers:

- AFRL/EUCOM DOWDING based system;
- UK NPCC WINDTALKER based heat map;
- Intent prediction development; draft contract with UK Industry (TBC)
- French system demonstration in Paris
- Happy to receive other suggestions from the floor ■

First Impressions from the NATO Counter – Unmanned Aircraft Systems (C-UAS) Technical Interoperability Exercise (TIE) 2022

By: Mr. Mario Behn, MSc ECE, MBA, BAss., Dipl. Ing. (FH) - NCIA
DEU VNC/Principal Scientist

Joint Intelligence, Surveillance and Reconnaissance

The NCI Agency supports NATO commands and Nations with technological and scientific expertise as well as procurement services in the C-UAS domain. This support ranges from assessment of new technologies, prototyping of C-UAS systems, development of systems of system architectures, definition of standards and organization of live exercises. The NATO C-UAS TIE series is the lead venue to nurture Technical Interoperability as one enabler in the C-UAS area (complemented with Operational Interoperability). TIE is conducted using a scripted scenario with a live red-team stimulus as the UAS threat. The C-UAS blue-teams concentrate on standards and data models, which enable exchange of information between a multitude of sensors, command and control (C2) systems and effectors. These industrial and governmental contributions from across the NATO & EU ecosystem allow for a wide range of Technical Interoperability Test Cases. TIE enables maturing interfaces – and hence allows improving real capability. This presentation will provide some first impression findings and observation of the second iteration of the NATO C-UAS TIE running from 13-23. September 2022 at the General Best Barracks located at in de Peel/Vredepeel, Netherlands.■

Pros and Cons of different C-UAS implementation solutions from the air defence perspective

By Colonel Jan FARLIK CZE (AF),

GS Assoc. Prof. Ph.D.
(jan.farlik@unob.cz)

Introduction

Unmanned aerial systems (UAS) are currently increasingly used for reconnaissance and offensive missions during various types of deployment. Recent or current conflicts in the world are proof of this. Modern armies must face this new threat and introduce antidrone (C-UAS) measures and buy C-UAS systems. Since the threat of UAS is very diverse, it is necessary to choose a variety of solutions. Defense against UAS Class II and III (according to NATO division) is more or less the domain of classical air defense using surface to air missile systems and is not the subject of this article. This article reflects on the threat of UAS Class I, especially category Small, Mini and Micro, including commercial drones freely available on the market. These UASs are the worst detectable and often less destroyable than the larger UAS. In essence, the article does not offer solutions, but summarizes questions that every army or alliance will have to deal with during the process of acquisition new C-UAS solutions.

What solution to choose?

The defense industry currently offers many different C-UAS solutions, each suitable for a specific type of deployment, fully in line with the known saying "There Is No Silver Bullet". There are solutions of static or mobile, armored or light C-UAS, with different types of detectors and both soft kill and hard kill effectors. Some solutions are closed (proprietary), while others are betting on interoperability and plug-and-fight solutions, where the system can be configured in various ways and selects the required components according to the type environment or mission. And here we get to the dilemma, what solution to choose to best suit the needs and way of deploying the forces of a particular user (army).
Possible solutions must be designed both according to the potential threat and according to the user who will use the solution. The danger from the UAS side is different for different types of forces and means. E.g. The airbase will solve different problems in the implementation of C-UAS solutions than the task group based on the mechanized brigade consisting of mobile armored elements. C-UAS solution for infantry platoon will be different from C-UAS solution for stationary command post. Much examples can be found.

Possible solutions

One of the main categories of land objects that are most at risk of using enemy class I (and no matter whether as reconnaissance or offensive) are undoubtedly ground forces on the front lines of own troops (FLOTs), maneuvering task groups, airbases, ammunition warehouses and command posts (mobile or stationary). Of course, this list is not final, but the most vulnerable in the ratio of "price/performance" or "profits/losses/risks". Each of these potential targets for enemy UAS has its specifics and it is necessary to use more or less different solutions to defend it.

Encapsulating C-UAS to various organizational structures

In essence, C-UAS systems can be implemented in the following organizational structures:

Classic Air Defense units - Within the ground/surfaced based air defense (G/SBAD), C-UAS units are designed not only for the protection of their own G/SBAD systems, but can also be earmarked as direct support for supported forces and troops. In this way, either a separate C-UAS battalion could be created within the brigade or regiment type of G/SBAD units, or separate C-UAS batteries could be created within the existing battalions. The third option could be to create a separate C-UAS firing platoon within each battery for its protection. However, the last option is insufficient to provide direct C-UAS support to other (non G/SBAD organic units). The optimal variant would then be the combination of the first or second variant and at the same time the realization of the third variant, which would serve purely for the C-UAS of the G/SBAD fire unit.

Army Organic Air Defence (AOAD) - Within AOAD, C-UAS units would be created for forces that normally do not have AD capability. An example is the airbase, which in its organizational structure has a stationary C-UAS system built into the airport infrastructure and a unit that operates these systems and defend the base. Another example is the mechanized brigade, which has armored C-UAS platoon purely designed to combat air targets.

Force Protection- Small units created purely to protect the living force. This unit is trained for C-UAS systems (usually man-portable) operation. These units are able to fully detect enemy UAS and partially destroy it, but only through lighter types of C-UAS solutions, because FP forces generally have the task to defend the force, another unit or base against a wider spectrum of threats, mostly ground. Undoubtedly, the above types of C-UAS implementation can be combined, but then there are higher demands on coordination and interoperability. In the next part of the article, there will be briefly introduced four models example (basic use cases) with C-UAS solution and possible problems in implementation.

Airbase

Use case A.1: Direct C-UAS support for airbase provided by G/SBAD brigade

The G/SBAD brigade (or regiment) will provide the C-UAS battery, which has the task to defend the surroundings and responding to possible attacks. In terms of efficiency, the number of separately standing sensors and effectors is important. In the case of a compact solution (one C-UAS vehicle), the variant is not very effective in terms of base size. Another problem may be interoperability and communication with the base staff during the air traffic. C-UAS solutions must not have systems (e.g. jammers) that would interfere with electromagnetic spectrum of airbase systems. There would be a high risk when using laser effectors (blinding pilots). The effectors are mostly cannon means and jammers.

Use case A.2: Organic C-UAS unit built within airbase organisation structure

The example airbase has a bespoke C-UAS system and its own trained unit. The system is designed for symbiotic operation with airbase systems and interference is excluded in the case of full base operation. The staff knows very well the surroundings

of the base, access routes, possible directions of threat and are able to respond quickly to the detected UAS. The staff knows the base infrastructure very well and can avoid accidental damage to key systems and infrastructure. The C-UAS solution is mainly a combination of active and passive sensors (mainly based on RF detection) optimally distributed around the base and effectors that cannot negatively act against their own forces and personnel. Operational procedures are designed to quickly find UAS and operator in the well-known landscape. Effectors include, for example, anti-drones, net throwers, or specially designed jammers. Many non-destructive means will ensure later forensic analysis. This unit can also operate within the airbase FP and provide its resources for purposes other than detection and elimination of UAS.

Note: The key elements of military airbases are mainly take-off and landing runways (TLR), other tracks, aircraft stands and also hives. When attacked by a class I drone, destructive damage or disruption of TLRs is rather not probable. However, aircraft stands may be possible targets, especially because of minimal protection of parked aircraft. The hives or hangars, i.e. shelters serve as a protective buildings, so there is a minimum chance of any damage from Class I UAS. The very likely targets are antennas, radar sites and navigation systems. All these elements are important components of the military airbases and ensure the activities and coordination of air traffic in the airspace in the immediate vicinity.

Mechanized brigade

Use case B.1: Direct support for C-UAS unit provided by G/SBAD brigade

In this case, the supporting C-UAS unit must be capable of moving with a supported unit, i.e. to be highly mobile. Its systems should be on one wheel or track platform, and have the ability to transform very fast from movement to combat ready status (ideally be combat ready after short stop in several tens of seconds. The unit must have practiced common procedures with a supported unit and know its way of fighting. Interoperability must be ensured for mutual communication, which is not always completely trivial in the case of cooperation between air and ground forces. In terms of the character of the supported unit, there is not so much emphasis on the type of effector. This includes both laser effector and broadband jammers. The cannon effector here is likely to be a systemic and operational restrictions requirements during the acquisition process so there will be minimal necessity in terms of its own viability of the platform within the ground combat activity. The sensor system will have to have a UAS detection radar with range at approximately 6+km (for UAS with RCS comparable to DJI Phantom) for early detection. The electro-optical detection system in the range of visible and thermal spectrum is a necessity.

Use case B.2: AOAD C-UAS units (or AOAD units for very short AD)

The primary effector is likely to be a cannon (30 or 35 mm) or laser and as a supporting effector a machine gun and/or jammer. In terms of the nature of the combat activity, the AOAD unit is unlikely to have capability to detect of an enemy UAS operator as well as the non-lethal elimination of UAS for later forensic analysis. Primarily, it will be a hardkiller. Sensor systems will probably be built at least on the radar with range of 6+ km (for early warning) and the electrooptical system (for guiding the effector). This organic AD element will be able to act not only against air, but also against ground targets, so that it can be used in the "classical" combat activities of the armored unit. In order not to be applicable against UAS only, it should have very short range guided missiles for action against enemy helicopters or subsonic aircraft.

Conclusion

This article defined some questions that will have to be answered by those who will decide to acquire a C-UAS solution for their national armies. C-UAS as such cannot only be defined as one system against enemy drones. It is very important to define the environment in which the future C-UAS system is to operate.

The C-UAS system is inherently a multifunctional device, often modular, whose possible components has its pros and cons and can only be deployed under certain conditions so as not to cause more damage to its own forces and systems. When creating specifications and requirements for future C-UAS, it is necessary to first define the scope and final users (stakeholders) that will use the specific variant of C-UAS system. For example, if it is necessary to secure the stationary C-UAS military airbase, it will probably not be possible to deploy the laser system and certain types of jammers. If so, it will be necessary to ensure

danger for its own troops (e.g. by blinding pilots, disturbing communication and airport security, etc.).■

U.S. Combat Training School: Advancing sUAS Training in Europe

By Dr. James C. Bailey
USAFE-AFAF Combat Training School
Ramstein AB, Germany

Contact Information
Please direct any questions to Dr. James C. Bailey at james.bailey.56@us.af.mil or call the Combat Training School at +49 (0) 6371-405-6150.

Overarching Questions

With the rapid advancements of drone technology in warfare, military leaders around the globe face a myriad of questions related to their employment. How can drones augment military duties to accomplish a mission? What are the limits of technology and the speed of its development? What threats do military organizations face with regard to nefarious groups using drones? Can forces systematically thwart drone threats or minimize potential damage? What are Counter-small Unmanned Aircraft Systems (C-sUAS)? Is there a one-size-fits-all solution? Can traditional air defense systems detect, identify, track, and defeat sUAS? Who is responsible for protecting military forces from drone attacks? Are systems and procedures interoperable enough to work jointly without fratricide? What rules and regulations must be followed? What can we do?

Approach to Finding Answers

A single organization cannot surmount a problem set this vast. Current events are proving just how fast technology evolves during conflict. Thousands of sUAS are successfully executing a host of mission types on any given day. Identifying a piece of the macro puzzle that aligns with an organization's strengths is where work can be catalyzed. Exponential opportunity exists when talented individuals from multiple stakeholder organizations collaborate to build dynamic teams that have access to a broader portfolio of capabilities and essential creative and organizational skills to produce results. For any progress to be realized, the scope of work must be commensurate with available resources. According to Desmond Tutu, there is only one way to eat an elephant; a bite at a time.

Scope

This paper will briefly describe the current administrative environment of this problem set and capture how the Combat Training School (CTS) advances related capabilities in Europe.

sUAS Classifications

Unmanned Aircraft Systems (UAS) consist of the unmanned aircraft vehicle (UAV) and necessary components for flight operations. The U.S. and NATO have different UAS classification definitions regarding size and range capabilities. Furthermore, conflicting definitions amongst U.S. agencies exist. According to the U.S. Federal Aviation Administration (FAA), sUAS weigh less than 55lb (25kg) (14 *C.F.R.* § 107, 2022). However, the U.S. Department of Defense (DOD) C-sUAS Strategy (2021) states that sUAS range up to 1,320lb (600kg), fly up to 18,000ft MSL, and have speeds up to 250 knots.

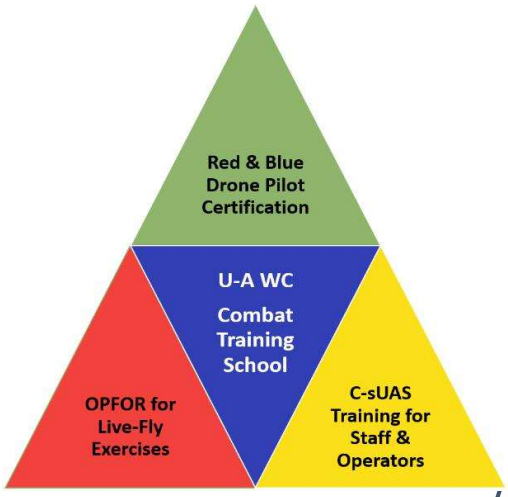
NATO class 1 covers drones weighing up to 150kg (330lb), flying up to 5,000ft AGL, and as far as 50km line of sight (NATO, 2014). Existing classification matrices do not discriminate between fixed and rotary wing configurations.

The Combat Training School

In 2011, the European Integrated Air and Missile Defense Center (EIAMDC) was founded to champion the increasing need for Integrated Air and Missile Defense (IAMD) education and training in support of the European Phased Adaptive Approach (EPAA). The EIAMDC was operationally capable by 2015. In 2021, this unit became the U.S. Air Forces in Europe and Air Forces Africa (USAFE-AFAF) Warfare Center's Combat Training School. The CTS mission is to develop joint and coalition IAMD forces through tailored academics, assessments, experimentation, and wargaming in collaboration with key partners (USAFE-AFAF, 2022).

sUAS Training Approach

The CTS pursues three distinctly separate lines of effort under the sUAS umbrella:



Effort 1 - sUAS Pilot Training

In coordination with colleagues at Air Force Special Operations Command (AFSOC), the CTS develops and circulates approved lessons to ensure red and blue sUAS forces are ready to support military operations, related tests, and exercises. The Polygone Range in Germany affords the CTS with a 10-acre practical training site to conduct proficiency training under controlled airspace.

Effort 2 - Training for Staff & Operators

Staff Academics. This one-day seminar provides personnel with an understanding of IAMD strategy, doctrine, and policy considerations, which includes fundamentals, threats, current events, sensors, interceptors, communications, command and control (C2), readiness, planning considerations, and IAMD future forces. This course educates students on the significance of integration and interoperability in the joint fight. The seminar is intended to reach U.S. military staffs performing functions of IAMD operations and planning.

Mobile Education Training Team Events. In coordination with the Competence Centre Surface Based Air and Missile Defence (CC SBAMD), the CTS travels to provide tailored courses to multinational audiences.

Collaboration with Outside Agencies. Professional currency is an important ingredient of credibility. The CTS consistently attends the NATO C-UAS Working Group to build important relationships, maintain awareness of current projects, and contribute to the cause. The CTS also sends its members to kinesthetic training opportunities, such as the U.S. Joint C-UAS Academy and Threat Management Group's Unmanned Aircraft Systems Emerging Threat (UASET) courses.

On-demand. General and flag officers often reach out for training on specific emerging threat topics, which recently consisted of sUAS and hypersonic briefs to the 3rd Air Force Commander. The CTS routinely provides instructional courses for NATO School Oberammergau, the U.S. Army's Multidomain Taskforce, and the Joint Ballistic Defense Training and Education Center (JBTEC).

Effort 3 - Exercise Involvement

The CTS has historically provided modeling and simulation (M&S) and expert analytic support to large-scale joint and multinational IAMD exercises. As an office working on defense designs, identifying events that are optimal to test or validate certain capabilities is a challenge. The CTS championed the addition of C-sUAS into the 2022 iteration of EUCOM's premier IAMD exercise, Astral Knight (AK). The CTS was instrumental in coordinating with force protection professionals to develop and publish C-sUAS training objectives, which were essential to incorporating this layer of IAMD into AK-series exercises. In AK23, the CTS will fly sUAS opposing forces (OPFOR) sorties in order to provide a tangible threat representation for participants.

sUAS Office of Primary Responsibility (OPR)

This year, the CTS formally assumed the USAFE-AFAF sUAS OPR role. In accordance with AFMAN 11-502 (2019), this position oversees small drone programs for U.S. Air Force organizations on the European and African continents. The CTS coordinates with other major commands, cultivates best practices, and reviews pilot training programs for sUAS operators at subordinate installations.

USAFE-AFAF sUAS Partners

Within the Air Force Staff, a number of offices support

efforts relating to drone operations. The CTS works continuously to synergize these offices and produce the best outcomes for the air component commander. The roles and responsibilities for operations, logistics, and strategic management of sUAS and C-sUAS programs is distributed between several key organizations within USAFE-AFAF.

A4S

This office equips air bases with C-sUAS capabilities. A4S is primarily staffed with security forces troops who liaise between EUCOM and AFRICOM J34 (C-UAS) and the operators at air bases. They currently secure funding for C-sUAS equipment and oversee the field service representatives (FSR) who train operators and maintain C-sUAS equipment.

A5M

This office probes defense designs for Air Base Air Defense (ABAD). The growing cruise and ballistic missile threat to air bases in Europe is forcing USAFE executives to reassess defensive options, including active ground-based systems currently assigned to the U.S. Army (Vick et al., 2020). As the ABAD OPR, A5M houses an innovation lab that directly engages in sensor fusion activities to ensure operations centers have early warning indication of all threats in the skies. Furthermore, this office evaluates command and control (C2) methods to develop streamlined processes and tangible prototypes. A5M planning efforts allow air defense operators and leaders to execute more efficiently and effectively.

86th OSS

Ramstein Air Base's 86th Operations Support Squadron is not a major command headquarters office; however, assigned C-130 pilots are administratively standardizing sUAS flight operations at the 86th Airlift Wing. Their regulatory products directly establish guidelines for Ramstein Air Base while also informing sUAS programs at other bases throughout USAFE-AFAF.

Message to Multinational IAMD Professionals

According to the U.S. DOD C-sUAS Strategy (2021), we cannot rely on technical and procedural solutions alone to protect our interests. The U.S. continues to leverage its biggest competitive advantage by being the partner of choice. With long-standing relationships across the globe, the U.S. prioritizes interoperability and information sharing to protect its interests and assist its allies and partner nations.

The CTS is an agile, highly specialized organization that delivers value-added training experiences to air component members, joint colleagues, and in some cases for international partners. As our allies and partners integrate sUAS into their national airspace systems, commanders abroad will need to adapt to the implications of increasing numbers of sUAS operating in the vicinity of U.S. forces (DOD, 2021). The CTS is here to help navigate the challenging operating environment in concert with other progressive organizations.

References

14 C.F.R. § 107 (2022). Small Unmanned Aircraft Systems. Retrieved from: https://www.ecfr.gov/current/title-14/chapter-I/subchapter-F/part-107

NATO Standardization Agency (2014). NATO STANAG 4670 – ATP-3.3.7, (Edition 3) Guidance for the Training of Unmanned Aircraft Systems (UAS) Operators. Retrieved from: http://everyspec.com/

U.S. Air Force (2019). Air Force Manual 11-502; Small Unmanned Aircraft Systems. Retrieved from: https://static.e-publishing.af.mil/production/1/af_a3/publication/afman11-502/afman_11-502.pdf

U.S. Air Forces in Europe and Air Forces Africa (2022). Combat Training School. Retrieved from: https://www.usafe.af.mil/Units/Warrior-Preparation-Center/Combat-Training-School/

U.S. Department of Defense (2021). Counter-Small Unmanned Aircraft Systems Strategy. Retrieved from: https://media.defense.gov/2021/Jan/07/2002561080/-1/-1/1/DEPARTMENT-OF-DEFENSE-COUNTER-SMALL-UNMANNED-AIRCRAFT-SYSTEMS-STRATEGY.PDF

NATO STANAG 4670 – ATP-3.3.7, (Edition 3) Guidance for the Training of Unmanned

Aircraft Systems (UAS) Operators, NATO Standardization Agency, 2014. http://everyspec.com/ (Accessed 24 Feb 2016).

Vick, A., Zeigler, M., Brackup, J., Meyers, J. (2020). Air Base Defense: Rethinking Army and Air Force Roles and Functions. Rand Corporation. Retrieved from: https://www.rand.org/pubs/research_reports/RR4368.html

“How can we improve individual & collective IAMD training to adapt to new challenges?”

By LtCol C.W.Pronk NLD (AF)
JAPCC SME for SBAMD

In a world facing such a substantial geo-political shift, Integrated Air and Missile Defence (IAMD), and more specific Surface Based Air Defence, is gaining more importance as an essential part of NATO’s Defence Counter Air capability. Are NATO’s SBAMD forces ready for this? In the 1980’s, the US Army had a promotional poster stating: “Air Defence, First to Fire!” This was as true a statement during the cold war, as it is now 40-years later. Since the early 1990’s operations, both allied and non-allied, have all started with an air dominant operation to neutralise the enemy’s Command and Control. This also means that air defence must be able to fight in the twilight between crisis and conflict, with little or no warning time. Operating in that twilight zone means that civil and military air-procedures and structures will be in force. The protection of friendly aircraft is as important as maximum attrition of the enemy. Further, and especially during conflict, it is of paramount importance that proper coordination and clear identification procedures are understood and in place, where blue-on-blue engagements are a near constant possibility. It is of vital importance that air defence operators are at full NATO mission readiness now and not tomorrow, since there will never time enough for education and training, especially when it is too late to realise the need. Nations, supported by NATO should take every available step, now, to ensure combat-ready SBAD for a time when conflict may be upon us. The alliance has the required tools in its inventory, but how can we sharpen, shape and use these tools most efficiently? ■

NEW E&T OPPORTUNITIES FOR FUTURE IAMD CHALLENGES

Introduction

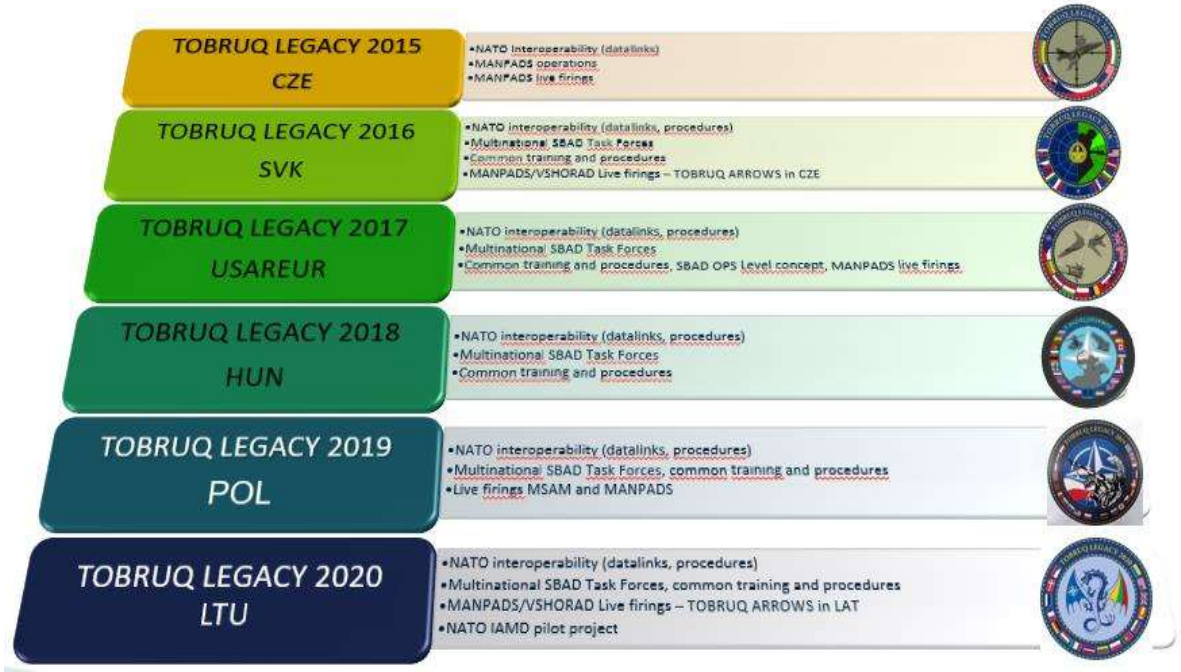
This article aims to introduce the most recent achievements, developments and offers in the field of IAMD Education & Training. The focus will be on two major activities directed towards the NATO nations which are RAMSTEIN LEGACY EXERCISE and IAMD COMMON EDUCATION & TRAINING PROGRAM.

By Maj Peter RABINAK CZE (AF)
IAMD CoE SME

RAMSTEIN LEGACY

Starting with little bit of the history, one of the first initiatives to reestablish sort of **multinational SBAD** training appeared in 2015 with first iteration of TOBRUQ LEGACY (TOLY) Exercise. The idea was to have a SBAD exercise focused on interoperability and TTPs which will be organized every year by different framework nation.

There were six consecutive iterations conducted and the idea of the exercise grew over the expectation. In the beginning it was tiny platoon level exercise focused mainly on cooperation of MANDPADs units on the battlefield which has turned in a simulation of high scale NATO IAMD operation where all levels of commands going from JFAC through national CRCs all the way to the last fire unit were exercised. Tens of nations participated with multiple thousands of soldiers every year with gradual support of flying forces, NATO AWACS, NCIA and other NATO entities.



In the end TOBRUQ LEGACY was so big, that it was impossible to be handled by one single nation. Therefore, new concept of the exercise called RAMSTEIN LEGACY has been adopted and introduced by NATO.

RALY is the first (and only) NATO's LIVE IAMD Exercise which:

· provides a venue to test new NATO IAMD Concepts,
· combines several air exercises on the timeline to benefit from each other,
· has a Tactical Focus with an Operational Impact and a strong Strategic Message!

Speaking about strategic massage, during first iteration of the exercise conducted in Jun 2022, 14 nations were able and willing to deploy their SBAD systems into the exercise theater (POL, EST, LAT, LTU) and train together despite having been dealing with real world situation at Ukraine.

Planning considerations of the exercise were as follows:

1. Project of future NATO Live IAMD Exercises in line with SACEUR's Deterrence and Defence of the Euro-Atlantic Area (DDA).
2. Incorporates existing live exercises into one HQ AIRCOM led IAMD MTEP Ch1 exercise on biennial basis.
3. C2 components with AWACS support, national airborne AD and SBAMD forces to exercise tactical C2 of IAMD across all domains in a 2-years cycle.
4. NATO crisis TDL network design.
5. Supported with flying assets from NATINAMDS / AIR POLICING exercises.

Supported with one of the itineration of Electronic Warfare (EW) LIVEX.

All the considerations were at least partially turned into the reality during the first run conducted in June 2022. This fact appears to be very promising for the future iterations which are going to be hosted by Romania and Bulgaria in 2024 and Czech Republic, Slovakia and Hungary in 2026.

IAMD COMMON EDUCATION & TRAINING PROGRAM

The second part of the paper is dedicated to the IAMD COMMON EDUCATION & TRAINING PROGRAM (CET-P), which origins are heavily connected to the TOBRUQ LEGACY Exercise.

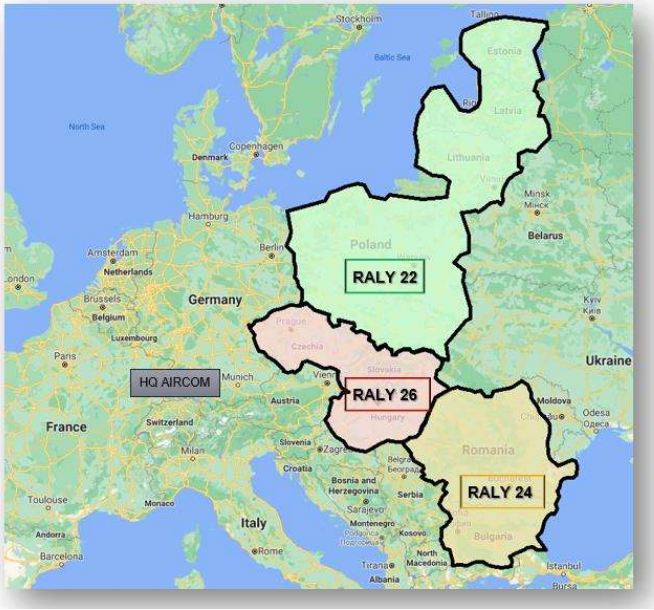
Through the process of execution of the first two iterations of TOLY participants themselves realized they were still missing something more important than any technology. There was neither knowledge nor common understanding of NATO TTPs.

Most of the nations used their national procedures to control their units but when it came to the execution of the operation in multinational environment it was real struggle. Therefore, pre-exercise academics started to be held since 2017 teaching participants NATO procedures.

In 2021, based on TOBRUQ LEGACY 2015-20 findings, the initiative to establish NATO SBAMD CET-P has been taken by CAOC UE. Initial letter mentioned that a wide variety of different initiatives were ongoing to gain improvements in one of NATO's major challenges: The integration and connectivity between national SBAMD forces, national CRCs and NATO entities. Beside the technical challenges, we were also facing the issue of a lack of common understanding on execution of NATO TTPs. This lack of common understanding hampers the conduct of multinational Training & Exercises and has a subsequent negative effect on mission execution of NATO IAMD Task Force & Mission

At the same time, available education offers at NATO level (courses at Oberammergau) were neither sufficient nor detailed enough to fulfil the needs of operators at the tactical level. So, the intent was to develop a standardized set of education modules and to offer the opportunity for Nations to request NATO provided Training in preparation of multi-/national exercises and missions (starting with RALY EX, VJTF mission etc).

To fill the gap in NATO IAMD education, a course called IMAD CET-P has been developed and is being delivered by specialists from IAMD COE, JAPCC, CCSBAMD, AIRCOM A7 and both CAOCs.



RALY 22

Location: POL, LTU, LAT, EST
Combining: TOLY, RAAL, RAGU, AK
Focus: Art5, C2, SBAMD, Interoperability, Tactical level, Live Firing possibility

RALY 24

Location: ROU, BGR
Combining: TOLY, RAGU, RADU, US led EX
Focus: Art5, C2, SBAMD, Interoperability, Tactical level, Live Firing possibility
Coordination : Steadfast Defender 24

RALY 26

Location: SVK, CZE, HUN
Combining: TOLY, RAGU, RADU, US led EX
Focus: Art5, C2, SBAMD, Interoperability, Tactical level, VSHORAD Live Firing possibility

The creation of the course was based on following criteria:

- Based on TOBRUQUE LEGACY 2015 – 2020 findings, **NATO SBAMD TTPs** identified by AIRCOM as a **critical knowledge gap** among the NATO Nations.
- Aims to **provide NATO Nations with consolidated tactical education** on execution of SBAMD Operations under JFAC command.
- Creates theoretical bases which can be practically trained during RAMSTEIN LEGACY / JPOW exercises.
- Recently **added to BMD (Future IAMD) DAP** (Discipline Alignment Plan).
- **Primary Training Audience:**
  - **National SBAMD Instructors / Trainers / Lectors**
  - SAMOC / SBAMDOC / GOC / FU Operators / Planners
  - SAMCOs / CRC SAM Allocators / SAM Allocator Assistants

In addition, all the above-mentioned entities are forming the CET-P working group which makes sure that the overall content is relevant to the latest developments.

IAMD CET-P Topics:

- DAY 1: **Introduction to NATO IAMD**
  - NATO C2 Structure / Responsibilities
  - Air C2 / ATO Cycle / JPDAL process
  - Data Link Connection
  - Threats to SBAMD forces
  - Hot Wash Up
- DAY 2: **Tactical Education**
  - SBAMD Planning process / Principles
  - SBAMD Operating Areas / ACMs
  - MoC / MoO / TBMFs / COVREP / Movement Execution
  - TBMF Vignettes
  - Hot Wash Up
- DAY 3: **Tactical Education**
  - RS / WCS / FCOs
  - Reporting / SSTO / SSREP / KILLREP
  - Reporting Syndicate Work
  - Other Aspects of IAMD Mission – AOAD / C-RAM / C-UAS
  - IAMD Training Opportunities
  - Hot Wash Up
  - Training Critique

After AIRCOM's A7 initial lead & coordination of content development, there were first two iterations organized by JAPCC to prepare RALY 22 participants. One more iteration will be held in JAPCC in late 2022 provided mainly for JPOW 23 participants.
On 01st August 2022 IAMD COE officially took over the lead role and overall responsibility for the course and its first task will be organization of 2023 iterations in Chania and then conversion of CET-P into NATO "APPROVED" Course.

SUMMARY

The article was dealing with two major IAMD education and training initiatives.
Firstly, RAMSTEIN LEGACY as a new NATO LIVEX offering wide variety of opportunities to implement new technologies, experiments, concepts and lessons learned in order to be better prepared to face the future challenges.

Secondly, we spoke about IAMD CET-P – the first ever TACTICAL IAMD COURSE provided by NATO to its nations and their SBAMD forces.
But both introduced activities pointing to one undisputable fact: **Technology means nothing without well educated people following correctly the same tactics, techniques and procedures on the battlefield.** ■

IAMD CET-P SCHEDULED ITERATIONS & POCs:
07 – 11 NOV 2022 @ JAPCC / Kalkar
POC: LTC Gijsbertus "Berry" Pronk: Pronk@japcc.org
08 – 12 MAY 2023 @ IAMD COE / Chania
30 OCT – 03 NOV 2023 @ IAMD COE / Chania
POC: MAJ Peter Rabinak: p.rabinak@iamd-coe.org

How the Proliferation of Stealth Technology Leads to New Air Defense Challenges

By Prof
Marc Jean Médard ABADIE
ICGM, University of Montpellier,
CNRS, ENSCM, Montpellier, France

INTRODUCTION

The development of novel materials for special /specific applications, like coatings for stealth technology, is an important challenge in the development of additive manufacturing. During the past few decades, Air Defences (Ground Based and Airborne ones) managed to create a lethal environment for modern day aircrafts (a.k.a A2/AD – Anti-Access/Area Denial). In turn Air Force based it's answer in several state-of-the art technologies, with the most dominant one being STEALTH technology. In general STEALTH technology incorporates a number of principles, like shape, airframe design, internal transfer of fuels and munitions and the implementation of **Radar Absorbing Materials (RAMs),** with the aim to minimize the detection range of a certain radar, in such levels where the STEALTH aircraft can fulfil its mission practically undetected and without being subject to fire (even retaliating one while egress from the target area). While RAMs can't solely reduce the Radar Cross Section (RCS) of a said target to minimal levels, they can provide a significant portion of the overall STEALTH efforts. It should be stated here that there is proportionate connection between radar detection range and RCS (based on Radar Equation) and in order to cut detection range in half you must reduce the RCS by a power of 4 (that's 16 times). Since their first implementation RAMs have constantly been evolving. One of the most commonly known types of RAMs is iron ball paint [1]. It contains tiny spheres coated with carbonyl iron or ion ferrite. Radar waves induce molecular oscillations from the altering magnetic field in this paint, which leads to conversion of the radar energy into heat. The heat is then transferred to the aircraft and dissipated [2].

Many attempts have been made for absorption with conductive and magnetic materials including carbon, metals and conducting polymers and recently using **Carbon Nanotubes (CNTs) reinforced composites to decrease reflectivity of the aircraft without ever reaching the ultimate state that leads to invisibility** [3]. Composite-materials with their exceptional multifunctional properties may transform the functioning of aviation (Defence) industry dramatically. One of the advantages of RAMs is that they can be applied directly to legacy systems without dramatically affecting aerodynamics and performances, and thus contribute to the reduction of their RCS (like the Have Glass program which is applied to the F-16s and the F-35s).

Recent publications try to update some general conclusions that must be considered. However, they are more general than specific. Thus Dr. H.L Zhang et al. [4] have used HNO3 as a π-type dopant to improve the EMS performance of CVD graphene. In a review published in 2018 A. Kolanowska [5] and her team have summarized and critically evaluated the hitherto efforts in the production and applications of CNT nanocomposites/hybrid materials as key constructional civil and military elements, preferably as coatings, layers, films, textiles or panels, towards attenuation of the radio wave radiation and have concluded that the research in the field is just at their beginning. J. Zhao [6] has recently studied high-temperature-resistant coatings with low infrared emissivity prepared using poly(siloxane) resins that show promising results to be used for infrared stealth technology or energy savings in high-temperature equipment. R. Guzman de Villoria [7] has studied the enhancement of laminated composites via aligned carbon nanotube interlaminar reinforcement. Dr J. Caro [8] has underlined the possibility of using Metal-Organic Framworks (MOFs) principle for advanced manufacturing materials while DK. Zikidis [9] and Marc J.M. Abadie and Sozon Leventopoulos [10] have made already preliminary investigations concerning Low Observable Principles, Stealth Aircraft with the VLO_tech project. After describing the EMI radiation and the mechanisms of shielding, we will focus on the nature and the chemical aspects that govern the furtivity (LO).

After describing the EMI radiation and the mechanisms of shielding, we will focus on the nature and the chemical aspects that govern the furtivity (LO).

ELECTROMAGNETIC INTERFERENCES (EMIs)

When electromagnetic (EM) wave radiation in the gigahertz (GHz) range interfere with the input signal of the electronic devices, they create a noise that is known as electromagnetic interferences (EMIs).

· EMIs consist of electromagnetic waves that comprising both the E (Electric) and H (Magnetic) field components and oscillate at right angles to each other – Fig 1.

· Each of these components respond differently to parameters like frequency, voltage, distance, and current.

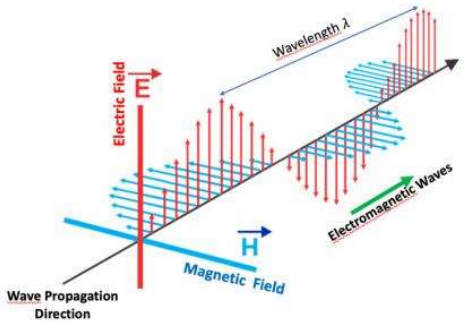


Figure 1. Electromagnetic radiation vector

The majors factors governing microwave attenuation are :

· **Electrical conductivity σ** (electric field)

- electrical conductivity is a measurement of how easily a material allows electric current to flow through it. Inversely, electrical resistivity measures how strongly a material resists the flow of electric current. The two properties are exact inverses of each other.

· **Permittivity ε** (electric field)

- a material with high permittivity ε polarizes more in response to an applied electric field than a material with low permittivity, thereby storing more energy in the material.

· **Permeability μ** (magnetic field)

- permeability μ is the measure of magnetization that a material obtains in response to an applied magnetic field.

MECHANISMS OF SHIELDING

Shielding efficiency (SET) could be defined as parameter that measures how well a material impedes the EM energy of a certain frequency when passing through it. Fig 2. represents the possible interactions of EM waves with materials.

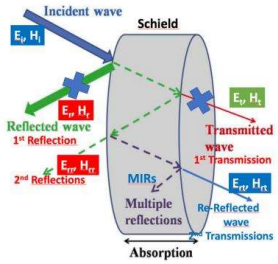


Figure 2. Schematic diagram of incident, reflected and transmitted power and electromagnetic field intensities when an EM wave is incident on a 3D material

When the EM waves fall on the front-face of the material then a certain part of the incident power (PI) is reflected (PR), while a certain part is absorbed and dissipated in form of energy, and the remaining part is transmitted (PT) through the shielding material. Therefore, three different processes namely reflection, absorption and multiple internal reflections contribute to the whole attenuation, corresponding to shielding effectiveness SER, SEA and SEM, respectively. The shielding efficiency is the ratio of the field before and after attenuation of electric and magnetic field and can be expressed as:

- $S_T\,(dB) = 10\log(P_I/P_T) = 20\log(E_I/E_T) = 20\log(H_I/H_T)$ and
- $S_T\,(dB) = S_R + S_A + S_{MR}$

with P, E and H refer to power and electric and magnetic field intensities while subscripts I, T, R and MR represent the incident, transmitted, reflected and multi reflected components, respectively.

- Shielding effectiveness through reflection loss (SE_R)

$$SE_R = -10log_{10}\left(\frac{\sigma_T}{16\omega\epsilon_0\mu_r}\right) \quad \Rightarrow \quad SE_R\,(dB) \propto F(\sigma T/\mu r) \qquad \text{Eq. 1}$$

From the relation it is clear that the reflection of MI radiation is mainly governed by the ratio of electrical conductivity and permeability of the shield material.

- Shielding effectiveness through absorption loss (SE_A)

$$SE_A = -8.68t\left(\frac{\sigma_T\omega\mu_r}{2}\right)^{\frac{1}{2}} \quad \Rightarrow \quad SE_R\,(dB) \propto F(\sigma T.\mu r) \qquad \text{Eq. 2}$$

The magnitude of SEA is dependent on the product of the electrical conductivity and permeability of the shield material.

- Shielding effectiveness through multiple reflections (SE_{MR})

$$SE_{MR} = 20log_{10}\left(1 - e^{\frac{-2t}{\delta}}\right) = 20log_{10}\left|\left(1 - 10^{\frac{-SE_A}{10}}\right)\right|$$

$$\delta = \frac{1}{\sqrt{\pi f \mu \sigma}}$$

where :

- σ_T represents total conductivity
- μ_r corresponds to the relative permeability
- ω the frequency
- $\epsilon 0$ the permitivity
- t is the thickness of shield
- δ corresponds to the skin depth

The SEMR is closely related to absorption ability of the shielding material and is mostly important for the materials like composites with dispersed filler and structure with multiple boundaries. From the relation it is clear that in case of shield with high absorption ability (SEA) and thickness, the SEMR can be safely neglected. This is mainly due to the fact that at higher frequencies, while travelling from one boundary to another the magnitude of EM wave becomes negligible due to the absorption. SEMR can also be neglected when SEA is greater than 15 dB or the shield thickness is higher than the skin depth due to increasing absorption from the internal surface :

$$\Rightarrow \quad SE_T\,(dB) \approx SE_R + SE_A$$

The electric field components, EMI attenuation can be improved via materials with high conductivity, but reduced by materials with increased permeability, which in contrast improves attenuation for the Magnetic Field Component. As such, increased permeability in a system with E-field dominated EMI will reduce attenuation but the attenuation will improve in a Hfield dominated EMI. However, due to recent advancements in technologies used in creating electronic components, the **E-field is usually the major component of the interference.**

Note that the efficiency of shielding materials (SE) towards attenuation can be estimated using a vector network analyzer (VNA). Since operating frequencies of signals are widely spread in GHz frequency range, analysis of EM attenuation parameters in broadband frequency spectrum is necessary. The incoming EM radiation interacts with the shield and attenuates it through various mechanisms like reflection, absorption and multiple reflections depending on the characteristics of shielding material.

COMPOSITION OF THE SHIELDING MATERIALS

The analysis of EMI physics and its consequences on stealth shows that the absorbing part – shield, as the barrier to EM waves is the main core of the stealth efficiency. In particular the structural and chemical composition of the absorber container, but also its thickness. We will describe this evolution by presenting its various components and their role in the shielding effectiveness.

- **Composites vs. Nano-Composites** The reinforcement of polymer matrices with fibers (glass, carbon, aramid Kevlar®) or woven fabrics (tissue, chopped tissue, plate, mat, chopped mat, Rovimat ®) has led to the formation of new materials called "**composites**" with mechanical and physical properties considerably superior to the unfilled product.

A new advance in the composition of composites has led in the late 1980s the company Toyota to develop a new type of composite reinforced by nanometric fibers (nano-platelets clay MMT) at a very low concentration of a few percent, (1 to 5 wt. %) called "**nano-composites**", allowing a lightening of the material without losing mechanical properties. This revolution has been exploited in many fields, in particular in the field of furtive materials. For both composites and nano-composites the interface/interphase play a crucial role in the integration of the reinforcement agent into the matrix. In contrast for nano-composite the filler at nano scale (10-9 m) does matter by increasing the surface area on nanoparticles. In that case the dispersion of the nanofiller and the homogeneity of the nano-composite has to be considered and treated.

- **"Get-lost" Concept**

One of the major innovations is based on the use of conductive nano-reinforcement agents in order to perturb and improve the dissipation of electromagnetic waves inside the shield. In this way it make it possible to treat the incident electromagnetic radiation in such a way that there is no reflection or at least highly minimized. The goal is to "scare and panic" the incident radiation by subjecting it to different reflections, collisions, absorbance, etc., properties that will be rendered by simple coating as monolayer or multi-layer design of the cladding by stacking lamina lay-ups and make up the laminate composite. Therefore this phenomenon is regarded by us as the "**Get-lost**" strategy – **Fig. 3** shows multiple reflections for the structure of carbon nanotubes (CNTs) compared to the carbon fibers (CFs) indicating a better absorption of EM radiation.

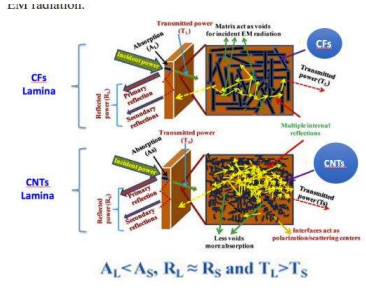


Figure 3. Comparison of EM waves process and pathways for lamina with carbon fibres CFs or carbon nano-tubes CNTs

- **Fillers and Nano-fillers**

According to Eq. (1) and Eq. (2) the stealth efficiency is proportional to the electrical conductivity σT whereas the magnetic component corresponding to the relative permeability μr has to be optimized.

To reduce reflection loss and significant absorption of the radiation, the shield should have electric and/or magnetic dipoles which interact with the electromagnetic fields in the incident radiation. Therefore, numerous attempts have been made to introduce at a molar scale fillers such as :

– dielectric (BaTiO3, TiO2, ZnO etc.) materials,

– magnetic (γ-Fe2O3, Fe3O4, BaFe12O19 etc.) materials or

- multiferroic magneto-electric compound bismuth ferrite BiFeO3 (BFO) within various matrices as filled inclusions.

At nano-scale, for which you have greater surface compared to molar scale and therefore much more reflections (more absorbance), you find graphene platelets GNPs [11] and related structures such as graphene oxide (GO), reduced graphene (r-GO), CNTs (SWCNT, MWCNT) [12, 13], graphite – **Fig. 4**. GO, obtained by oxidation of graphene, having many polar functionalities allow a better integration of the nano-filler inside the matrix as well as a better homogeneity without tendency to create aggregates as it is for r-GO – **Fig. 5** [14].

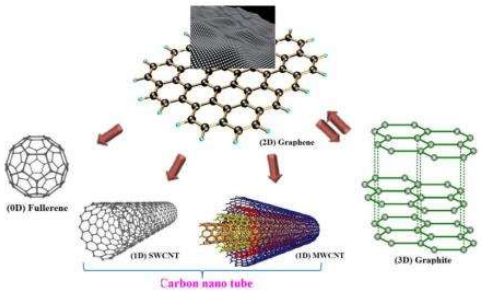


Figure 4. Graphene and related structures

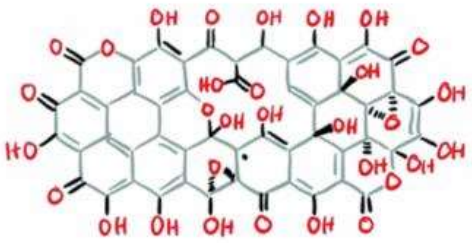


Figure 5. Structure of graphene oxide

Carbon nanotube from layered transition metal dichalcogenides [(inclusion structure with tungsten disulfide (WS2)] developed by Reshef Tenne [15] have also been considered and prove their stealth efficiency [16]. Interesting cage structures have been developed such as Polyhedral Oligomeric Silsesquioxane (POSS®) consisting of a silica cage core, as well as other organic functional groups attached to the corners of the cage (such as alkyl, alkylene, acrylate, hydroxyl, or epoxide unit). The main advantage of POSS® is the ease of changing of the functionality, solubility, polarity, and reactivity of these molecules through modifying the organic groups with a variety of functional groups – **Fig. 6a**. Recently a modification of the cage has been reported where a new cage structure has been proposed by replacing the Si atom by a Metal (Fe, Co, Cu, Ag, Au, Sc, Y etc. and lanthanide group) to accede to a new class of conductor system, the POMS® family – **Fig. 6b**.

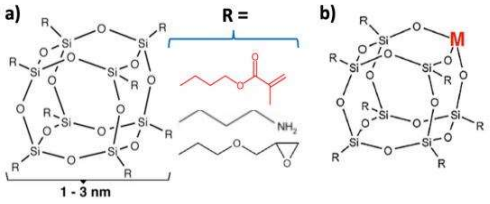


Figure 6. a) Polyhedral Oligomeric Silsesquioxane POSS®, **b)** Metal-polyhedral Oligomeric Silsesquioxane POMS®

During the last decade a great number of publications has been produced. All of them used on its own or in combination reinforcement agents at molar scale (metal) and/or at nano-scale. Best results were obtained with a mixture of fillers and nano-fillers. For example Injamamul Arief et al. [17] and Sourav Biswas et al. [18] have reported and compared a blending of conducting multiwall carbon nanotube (MWCNT) and highly efficient replacement by blending conducting multiwall carbon nanotube (MWCNT) and FeCo anchored covalent cross-linked reduced graphene oxide (r-GO) with poly(vinylidene fluoride) (PVDF) – **Fig. 7.**

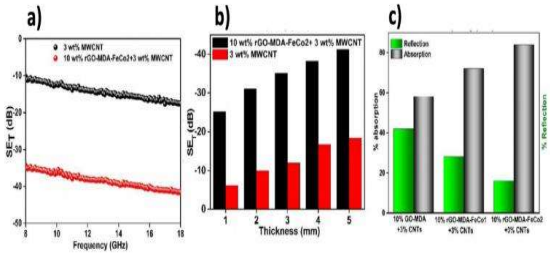


Figure 7. a) SE_T values of the composites as a function of frequency, **b)** total shielding effectiveness with respect to shield thickness, **c)** absorption and reflection component of total shielding at 18 GHz [17]

· **Matrices**

It is well known that Polymers are insulator. However in the 1980s Shirakawa et al. [19] found that once doped a few class of polymers such as polyacetylene, polyaniline, polypyrrole – **Fig. 8** are conductor of electricity.

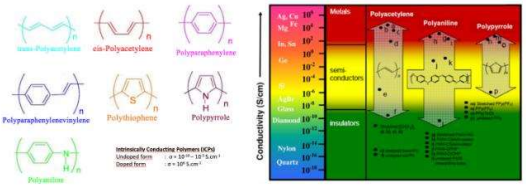


Figure 8. Conductive polymers

But the constraints inherent to the products (solubility, chemical stability of the dopant) and their industrial exploitation have ruined the hopes carried on these conductive polymers.

One of the originalities of the laminate is the use of polymeric binder having in the chemical structure metals along the chain (PFSs) or incorporated by complexation (MOFs). These types of binders represent groundbreaking objectives that have not been considered so far by any patents search carried out [20].

Another approach to promote conductivity inside the matrix is to use supramolecular chemistry. As example the presence of an inorganic element (metals and metal centers) in organic moieties – metal-containing macromolecular systems Metallopolymers [21], has led to a number of new physicochemical properties while implementing novel functionality to the polymer matrix.

A good example is given by Polysiloxanes with ferrocene as pendant groups or along the chain and ferrocenyl functionalized monomers [22] – **Fig. 9.**

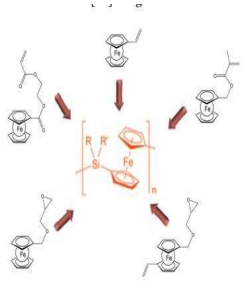


Figure 9. Metallopolymer : Poly(ferrocenyl dimethylsilane) [PFS] surrounded by typical ferrocenyl functionalized monomers.

For coating, the majority of resins used are based on epoxy or polyurethane. Surprisingly, apart from polyurethane and silicone, elastomers are ignored

even though they have interesting damping properties and can be an EMI absorber. Polybutadiene, polyisoprene and polystyrene - polyisoprene PS-PI diblock or polystyrene-polyisoprene-polystyrene PS-PI-PS triblock copolymers are particularly promising.

Recently K. Nath et al. [23] proposed the use of poly(lactic acid) as biodegradable material used as binder of the shield.

Another point that should be mentioned is the influence of the presence of air bubbles on the shielding efficiency in terms of reflection/absorption [24]. P.Banerjee et al. [25] show that the the specific EMI shielding for the foamed composites (1.0 wt.% loading of MWCNT) was higher at 21.3 dB cm3 /g than the corresponding solid epoxy composites with a value of 5.2 cm3 /g. Here, absorption is the primary mechanism of shielding. The presence of microcellular structure increased the absorbing ability of materials by 62.7–79.5%. An interesting alternative is to use microporous polymer networks MPNs [26].

CONCLUSION

The various studies of the last 20 years have shown that the combination of micrometric and nanometric elements, different geometries (form of particles, mats, long and short fibres) as well as the presence of air microcavities into the matrix of the composite are all contributing parameters that improve the shielding effectiveness and make the material LO. One may regret that, despite the large number of studies that have been done, there have been no systematic approaches to compare the disruptive elements of EMI radiation in order to draw up a precise and quantified inventory of their effectiveness. This is partly what guided us in the development of the VLO_tech project.■

REFERENCES

[1] A. Swayam, K. Ramanpreet - Stealth Technology and Counter Stealth Radars: A Review, International Journal of Engineering and Science, 3(12), 13 (2013)

[2] J. Blanco, E. J. García, R. Guzmán de Villoria, B. L. Wardle - Limiting mechanisms of mode I interlaminar toughening of composites reinforced with aligned carbon nanotubes, Journal of Composite Materials, 43, 825 (2009)

[3] R. D. Batten, F. H. Stillinger, S. Torquato - Classical desordered ground states: super-ideal gases and stealth and equi-luminous materials, Journal of Applied Physics, 104, 033504 (2008)

[4] H.L. Zhang, Y. Xia, J. G. Gai - Ultrathin active layer for transparent electromagnetic shielding window impact shielding system, ACS Omega, 3, 2765 (2018)

[5] A. Kolanowska, D. Janas, A. P. Herman, R. G. Jedrysiak, T. Gizewski, S. Boncel - From blackness to invisibility carbon nanotubes role in the attenuation of and shielding from radio waves for stealth technology, Carbon, 126, 1 (2018)

[6] J. Zhao, W. Luo, L. Qi, L. Yuan, G. Huang, Y. Huang, X. Weng - The high-temperature resistance properties of polysiloxane/al coatings with low infrared emissivity, Coatings, 8, 125 (2018)

[7] R. Guzman de Villoria, P. Hallander, L. Ydrefors, P. Nordin, B.L. Wardle - In-plane strength enhancement of laminated composites via aligned carbon nanotube interlaminar reinforcement, Composites Science and Technology, 133, 33 (2016)

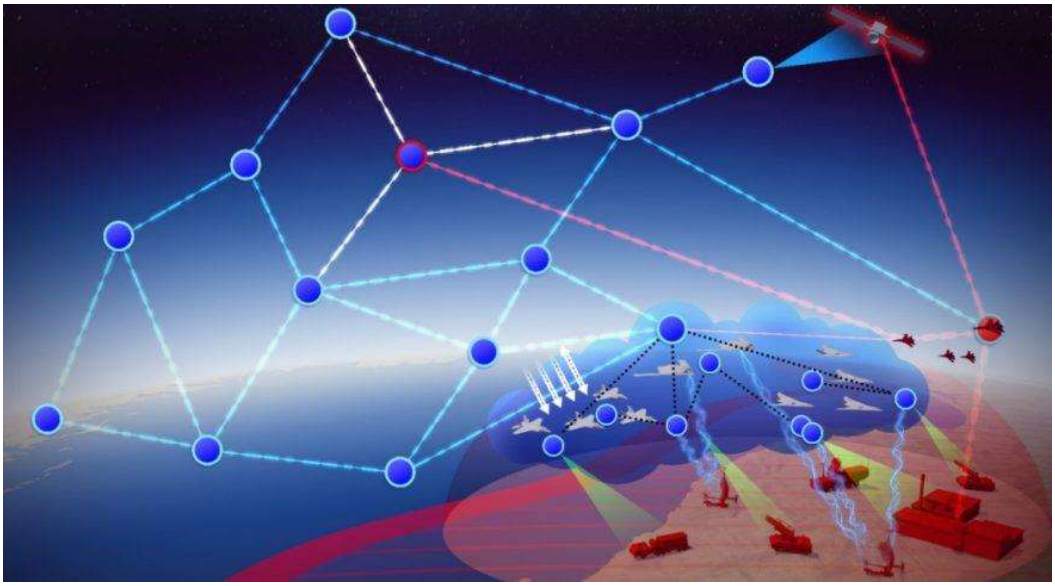
[8] J. Caro - Quo vadis, MOF?, Chemie Ingenieur Technik, 90. 10.1002/cite.20180003490 (2018)

[9] Konstantinos Zikidis, Alexios Skondras, Charisios Tokas. Low Observable Principles, Stealth Aircraft and Anti-Stealth Technologies, Journal of Computations & Modelling, vol.4, no.1, 2014, 129-165 ISSN: 1792-7625 (print), 1792-8850 (online) Scienpress Ltd, 2014

[10] Marc J.M. Abadie and Sozon A. Leventopoulos. Very low observable technology nano-composite systems based on supramolecular and polymer chemistry VLO_tech. Open call "Research and Innovation actions" New Horizo 2020 by European Union (2020)

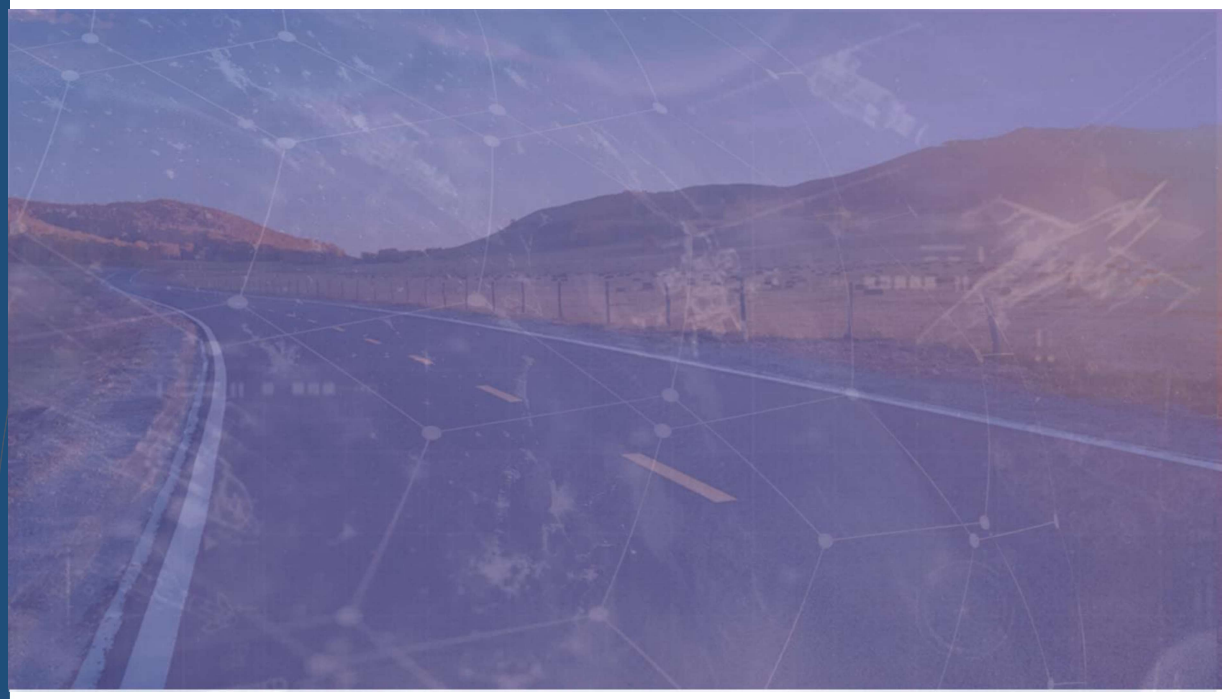
How space can help facilitate our work regarding IAMD

By LtC John PATRICK US (AF)
Director NATO Space Center Ramstein



In December of 2019, NATO declared Space an operational domain, recognising its importance in keeping us safe and tackling security challenges, while upholding international law. By declaring Space an operational domain Space is now on par with Air, Land, Sea and Cyber domains. Both military and commercial systems rely heavily on Space systems to conduct daily operations and are interwoven into the daily lives of more than 1 billion individuals that NATO is charged to protect and defend. However, Space is ever increasingly contested and congested which requires a suite of functions and services that are necessary to ensure unfettered access and use of Space. In order to protect and defend the Space domain, it is necessary to incorporate space systems and service in all operations and activities from planning to execution. While NATO is not striving to be an independent Space actor, the services provided across the space spectrum are critical dependencies that require attention.

How New Technologies Can Improve IAMD



By Cpt Emmanouil MAVROGIANNAKIS (GRC AF)

IAMD CoE SME

INTRODUCTION

NATO faces the most complex security environment since the end of the Cold War. Emerging technologies and innovations are rapidly changing the world around us, bringing new opportunities. Defense innovation has been critical to NATO's technological edge, deterrence and defense posture against multiple threats. Technological progress in artificial intelligence (AI) and machine learning, advanced robotics, biotechnologies and human enhancement, quantum technologies, big-data analytics, and fifth-generation telecommunication systems, as well as growing autonomy in the critical functions of military systems, promise to change how wars are fought, how fast, where, and by whom.

NATO IAMD missions vary depending on the specific circumstances of any concrete situation and can include Air Policing, Air Defense, Ballistic Missile Defense, Cruise Missile Defense, Counter Rockets, Mortar and Artillery, or Counter Unmanned Aircraft Systems.

The word 'integrated' indicates the technical and operational collaboration between systems of different military branches or even various Armed Forces to provide a robust and layered defensive architecture.

Modern and Smart Integrated Air and Missile Defense (IAMD) is built on an architecture including multi type of RADARs, fire control command centers, missile launchers and Multilayered, Multidomain Command and Control systems (M2C2).

Creation of a single integrated picture (SIP) can increase the defended area, can provide flexibility and can achieve three hundred sixty degrees coverage by reducing the possibility of undetected threats and protect more effectively the Air Space. This will be accomplished by using data generated by multiple sensors and broadcast via a sophisticated logistical information distribution system.

THREATS

In peace time there are two types of missions for NATO's IAMD: NATO Air Policing (AP) and NATO Ballistic Missile Defence (BMD). But IAMD mission can also vary depending on the circumstances of any concrete situation and can include Air Policing (AP), Air Defence (AD), Ballistic Missile Defence (BMD), Cruise Missile Defence (CMD), Counter Rockets, Mortar and Artillery (C-RAM) or Counter Unmanned Aircraft Systems (C-UAS). Most of these missions refers to threats which are:

- Cruise missiles
- Ballistic missiles
- Fixed –Rotary wings vehicles and
- Hypersonic vehicles.

CRUISE MISSILES

Cruise Missiles, missiles whose primary mission is to place an ordnance on a pre-determined target with continuous propulsion until the time of impact. They remain in the atmosphere and flies the major portion of its flight path at subsonic, supersonic, or hypersonic speeds. Modern cruise missiles are capable of self-navigating, flying at trajectory, these threat profiles result in late detection and shorter kill – chains due to the terrain masking and surface skimming tactics. They are also able to fly on non – ballistic trajectory.

Strom Shadow/ SCALP EG

BALLISTIC MISSILES

Ballistic Missiles are a type of missile that flies on a ballistic route to reach its pre-determined target. Ballistic Missiles are generally guided for a very short period of time or unguided. Ballistic Missiles fly unpowered in most of its total flight time and their trajectory is governed by gravity and air resistance. Ballistic missiles can be categorized by their range as Short – range Ballistic missile (SRBM) with Range between 300 to 1,000 kilometers (190 to 620 mi),

Iskander: The Russian Ballistic Missile

Medium – Range Ballistic Missiles (MRBM) with Range between 1,000 to 3,500 kilometers (620 to 2,170 mi), INTERMEDIATE – RANGE Ballistic Missiles (IRBMs) with Range between 3,500 to 5,500 kilometers (2,200 to 3,400 mi) and Intercontinental Ballistic Missile (ICBM) with Range greater than 5,500 kilometers (3,400 mi).

FIXED – ROTARY WINGS

Since World War I when the first military airplane was used, many developments have been done. Fixed

– rotary wings Vehicles like fighters, helicopters and many other have been developed and flew in the skies but always they need a pilot or a flight crew. However latest technology improvements gave IAMD a new threat to deal with, Unmanned Aerial Vehicles, which usually means an unmanned airborne platform and the equipment to control it remotely.

MANNED

Manned aircraft can be separated in two categories: these with Normal RADAR CROSS SECTION (RCS) and these with LOW RADAR CROSS SECTION (RCS). Low RCS aircraft is a challenging threat to IAMD because of the ways that they have, to reduce the aircraft's reflectivity to RADAR waves by burying the engines, eliminating sharp corners and diverting any reflections away from the RADAR sets of opposing forces.

UNMANNED AERIAL SYSTEM (UAS)

Unmanned Aerial System (UAS) usually means an unmanned airborne platform and the equipment to control it remotely. However, recent technological advances mean that some UAS can now operate autonomously without the need for human control/intervention during flight. Many of the smaller UAS threat systems employed are low-cost platforms that can be readily configured into swarm configurations to challenge IAMD surveillance system. The large variety of UASs can be classified according to several characteristics like role, range, weight, endurance, maximum altitude, wing loading, engine type etc.

NATO has classified the UAS in three classes:

- Class I which include UAS smaller than 150kg, which can also separated in small, mini and micro
- Class II which include UAS between 150 and 600kg which are tactical UAS
- Class III which include UAS bigger than 600kg which can also classified as Medium Altitude Long Endurance, high Altitude long endurance and STRIKE or Combat UAS

HYPERSONIC VEHICLES

Last years the threat set has been augmented with a new class: hypersonic vehicles. This new class of threat combines the advantages of Ballistic Missiles and Cruise Missiles in terms of high speed and manoeuvrability, presenting challenges for the current integrated air and missile defence (IAMD). There are three types of hypersonic threat:

- Hypersonic Glide Vehicles (HGVs) and
- Hypersonic Cruise Missiles (HCMs)

The new, emerging hypersonic threats offer challenges to IAMD:

- because of their ability to perform manoeuvre and atmospheric 'skipping' which makes point of impact prediction extremely difficult.
- Their high speed will greatly shorten reaction and engagement timelines, reducing range at engagement.
- Their ability to carry CBRNE warheads means that even if engaged, there may still be casualties as material continues on a ballistic trajectory.
- Their extensive range, coupled with high manoeuvrability, can be used to exploit the engagement capabilities of existing missile defence systems.

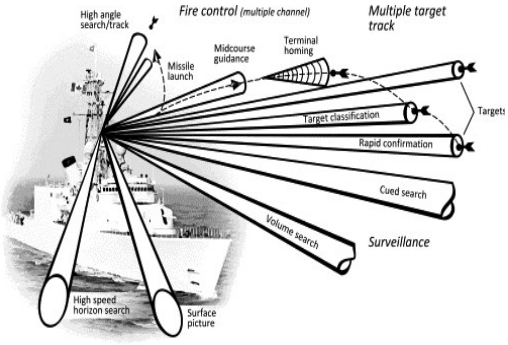
SENSORS

To defeat a threat first you have to detect it, for this reason we use sensors. Sensors which can be separated due to their function or characteristics as:
Multifunction RADAR
Airborne RADAR
Over the Horizon (OTH) RADAR
Cooperative RADARs
Early Warning Sensors
EO/IR Sensors
Passive RADARs
Passive Electronic Support Measure Trackers

MULTIFUNCTION RADAR

Multifunction RADARs (MFCR) are 3D RADARs based on active arrays (AESA) for land and naval applications. The choice of the RADAR band for MFR is typically related to the RADAR main mission requirements and industrial technology. Typical main functions performed by MFCRs are:

- Surveillance Air, Surface (or detection)
- Tracking
- Internal threat evaluation
- Dedicated tracking of Track while scan
- Track on Jammer
- Firing support
- Dedicated tracking for active missile guide
- Uplink for own missile guidance



Multiple functions of ship-borne radar systems

The main characteristic of the MFR is the capability to dynamically program the activities to be carried out to optimally adapt to different operational situations. In other words, the key concept of MFRs consists of their adaptive management in allocating in real time the RADAR time budget to the different activities, according to a ranking of priorities.

AIRBORNE RADAR

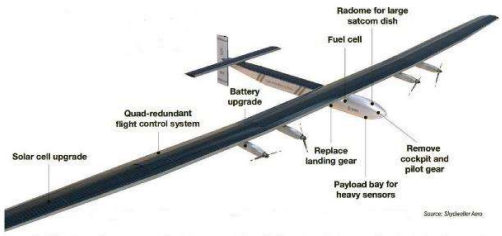
Each air platform is able to carry a RADAR. The purpose of the RADARs and their capabilities are heavily dependent on the platform and its mission.

Airborne early warning RADARs are typically combined with command & control functions. The RADARs are long range surveillance systems. The RADAR systems are able to detect small aerial targets at long distances and can track many targets simultaneously. Often, these systems also have a maritime mode, which can detect ships or smaller boats on the surface of the ocean.

Fighter aircraft typically carry a multi-function RADAR within their noses. The nose RADARs are multifunction RADARs with a large number of modes. These modes include a number of air-to-air and air-to-ground modes. In air-to-air modes the RADAR can search a sector or volume for other aircraft, track dedicated aircraft with higher precision, generate fire control data for own weapons or guide own missiles to their targets. It can also be used for non-cooperative target recognition by producing range profiles of unidentified targets. In air-to-ground modes, the RADAR searches for targets on the ground, either for ships on the water, or ground moving vehicles.

All **UAVs** can carry a type of sensor large one can carry and provide sufficient power to operate a RADAR system, other can carry some kind of camera either optical or infrared. Some of them can also carry alternative sensors like systems for signal intelligence.

As Airborne Early Warning RADARs, **Elevated Sensors,** are aerostats which are used to elevate the RADAR and mitigate the geographical obstacles problem which cause the low detection of threats. These aerostats are powered via the cable that holds them in place which used also to communicate and exchange data with ground station. Technological advancements have led to increasingly affordable space capabilities. **SPACE BASED SENSORs** have contributions based on their electro-optic frequency and orbits. These sensors can provide key capabilities in the areas of missile warning, missile defence and battlespace characterization via satellites in geosynchronous Earth orbit (GEO) and sensors hosted on satellites in highly elliptical orbit (HEO).



High Altitude Pseudo Satellite Diagram

OVER THE HORIZON (OTH) RADARS

Over the Horizon (OTH) RADARs are in use or are being development by various nations and with long range coverage of over 3000km. There are two different types of OTH RADAR, **sky wave** which can generally see 1000 ± 3000km but there are highly dependent on ionospheric conditions and **surface wave** which typically detects out to a few hundred km, but only works over the sea surface as it needs a somewhat conductive surface for the propagation to be supported. These types of RADAR can detect both air and surface targets. Ballistic missiles and STEALTH vehicles are easily detected at HF frequencies.

COOPERATIVE RADAR

A Cooperative RADAR is a closed network of RADAR transmitters and/or receivers that operate cooperatively and act as a single sensor system. There are three types of Cooperative RADARs as follow:

Multiple Input Multiple Output RADAR which by its origins is fundamentally an antenna technique that extends the concept of a multichannel receive antenna or phased array to a multichannel transmit aperture. The distinguishing feature of a MIMO system is that it is intentionally designed to produce a spatially and temporally varying antenna pattern. This is typically accomplished by exciting a multiport, multiaperture antenna with a waveform or temporal response that varies among the antenna inputs. In this way, the MIMO RADAR system imparts a spatial encoding of a scene which, under the right conditions, can be decoded and exploited to improve both target detection and location performance. In some sense,

MIMO RADARs are a generalization of multistatic RADAR concepts.

Multistatic RADARs are to use emitters and receivers placed at different geographical locations. The RADAR emitters and RADAR receivers are synchronized: The receivers get complete information about the patterns and waveforms radiated by the emitters.

Distributed Coherent Aperture RADAR (DCAR) can be seen as an application of the multistatic RADAR concept. The goal is to achieve the same performances of a bigger aperture RADAR by the collaboration of smaller aperture systems. This is especially important in today's ballistic missile defence environment.

EARLY WARNING SENSOR

An **early-warning sensor** is any system used primarily for the long-range detection of threats. EW RADARs tend to share a number of design features that improve their performance in the role. For instance, EW RADAR typically operates at lower frequencies, and thus longer wavelengths, than other types of sensors. This greatly reduces their interaction with rain and snow in the air, and therefore improves their performance in the long-range role where their coverage area will often include precipitation.

ELECTRO-OPTICAL (EO)/ INFRARED (IR) SENSORS

Electro-Optical (EO) systems use part of the electromagnetic spectrum to perform their measurements. This includes the visible spectrum and Near InfraRed. They are sometimes referred as "TV" channels because they produce images with natural colors familiar to the human eye.

InfraRed (IR) sensors use the infrared part of the electromagnetic spectrum to produce an image or video of a scene. InfraRed (IR) sensors can be divided in 4 classes with each its sensing strengths and weaknesses as follows:

- Long wavelength IR (LWIR)
- Mid wavelength IR (MWIR)
- Short wavelength IR (SWIR)
- Visible and Near-IR (NIR)

Military sensors for air target detection generally use the long wavelength IR (LWIR) and especially the Mid wavelength IR (MWIR) band, which offers the best compromise for target detection against ground or air background.

EO/ IR sensors in military systems include the following types:

- Forward Looking Sensor
- Panoramic Sensor Heads
- Rotating Sensors Heads
- Staring Sensors Heads

PASSIVE RADARS

Passive RADARs or Passive Coherent Location (PCL) systems detect and track objects by processing the reflections of signals generated by external transmitters -so called transmitters of opportunity. Passive RADARs are like multi-static RADAR. The difference is that passive RADARs do not have organic transmitters that are optimized for RADAR purposes, and they have a special architecture to process waveforms emitted from different transmitters of opportunity.

PASSIVE ESM (ELECTRONIC SUPPORT MEASURE) TRACKERS

Passive ESM (Electronic Support Measure) Trackers or Passive Emitter Tracker (PET) Systems receive and process emissions from RADAR, IFF, navigation, communications, jamming signals on the target platforms, to detect and track them. These systems operate in 2D but can obtain the range information via multi-Iteration. ESM systems enable covert operation since they are passive systems. They can be used with the purpose of early warning and can detect earlier than a RADAR does. Moreover, they can perform better than a RADAR, at detection of difficult targets such as tangential moving or low-RCS objects. They can perform classification and identification when used with a good threat database. They can also provide detection information for Kill-Assessment.

INTEGRATION

Different systems provide different data. To overcome this, we must find a common language between them, this is integration and we can gain it with **Tactical Data Links (TDL)** and **Alternative Tactical Data Links (ALTDL)**

TACTICAL DATA LINKS (TDL)

There are several Tactical data links which help up to communicate and exchange of data. These are:

Link-1 is a low capacity, full duplex, point-to-point digital data link with automatic exchange of track and strobe data combined with link and data management messages. Link-1 mainly provides for the exchange of air surveillance data. It is not crypto secure and has limited to air surveillance and link management data.

Link-11, is a half-duplex relatively slow data link which is primarily used as a Maritime Data Link. It supports the exchange of air, surface and subsurface tracks, EW data and limited command data among C2 units.

Link-11B, is a point-to-point version of Link-11 which is typically used to disseminate a track picture between ground units in the same way as Link-1. Data is exchanged over a fully automatic, phase-continuous, full-duplex.

Link-16 is an improved tactical information digital data link used to exchange near real time information by using a specific message catalogue. Link-16 was developed as a modernization, upgrade to Link-11 and Link-11B. The main function of Link-16 is the exchange of real-time tactical data amongst military units, similar to Link-11 and Link-11B, but Link-16 also provides significant improvements, such as nodeless operation, jam resistance, flexibility of communications, separate transmission and data security, increased number of participants than the present tactical networks, increased data capacity, network navigation features and secure voice. Link-16 has been designed for all services (air, surface and land) and for all platform types.

Link-22, is a Data Link system that is designed to interconnect ships, submarines, aircraft and ground-based tactical data systems for the transmission of Command and Control Information in real-time. Link-22 has been designed to be compatible with Link-16 and a high compatibility between both systems will enhance Allied Interoperability and improve a Commander's situational awareness

ALTERNATIVE TACTICAL DATA LINKS (ALTDL)

Apart from Tactical DATA links there are in use by nations some other ways to build integration between systems known as **alternative tactical data links**, these can be separated in categories as:

- **ALTDLs Within the IP Networking Data Links Group** such as **Tactical Targeting Network Technology (TTNT)** which is used by US military to providing real-time information to quickly target moving and time-critical targets.
- **ALTDLs Within the Battlefield Support Data Links Group** such us **Situational Awareness Data Link (SADL)** which is used by ground forces and their air brigades for use in Close Air Support missions.
- **ALTDLs Within the Commercial/Civilian Data Links Group** such as **5G** with its high speed and high capacity characteristic can exchange real time data.
- **ALTDLs Within the Tactical Data links Group** such us **Joint Range Extension Application Protocol (JREAP)** which can provide satellite communications and data exchange.
- **Other ALTDLs Under Consideration ASTERIX** like **MADL (Multifunction Advanced Data Link)** which is currently in use on board the F-35 and has been designed as a Low Probability of Intercept (LPI) Data Link and enables the aircraft to communicate within and between flights in order to share a common view of the battle space
- **ALTDLs Within the ISR Data Links Group** such as **Digital Video Broadcast – Satellite (DVB – S)** which is the European military's interoperability standard for imagery and signal intelligence

IMPROVED SITUATIONAL AWARENESS

"Situational Awareness" (SA) is defined as being the quantity of operable information related to a situation in a given physical area and in a limited timeframe and has been recognized as a critical foundation for successful decision-making across a broad range of situations. It is therefore essential to know the operational situation with the greatest possible precision and anticipation of potential or real threats, both in an operational theatre and in a territory. To do this, sensor systems must make it possible to detect as early as possible the departure of threats and their characteristics.

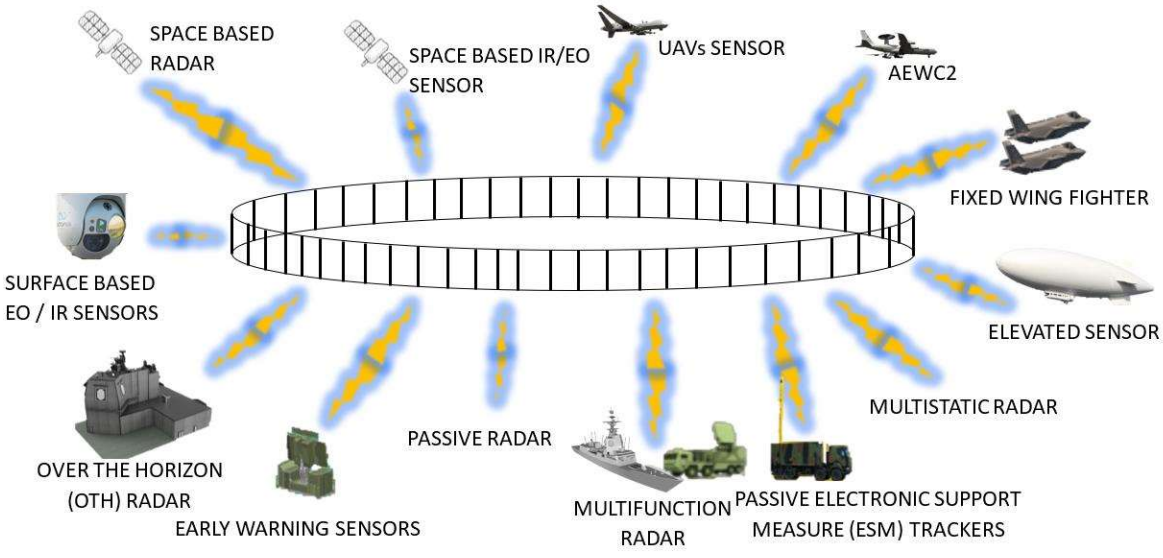
It is the early warning system which must provide early knowledge of threats, their origin and tracking them. To enhance surveillance sensors should be based on faster communication links allowing faster exchanges with faster refreshment rate. The combination and the corporation of sensors which are part of the early warning system can provide the maximum efficient result.

We can achieve very early detection and tracking capacity with space-based sensors with their electro-optic frequency and orbits. **Geo-stationary Orbit (GEO) Infrared satellites** enable detection of ballistic missiles, maneuvering tactical ballistic missiles and hypersonic glide vehicles during boost phase. **Low Earth Orbit (LEO) satellites**, depending upon their orbital inclination, can provide boost-phase and post boost-phase Infrared detection and tracking against the earth limb and cold space background. LEO satellites contribute to the detection and tracking of ballistic missiles, tactical ballistic missiles, and high-altitude glide vehicles. **High altitude UAVs or High-Altitude Pseudo Satellites** can also use their Infrared and sensing capabilities to detect and track threats. With their long endurance, these UAV's can monitor large areas of the ground for larger objects. including vehicles. **Airborne IR and RADAR** systems can be used both to early warning and track high velocity cruise

missile and low flying cruise missiles. This airborne RADAR and IR sensors can be networked for simultaneous ground, surface and air networked engagement, mixing IR data and RADAR data and surface-based RADARs. **Fighter's aircraft** multi-function RADAR can search a sector or volume for other aircraft, track dedicated aircraft with higher precision. It can also be used for non-cooperative target recognition by producing range profiles of unidentified targets. In air-to-ground modes, the RADAR searches for targets on the ground, either for ships on the water, or ground moving vehicles. Some RADARs also have further modes dedicated to electronic warfare or data transmission. It is possibly to switch rapidly between these modes. **Over The Horizon (OTH) RADAR** can detect aircraft and missile targets in distance over that 3000km. HF has good anti-stealth capabilities. Most types of targets can be detected, both air and surface. **Elevated Sensors** are aerostats with RADARs which can used for targets searching or to provide fire control data to an interceptor system. The main threat category addressed by this system are low-flying cruise missiles. The aerostats are powered via the cable that holds them in place and provide data communication to the ground station. **Early Warning Sensors** used for surveillance purposes due to their long distance that they can detect air threats. The sensor network that can best utilize Early Warning Sensor will have the best chance of surviving, but also to be the most effective. **Multifunction RADARs** can dynamically program the activities to be carried out (sector by sector) to optimally adapt to different operational situations. They can be used for surveillance or tracking purposes. They have better detection of stealth targets, Silent receivers, Lightweight receivers. **Surface based Electro-Optical (EO), Infrared (IR) and Radio Frequency (RF) sensors**, include sensors on ground and sea platforms. The benefits of use EO sensors is a considerable range of applications, to include masking, jamming, early detection of hypersonic missiles, identification and tracking under stressed and saturating conditions and identification**. Multistatic RADARs** can be also used to add protection of specific assets to increase resistance of specific sensitive assets against stealth and jamming when combined with MFR RADARs, Multistatic RADAR could be of interest to track hypersonic missiles and highly maneuvering threat if combined with a non-directive long range transmitter. **Passive sensors, and Passive Electronic Surveillance Measures (ESM) trackers**; can support active sensors against jammers, Detection of target, Surveillance and Early warning.

All these systems in a sophisticated network can help us to obtain a single Integrated air picture. Which means:

- Improved Accuracy and Range
- Better Track Quality
- Less Gaps in single Integrated Air Picture
- Better Threat Evaluation/Classification
- Better detectability of the stealth targets
- Resilience on saturation due to task splitting between several RADARs instead of letting them proceed to the same tasks on the same threat.
- Sensor Networks are less sensitive to sophisticated electronic countermeasures
- Kill assessment is improved
- The job of target decision algorithms of the ARMs is harder because of the smart- sharing of the illumination time between the RADARs
- Inclusion of Electromagnetic Attack capabilities coordinated with other sensors can reduce the capacity to accomplish it mission to attackers.■




1st ANNUAL CONFERENCE
INTEGRATED AIR & MISSILE DEFENCE
ACT KNOWING
CENTRE OF EXCELLENCE
Integrated Air & Missile Defence:
Challenges and Threats,
Developments and Opportunities
in a Rapidly Changing Environment
Chania/Crete
29 - 30 Sep 2022

INTEGRATED AIR & MISSILE DEFENCE
CENTRE OF EXCELLENCE
Souda Air Base, Chania, Greece
https://iamd-coe.org/

Follow us on: