Transforming Joint Air and Space Power

The Journal of the JAPCC

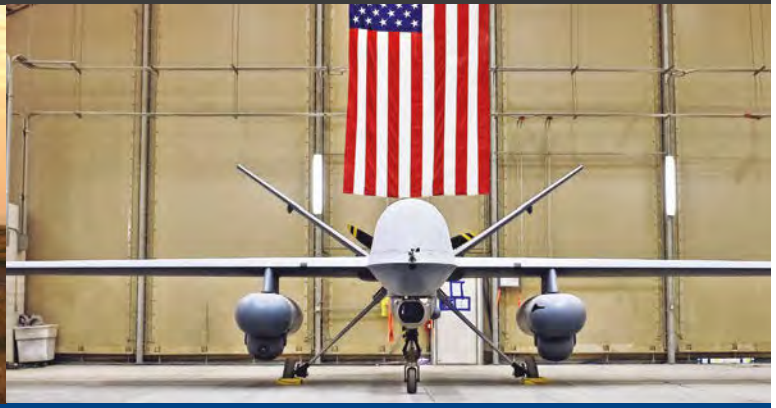
Edition 28, Spring/Summer 2019

SPEED. INNOVATION. PERFORMANCE.

Tasking, Collection, Processing, Exploitation & Dissemination System

Sierra Nevada Corporation (SNC) is a trusted leader in solving the world's toughest challenges through advanced engineering technologies in Space Systems, Commercial Solutions, Defense and National Security.

- Integrated Communications Vehicle (ICV)
- A-29 Super Tucano
- PC-12
- C-130H/J
- Dornier 328
- MQ-9 Reaper (Gorgon Stare System)
- M-28 Sky Truck



snc®

sncorp.com

As the Assistant Director of the JAPCC, it gives me great pleasure to introduce the 28th Edition of the 'Journal of the JAPCC' and congratulate authors for their most valuable contributions on Joint Air & Space Power.

I would like to start by providing a warm welcome to our new JAPCC Director, General Jeffrey L. Harrigian, who joins us from Ramstein AB, Germany and his previous position as Deputy Commander, US Air Forces in Europe – Air Forces Africa.

We have a variety of articles in this edition that will whet your appetite and we start off with an interview with the Romanian Air Chief Major General Pană, who offers us great insights into the changes of the past 15 years, since the Romanian Air Force joined NATO and the challenges lying ahead with the rapidly shifting and evolving requirements for a successful and reputable Air Force.

I am particularly grateful to The Commander of Italian Army Aviation, General Riccó, who provides answers and insight into the future of helicopters, the different kind of threats his personnel must be prepared to meet, how to improve the effectiveness of air-land integration and a 20-year outlook for Army Aviation.

The article 'Cyberspace NOTAM!' discusses the urgency of NATO's Vision and Strategy on the Cyberspace Domain. 'Is NATO Ready for Galileo?' takes us to the space domain and highlights the possibilities, capabilities and challenges of combining GPS and Galileo to improve the overall resiliency. 'Precision-Guided Munitions of the Future' provides an outlook on evolving demands and related developments in the area of future weapons, mentioning possible weak spots and requirements for successful integration. The two following articles 'Improving NATO Air Training' and 'Iniochos' provide different angles on Tactical Air Training. Whilst one presents a prospect of the Future Tactical Air Training, the other one gives an insight into the largest military exercise in Greece for NATO Allies and Partner Nations. Future and current challenges regarding IAMD training and interoperability are discussed in 'How can Modelling and Simulation Support Integrated Air and Missile Defence?' and 'Improving Ballistic Missile Defence Interoperability'.

Our final article in this Journal 'Command and Control in Digital Transformation' comes from an external industrial expert who introduces the command post of the future considering current and future technological developments.

I do hope you enjoy reading this issue and encourage you to provide feedback. We welcome discussion about our articles, and also contributions to future editions if you have an Air and Space Power issue about which you are motivated to write! Should you wish to contact us directly, please visit our website www.japcc.org, like us on LinkedIn or Facebook, follow us on Twitter, or simply send us an e-mail to contact@japcc.org and provide us with your input to help foster and further the debate on the Transformation of Joint Air & Space Power.

Ciao and enjoy!

Giuseppe Sgamba
Brigadier General, ITA AF
Assistant Director, JAPCC

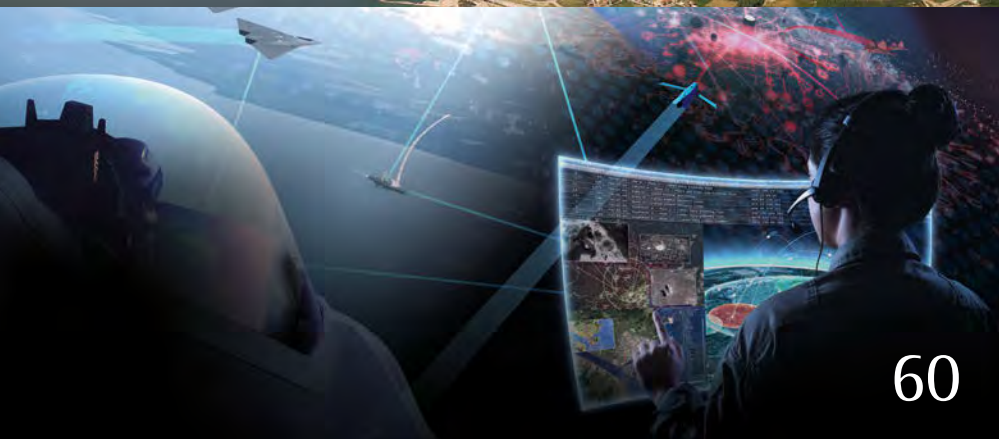
The Journal of the JAPCC welcomes unsolicited manuscripts.
Please e-mail submissions to: contact@japcc.org

We encourage comments on the articles in order to promote discussion concerning Air and Space Power.

Current and past JAPCC Journal issues can be downloaded from www.japcc.org/journals

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

Table of Contents



Inside the JAPCC

Book Reviews

Imprint:

Transforming Joint Air Power:
The Journal of the JAPCC

Director
Joint Air Power Competence Centre
Gen Jeffrey L. Harrigian

Executive Director
Joint Air Power Competence Centre
Lt Gen Klaus Habersetzer

Editor
Brig Gen Giuseppe Sgamba

Assistant Editor
Lt Col Daniel Wagner

Production Manager/
Advertising Manager
Mr Simon J. Ingram

Editorial Review Team
Col Brad Bredenkamp
Lt Col André Haider
Lt Col Panagiotis Stathopoulos
Mr Adam T. Jux

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

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

Follow us on Social Media

The Romanian Air Force – 15 Years in NATO

Interview with Major General Viorel Pană, Chief of the Romanian Air Force Staff

Where does the Romanian Air Force (ROU AF) stand after fifteen years membership of the North Atlantic Alliance?

To start with, I would like to stress that it is a great privilege for me to provide the readers with an overview of the current missions and challenges of the ROU AF and I want to highlight the efforts of the entire ROU AF personnel to fulfil their responsibilities, as we are now witnessing an unprecedentedly complex international security environment.

We face hybrid, conventional and asymmetric threats, combined and intertwined from the Baltic Sea to the Black Sea, from the North Atlantic to the Mediterranean, and from non-state actors or failed states. This requires constant and profound growth within the ROU AF to meet the new challenges confronting NATO. The ROU AF has adopted a dynamic approach to meet the modernization requirements and to integrate them into NATO.

We started the transformation process that touched upon all aspects of our Air Force and intended to transform our capabilities and to fulfil our missions while experiencing budget pressure for many years.

We implemented the first two stages of the transformation process; the main downsizing stage (2003–2007) and the NATO and European Union (EU) operational integration phase (2008–2015). Excellent progress was made towards generating an agile and adaptable force structure, which is more suited to today's security environment. This process is to be finalized in 2025 and translates into a full integration into NATO and EU.

The ROU AF has come a long way since 2002, when we deployed a C-130 aircraft to Afghanistan in support of the coalition effort. In 2005, we deployed four IAR-330 SOCAT helicopters into Bosnia for one year and the following year, for the first time, Romania became the lead nation of the Kabul Afghanistan International Airport (KAIA) for four months. In 2007 we deployed four MiG-21 LanceR aircraft to Lithuania to secure the Baltic Nations' airspace while performing the Air Policing mission and in 2008 we secured the NATO Summit in Bucharest together with our US allies. In April 2011 we took over once more the KAIA lead nation mission, this time for a full year.

But first and foremost changing the mindset of ROU AF personnel was critical, because of the implications on all the other aspects that come along with an Alliance membership; common doctrine, interoperability, increased role specialization, participating in multinational exercises and in coalition operations.

What does the Roadmap for the Transformation of the ROU AF look like?

Transforming the Air Force has been done to accomplish the following objectives: achieve NATO's and EU's commitments; upgrade to new Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) systems and Force Structure, add new logistics support structures, and modernize acquisition programmes.

Our main goals are to develop our Air Force to be capable of performing a broad spectrum of tasks such as transport, Search


VIOREL PANĂ

© ROU AF

and Rescue (SAR), Non-Combatant Evacuation Operations (NEO), air traffic management, reconnaissance, and most importantly protection of Romania's airspace within NATO Integrated Air and Missile Defence System (NATINAMDS).

Some of the acquisitions have been planned for quite a while, but in 2016 after the *'Romanian Armed Forces' procurement program for 2017–2026 timeframe'* was approved by the Homeland Defence Supreme Council, the situation changed and we were content to include those new assets foreseen to be a part of our inventory.

Today, at the core of the ROU AF are our fighters, helicopters, transport aircraft, the Air C2 system, radars and missiles.

We will continue to increase our operational capability through the multirole fighter aircraft procurement programme, projected to achieve a final operational air capability represented by three multirole fighter squadrons equipped with 5th generation F-35 Lightning II Joint Strike Fighters (JSF), through a transition period covered by three F-16 squadrons. To date, in the first phase of the programme, we have acquired twelve F-16 Mid-Life Upgrade (MLU) aircraft from the Government of the Republic of Portugal, we have trained our pilots and technicians, and the first squadron was declared operational last summer and is ready to execute Air Policing missions. There are ongoing activities to continue the programme, to train additional personnel and at the same time to facilitate our national defence industry involvement to be prepared to perform maintenance and logistic services for our F-16 fleet.

We started the programme to upgrade the IAR-99 Şoim aircraft to an advanced training platform. Now that we have the multirole F-16 aircraft in our inventory, the IAR-99 requires a reconfiguring of the avionics and flight control systems to transition pilots through to the F-16. This programme targets to upgrade 21 IAR-99 Şoim aircraft with a new configuration of the IAR-99 Super Şoim platform aiming to increase reliability of the on-board installations and systems and to extend the aircraft lifecycle. This upgrading programme will involve the national industry capabilities.

We have enough Air Transport aircraft to sustain our Army and the Navy operations. The four C-130 Hercules aircraft established our airlift capability, which has been further improved by the procurement of seven C-27J Spartan aircraft in the past years.

The ROU AF operates Puma SOCAT attack helicopters, Puma transport, Medical Evacuation (MEDEVAC) and SAR helicopters and recently we started an upgrade programme for our IAR-330L helicopters. Our aim is to modernize twelve helicopters to have the updated platform available for peace-time missions on national territory, to support the central and local authorities in case of emergency situations, and to participate in

United Nations (UN) peacekeeping missions as a part of Romania's commitment. We are currently in the first stage of the programme where seven helicopters are modernized and we will start the second stage for modernizing the remaining five as soon as the *'Helicopters procurement and endowment conception for the Romanian Armed Forces'* is approved.

Another important major acquisition programme was triggered when the decision was made to procure the long-range surface-to-air PATRIOT missile systems. The aim of this programme is to equip the Air and Land Forces with seven PATRIOT missile systems, to include the missiles, the C2 elements, the initial logistic support and personnel training, in order to defend the national airspace and the vital and strategic military and civilian critical assets. The first four systems are expected to be delivered by the end of 2022. Moreover the Short Range Air Defence/Very Short Range Air Defence (SHORAD/VSHORAD) integrated weapon systems are considered to be purchased as Romania is determined to implement the Integrated Air and Missile Defence (IAMD) concept.

The radar units utilize several types of digital radar stations such as Fixed Radar Surveillance 117 (FPS 117), Transportable Radar Surveillance 79 (TPS-79) Gap Filler and TPS-77. Our aim is to establish a reliable and sustainable C4ISR system.

What do you see as your priorities in meeting the modernization challenges in the ROU AF?

For this year we intend to fully integrate and exploit the F-16 starting with the execution of Air Policing mission and to train our aircrews as well as the maintenance, planning, operations and logistics officers and Non-Commissioned Officers (NCOs) who will be deployed alongside four IAR-330L helicopters in less than four months in Mali. In two to three years, we want to train and educate our men and women to strengthen our Air Defence posture when the Patriot systems will enter service.

I have already mentioned the human resource as an essential factor and I want to provide, as one of my top priorities, well trained and equipped airmen and women for the future challenges. With this in mind, officers, NCOs, airmen and civilian employees undergo a comprehensive training program throughout their careers. We are continually reviewing the training methodology and the syllabus to enhance situational awareness, leverage knowledge and, at the end of the day, to have the right airmen taking the right decisions, to execute a mission in the most effective manner.

Since March 2018 the C-27J Spartan Detachment is the first NATO airlift detachment to finish the Tactical Evaluation (TACEVAL) programme and is able to accomplish its mission according to Alliance's standards, as it went through a successful Capability Evaluation-type check-up by the TACEVAL/AIRCOM Ramstein Division. Our C-27J Advanced Training and Maintenance Facility has offered reoccurring currency training for

the Hellenic Air Force's specialists and there are ongoing discussions and negotiations to start training specialized personnel from Lithuania, Bulgaria and even the Peruvian Air Forces, as our intention is to transform it into a regional C-27J training hub in South Eastern Europe.

The MiG-21 LanceR was the workhorse of the ROU AF for decades, maintaining Quick Reaction Alert (QRA) to address potential airborne threats. This task will be taken over by the F-16, ensuring increased responsiveness and reactivity. There are different sorts of activities that prove our strong commitment to maximize this capability, to including the beginning of air-to-air refuelling missions. Our F-16's now participate in extensive and comprehensive training to increase interoperability with our allies, from a complex point of view; communications, flight procedures, and logistics, according to NATO standards.

PATRIOT missiles systems will shape a new architecture design for our Air Defence posture and will enhance our contribution to the Alliance to deter and defend NATO territory.

Closing Remarks

We need to keep pace with the new security environment and the asymmetrical challenges, intellectually and doctrinally, and our equipment needs to have the embedded flexibility to be capable of adapting to future demands.

In recognition of the changed security environment, the National Defence Strategy (NDS), published in 2015, included a specific commitment to meet NATO expectations. This specifically targets military modernization by allocating two percent of Romania's Gross Domestic Product (GDP) to defence spending starting from 2017 for a minimum of ten years. Such commitments are meant to sustain the aspiration that Romania is an important security provider in the region, not just a recipient.

The Enhanced Air Policing missions executed in partnership with the Royal Air Force and the Royal Canadian Air Force reinforced the cooperation and, at the same time, effectively contributed to the collective effort in managing the threats against Euro-Atlantic security.

Our agile and deployable force structure, supported by the ongoing modernization and procurement programmes will further strengthen our Air Force and the deterrence and defence posture of the Eastern flank of the Alliance.

To conclude, the ROU AF is effectively contributing to homeland security by safeguarding the national airspace. We will continue to upgrade and consolidate our combat capabilities with a view of defending our national and rule-of-law values and respecting the commitments made by our country at the international level to bolster regional and Alliance security.

Sir, thank you for your time and your comments.

Major General Viorel Pană

started his military career in 1989 as a fighter pilot on MiG-21 aircraft. In 1992 he became an airlift pilot on AN-24, and continuing with C-130 Hercules and C-27J Spartan. He is instructor pilot on C-130 Hercules and on C-27J Spartan. He has over 3,100 flying hours logged as an airlift pilot.

In 2014 he assumed command of the 90th Airlift Base. He was appointed as the acting Chief of the Romanian Air Force Staff on October 2017 and became the actual Air Chief at the beginning of 2018.

He was promoted to the rank of Major General on 1 December 2018.


© Comando Aviazione dell'Esercito

Mission and Vision of Italian Army Aviation

An Interview with General Paolo Riccò, Commander of Italian Army Aviation

By Lieutenant Colonel Livio Rossetti, ITA AA, JAPCC

Sir, thank you for taking the time to answer some questions and to provide an insight into Italian Army Aviation. Can you please describe the current posture of Italian Army Aviation?

Over the last thirty years, without interruption, Italian Army Aviation has been employed in missions abroad and has operated in a broad spectrum of geographic and climatic locations. Army Aviation has adapted to combat multidimensional threats which are very different from the threats they were originally trained to fight. Across the globe, the most significant missions have been in Bosnia and Kosovo in the European theatre, Somalia and Mozambique in the African theatre, Iraq and Lebanon in the Middle East and Afghanistan and East Timor in Asia. Thanks to the service's collective operational experience, it has been possible to develop and introduce a new family of weapon systems and aircraft into service. These systems and aircraft were designed from the ground up to allow Army Aviation greater flexibility and survivability. Army Aviation is an important operative enabler of the

Armed Forces and an amazing resource for the nation. Army Aviation is always ready and at the forefront of all operations conducted in both national and international territories. Italian Army Aviation emphasizes the concept of 'dual-use', meaning we are trained and equipped to handle the full spectrum of military operations as well as support to civil security for the population. Firefighting campaigns, emergency medical support and search and rescue are only a few of the tasks in which we are involved on a daily basis. Army Aviation is a modern force which operates technologically advanced equipment, in combined-force operations and international arenas. Army Aviation provides a host of capabilities, which generate security while supporting progress and prosperity at a national and international level. Our crews are multi-skilled with a remit to conduct transport (Air Movement, Tactical Transport and MEDical EVACuation [MEDEVAC]), Attack (Close Air Support, Close Combat Attack), direction and control of fire, Command, Control and Communication (C3) support, personnel recovery and Reconnaissance, Surveillance and Target Acquisition (RSTA). I can confidently state, that Italian Army Aviation today stands fully capable of conducting a wide spectrum of missions in any environment and weather condition, and is ready to fulfil the needs of Italy and the NATO Alliance.

In your opinion, will the tiltrotor-aircraft replace helicopters in the near future?

Tiltrotors carry similar-sized payloads to transport helicopters but fly much faster and with longer range. I believe they will be a possible alternative, but only for the replacement of utility/medium-lift helicopters. Most likely, in the near future, tiltrotors will enable a wide spectrum of transport like airborne, air movement and MEDEVAC missions. However, as far as combat helicopters are concerned, I believe the possible choices will only be between 'conventional' and 'coaxial rigid-rotor' helicopters. This is because combat helicopters need to be much more manoeuvrable, not only for air-to-air and air-to-ground combat but also to enable hovering; i.e. enabling masking and unmasking in crucial combat and target acquisition phases of flight. This is the reason why, coherently, we are now starting to develop a new eight-ton class attack helicopter, which will provide Italian Army Aviation with an increased technological advantage, greater performance and lower operating costs. This will meet the diverse mission requirements of future conflict for the next 30 years or more.

Considering a hypothetical near-peer enemy conflict, characterized by a lack of airspace supremacy and being affected by capable Electronic Warfare (EW), hybrid or cyberattack; is Italian Army Aviation ready for this? How would you prepare your personnel to meet these kinds of threats?

It is known that our potential peer adversaries have consistently invested in EW modernization across the electromagnetic (EM) spectrum. Moreover, they demonstrate a remarkable capability in hybrid and cyber environments and are ready to infiltrate, exploit and degrade access to our networks and data. So, of course, if I have to hypothesize a conflict and I must consider their capabilities to target our Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR), most likely with packages capable of inhibiting or degrading the use of our frequencies and operating systems. We must be fully prepared to fight in this environment. For this reason, Italian Army Aviation, following NATO's advice and instructions, is concentrating its EW efforts on two pillars: development and training. We are developing our ability to prevent, detect, defend against, and recover from a complex attack by working closely with military authorities, agencies and industry to keep our helicopters, and all the systems used by Army Aviation for storing, coordinating, and protecting information, updated and effective. To increase our level of training, we have been conducting a new training method called Complex Airmobile Exercise (CAEX). It is a Live Exercise/Field Training Exercise (LIVEX/FTX), which is held every year in two or three sessions at Brigade level. In these exercises, we include Opposing Forces (OPFOR) and reproduce typical operational contexts, which replicate the same operational stress that the crews may encounter when deployed. We

created an EW/cyber/hybrid scenario which forces crews to operate with minimized radio communications and without the use of Global Positioning System (GPS) signals, thereby forcing use of on-board backup systems like Doppler and the Air Data System (ADS) for navigation. Also, during planning phases with ground forces, they practice visual signals for coordinating fire support. This innovative and advanced training programme was conceived and developed to verify and validate techniques, tactics, operating procedures and standardization of different Italian Army assets through various aerial missions (e.g., Quick Reaction Force, Quick Reaction Action, Personnel Recovery, MEDEVAC, Air Assault). No country can face an EW/cyber/hybrid scenario threat alone. We are stronger when we work with our international partners. Consequently, we share intelligence, combine forces and coordinate responses to develop new, effective tools, technologies and strategies to make our organization resilient to cyber, hybrid and EW attacks. Ultimately, in my opinion, you cannot survive on the modern battlefield unless you are truly competitive in these areas.

How can Army Aviation develop and improve air-to-land integration?

Thanks to the ongoing Services Industry NATO-sponsored activities, such as the Joint Capabilities Group Vertical Lift (JCGVL) and the Study Group-227 Manned-Unmanned Teaming (NIAG SG-227 MUM-T), a new roadmap was developed for ATP-49G (operations). This is to address the requirements for high speed, long-range and extended-endurance Next Generation Rotorcraft (NGR) insertion, with high-autonomy Unmanned Aerial Systems (UAS). It is envisaged that these rotorcraft will operate in Restricted Operating Zones (ROZ), with both, manned aircraft or Optionally Piloted Vehicles (OPV) roles at all phases of operations. In the future, Army Aviation will operate over large areas of responsibility, providing combat and scout capabilities. With these newly-developed procedures, we will ensure the development and improvement of air/land integration. This will include a long-range data link capability, which will accelerate the ability to deliver timely C3 and intelligence information to all commanders at tactical, operational and strategic

levels. The air assault operational capabilities, first tested during the European Defence Agency (EDA) Exercise 'Italian Blade 2015', have been used as the basis to introduce new possible Manned Unmanned Teaming (MUM-T) capabilities in the Army Aviation operational segment. During this exercise, a Level of Interoperability (LOI) 3 capable Rotorcraft Unmanned Aerial System/Optionally Piloted Helicopter (RUAS/OPH) was integrated via Ground Control Station with Attack Helicopters (AHs), Utility Helicopters UHs and a ground Joint Terminal Attack Controller (JTAC). Besides doctrine, procedures and effectively incorporated training, a reasonably good level of integration requires at least the availability of effective Command and Control capabilities, improved situational awareness and reliable communication systems. To that end, we are sure that the right application of technology will play a key role in the future to closely connect air, sea and land portions of the battlefield and to allow crews and personnel to operate with maximum safety, reduced risk and higher levels of efficiency.

Where do you see Army Aviation in 20 years?

Army Aviation has to keep in mind that it has been, and absolutely will be in the future, a key enabler for Army and joint missions. It brings unique capabilities to fulfil mission requirements across the full spectrum of Army military operations. For example, the development of an integrated airmobile component in an Italian Army Aviation airmobile brigade gives flexibility, manoeuvrability and timely responsiveness to orders from the ground force Commander. Army Aviation has been, and will remain, the principal way to provide ground forces with fire, mobility, and intelligence capabilities. We must be prepared to focus combat power on multiple targets, on short notice to move, and ensure a sustainable capability to rapidly provide logistics support to manoeuvre forces. The ability to quickly deploy, build, and sustain combat power will remain at the vanguard of our unique capability. Army Aviation will be critical across the full spectrum of operations and fully integrated within joint, interagency, and multinational frameworks. A transformation process has begun and will develop Army Aviation in the years to come, with the aim to improve operational and logistics functions, including related organizational structures. This will increase lethality, agility and versatility. The goal is a networked force, capable of providing a wide range of options across the full spectrum of conflict. We have to retain conventional war capabilities along with very well trained and educated personnel who can fight across this wide spectrum. Personnel must be able to adapt rapidly to threats, especially in the cyber, hybrid and EW domains, when radio, standard navigation systems, and tactical links are severely degraded. In the end, the ability of our personnel and equipment to operate effectively in various environments will determine the success or failure of the mission.

Sir, thank you for your time and your comments.

Brigadier General Paolo Riccò

graduated from the Italian Army Academy with a Masters Degree in Strategic Science in 1989. He started his career as parachutist and was awarded the Bronze Medal for Military Value while employed as a parachutist company Commander in the UN Operation 'Restore Hope' in Somalia, 1993. In 1995 he was rated pilot and started his adventure in Army Aviation, subsequently commanding at the squadron, group, regiment and brigade levels. During his career, he has joined various NATO/UN operations in Bosnia-Herzegovina, Albania and Afghanistan, serving in numerous positions as Commander and staff officer. He is a pilot rated on aircraft types NH-500, AB-206, AB-205 and AH-129C/D 'Mangusta' and has approximately 1,500 flight hours. Since the 24th of March 2017, Brigadier General Paolo Riccò has been the Commander of Italian Army Aviation.

Logo: © NATO; Binary Code: © Yurchanka Siarhei/shutterstock; Circuit Board: © Kotkoa/shutterstock

Cyberspace NOTAM!

NATO's Vision and Strategy on the Cyberspace Domain

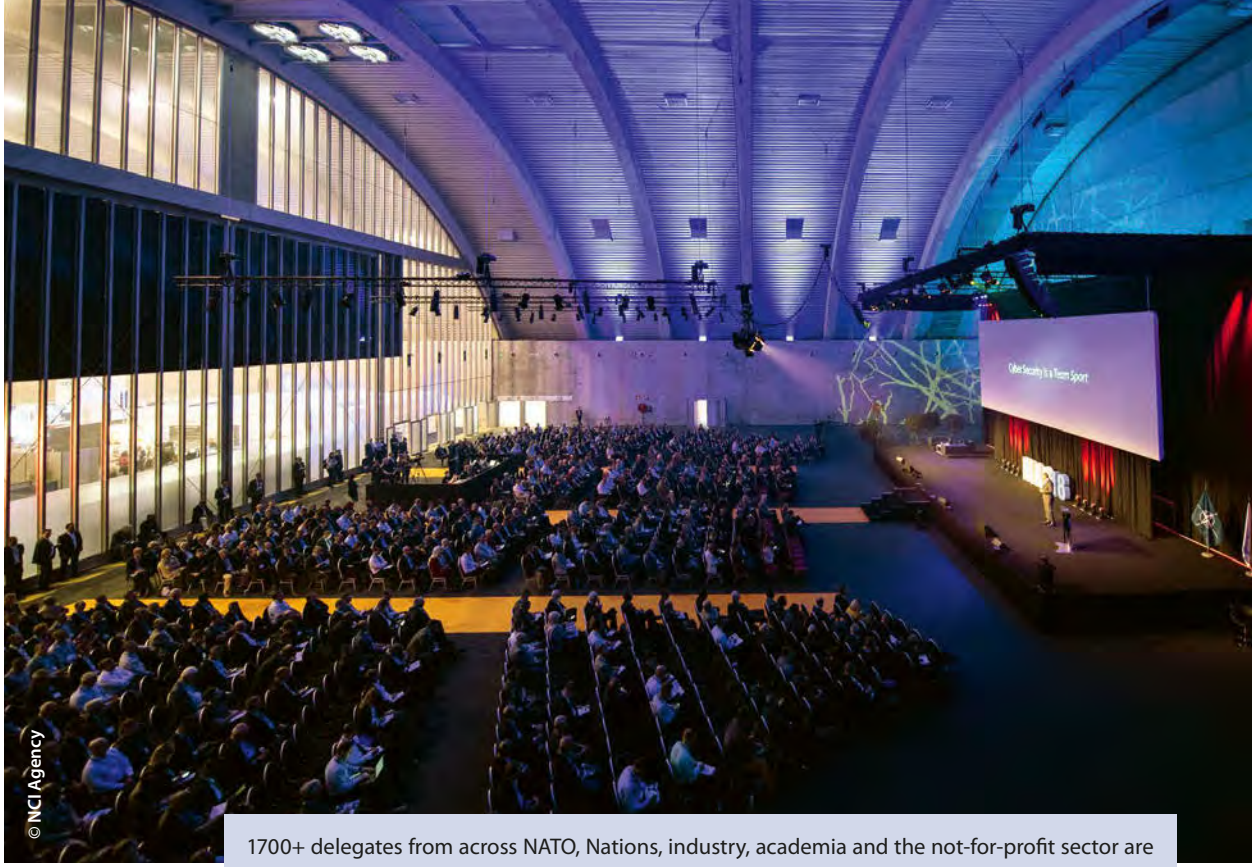
By Lieutenant Colonel, Paul J. MacKenzie, CAN AF, JAPCC

Introduction

On 6 June 2018 the North Atlantic Council (NAC) approved the Military Committee's (MC) Vision and Strategy (V&S) on Cyberspace as a Domain of Operations, a significant milestone in the ongoing development of this Domain for the Alliance – essential for policy, capability and doctrine development as well as for guiding operational planning and mission execution. The high-level message up front: NATO **must be able to defend itself in Cyberspace** (during peacetime, crisis and in conflict) as effectively as it does in the other Domains, and **must integrate Cyberspace into a coordinated cross-domain approach** to achieve joint operational effects in support of NATO's deterrence and defence posture. Furthermore, two guiding principles permeate the V&S, that effective Cyberspace defence requires *'a persistent level of readiness'* and that *'coordination of cyberspace operations . . . is best centralized.'*[1] Personnel throughout the Alliance must understand what this means in order to adapt and/or refine how we function to be able to support the ongoing development of our capabilities in Cyberspace. Those in the Air Forces in particular, charged with maintaining policy and doctrine, as well as those planning and coordinating the projection of Air Power assets, must ensure the Air Domain and rapidly developing Cyberspace Domain are aligned and 'fly in formation', or change their flight plan and alter heading as required.

Defence: Possess and Defend

Toward defending itself in Cyberspace, and though it may seem somewhat contradictory, the MC recognizes two lines of effort: NATO must **possess and**



1700+ delegates from across NATO, Nations, industry, academia and the not-for-profit sector are meeting in Mons to discuss cross-domain applications of cyber security.

maintain its own networks (modern and secure, static and deployable) and at the same time **be prepared to carry on with Alliance Operations and Missions (AOM) in a degraded environment** in the event that attacks conducted in and through Cyberspace against our systems are successful. As far as possessing and maintaining our own networks, the NATO Communications and Information Agency (NCI Agency or commonly referred to as 'NCIA') is the principle Command, Control and Communications (C3) capability deliverer, Communications and Information Systems (CIS) service provider and Information Technology (IT) support organization for the Alliance, and this will not change in the foreseeable future. With a great deal of technical expertise and experience, formed into its current state in 2012 but with roots going back 60 years, NCIA is emerging as a premier agency for providing modern and secure networks. Aside from the more familiar services (such as the NATO UNCLASSIFIED and SECRET Networks), NCIA delivers a host of specialized support such as the Command and Control (C2) technology to support Ballistic Missile Defence (BMD), the Air Command and Control Systems (ACCS) and the Federated Mission Network (FMN)[2].

NCIA and its detachments throughout NATO are highly trained and well equipped to provide the level of security necessary for its networks. Their Annual Report for 2017 admits, however, that vacancies, aggravated by a competitive market and cumbersome personnel regulations, meant it struggled to achieve the level of workforce required to make good on all of its service delivery demands.[3] Despite fewer staff than required, the first-class skills and agility of its personnel are proven. It was NATO's team of 30 cyber defenders led by NCIA that won the international Cyberspace Exercise 'Locked Shields' in 2018.[4] Locked Shields is generally believed to be the 'largest and most advanced live-fire cyber defence exercise in the world […] for national Cyber defenders to practice the protection of national IT systems and critical infrastructure under the intense pressure of a severe cyber-attack'.[5] So, in terms of NATO's own systems, the Alliance is at least 'on course' to providing, maintaining and defending its networks.

What of more specialized, aerospace systems and networks critical to NATO AOM but not provided or supported by NCIA? Michal Kalidova and Alexander DeFazio, from the Defence Investment Division of the NATO HQ International Staff, examined the defence of NATO's aviation capabilities against attacks in/through Cyberspace. Unsurprisingly, they reported that our collective aviation assets (military and civilian) are

heavily dependent on Cyberspace, and not only on traditional IT/CIS. This dependency extends through operational systems in our Air Operations Centres, Air Traffic Management (ATM) and other specialized mission systems and, finally, into our aircraft platforms themselves. They remind us that many of the aviation systems in use today were designed decades ago before the explosive growth of the Internet and the full extent of the threat of attack possible through Cyberspace was fully appreciated. Consequently, there remain numerous potential access points for would-be attackers, including 'maintenance and logistics systems, radios and datalinks, and other systems that connect operators and platforms (i.e. aircraft, pods or weapons)'.[6] Given the prominence of legacy systems and numerous potential access points, they concluded that the best way to defend aviation assets and systems from Cyber attacks 'is through a combination of defence in-depth, resiliency and advanced defence measures'.[7] Briefly, by 'defence in depth' they mean sound system design/engineering and efficient application management to reduce attack surfaces, having layers of barriers to thwart unauthorized access, borders to prevent lateral movement within systems, measures to deny privilege escalation and features preventing data exfiltration. 'Resiliency' refers to the ability to continue operating despite being under attack (a recurring recommendation). By 'advanced defence measures' they mean those procedures and tools to enable monitoring, detecting, isolating and defeating attackers, as well as incorporating Cyberspace into the comprehensive and well-established Aviation Safety and Airworthiness programs. While the V&S does not specify aerospace systems, the direction and guidance to achieve the requisite level of security certainly apply. Naturally, if the experts assess that defence in depth, resiliency and advanced defence measures are required, then it rests upon personnel at all levels in operational and supporting roles in the air environment to apply the necessary rigour to establish the goals and identify, implement and enforce the standards to achieve this level of security.

'… where this might be applicable is when the source of attacks through Cyberspace against NATO can be reliably pinpointed to a structure housing a data centre or a server farm within enemy territory.'

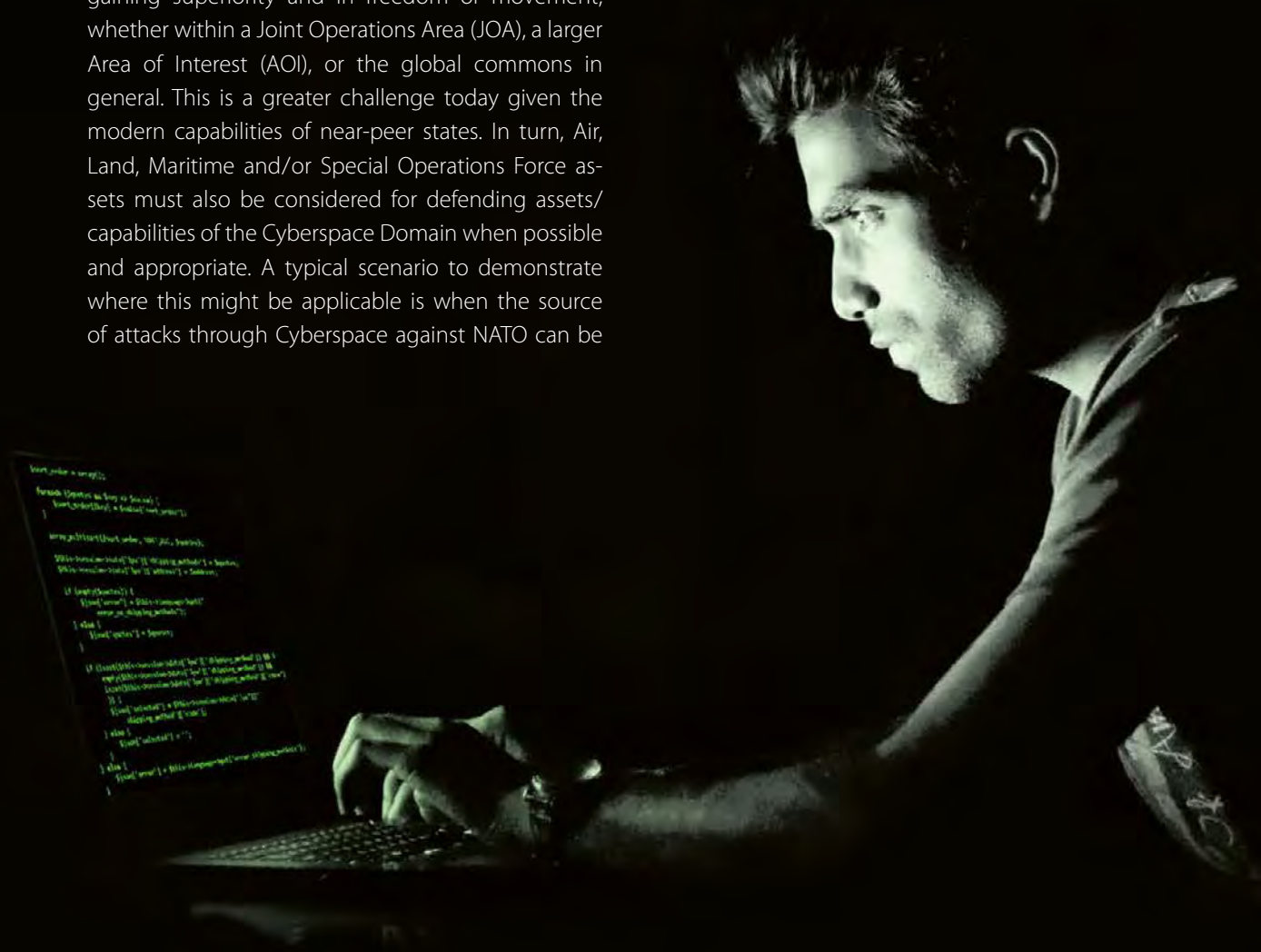
Defence: Prepare for a Degraded Environment

What of the second line of effort, preparing for the dreaded possibility of having to work in a degraded environment? If the defensive posture should fail and the integrity or availability of networks/systems are compromised, NATO must still be able to carry on with AOM. Despite the theft of designs[8] and cyber defence vulnerabilities[9], let us presume for the moment that the adversaries do not have the ability to infiltrate and degrade NATO's flying platforms or tactical weapons systems and restrict consideration to IT/CIS and C2 systems. How prepared is NATO to operate in a degraded environment? Are NATO planners and coordinators able to 'retrograde', back to the point of using past tools such as pens and paper, grease pencils and plastic boards, telephones and faxes if necessary? We will not know the answer to these questions until we exercise under these conditions. The argument most often heard during exercises is that we can't take down our systems since that will interfere with achieving the training objectives. Perhaps we need exercises specifically focused on planning, executing and coordinating operations in a degraded environment; it's not unheard of as senior Russian officials insisted on doing just this after they discovered that their junior officers became too dependent on modern IT/CIS and were no longer able to conduct 'low tech' war.[10]

Integration with Other Domains

The second high-level aim is to integrate Cyberspace into a coordinated, cross-domain approach in the planning and execution of Joint Air Operations; this is not going to happen overnight. It is generally well-known that those personnel working in the Cyberspace Domain support air operations. Less understood is that the converse is equally true and accepting this could indeed represent a shift in culture. Until this

shift is achieved, there will remain a requirement to actively ensure commanders at all levels, and their staff, are continually kept appraised of the operational dependencies on Cyberspace and the related risks to the mission, as well as the importance of both mitigation measures and responses. Though the Air Force's historical advantages were speed, reach and precision when compared to the other traditional Domains, effects in and through Cyberspace can be delivered faster, further and with greater precision. But, as we strive to achieve joint effects, we must avoid such comparisons that serve to distinguish Domains. Rather, it must be determined where and how these unique characteristics of Cyberspace can be brought to bear in concert with the other Domains to achieve the greatest impact, the greatest advantage in terms of gaining superiority and in freedom of movement, whether within a Joint Operations Area (JOA), a larger Area of Interest (AOI), or the global commons in general. This is a greater challenge today given the modern capabilities of near-peer states. In turn, Air, Land, Maritime and/or Special Operations Force assets must also be considered for defending assets/capabilities of the Cyberspace Domain when possible and appropriate. A typical scenario to demonstrate where this might be applicable is when the source of attacks through Cyberspace against NATO can be reliably pinpointed to a structure housing a data centre or a server farm within enemy territory. The Joint Force Commander in this instance might consider using [or employing] Air Forces to launch a kinetic strike to destroy the systems in order to stop the attacks. Another potential scenario could include where a combatant is identified as a key agent in the C2 structure continually directing/coordinating attacks on [or against] NATO in/through Cyberspace. This agent could legitimately be considered for assessment and inclusion in the commander's targeting cycle by any number of means available to them in order to stop, or at least delay, further attacks against NATO. The V&S acknowledges that, if the only, or most appropriate,



© iAmMrRob/pixabay
Source Code: Boskampi/pixabay

response is assessed to be offensive effects through Cyberspace, this integration must include a mechanism for NATO to seamlessly incorporate sovereign capabilities provided voluntarily by allies – in other words the ability to leverage a member nation's offensive capability via Cyberspace when necessary, but not develop or generate offensive effects itself. After all, NATO remains a defensive Alliance and currently has no plan to develop its own offensive capabilities for the Cyberspace Domain.[11]

Readiness: Train as You May Have to Fight

The V&S stresses the importance of having highly educated and well-trained forces employed in the Cyberspace Domain. Along with member nations developing and training their own personnel, NATO must ensure realistic and challenging exercises, not only for the Cyberspace experts (such as 'Locked Shields' and 'Cyber Coalition'[12]), but ensure that the Cyberspace Domain is a key part of its major exercises, fully integrated with the other Domains. NATO is not unlike member nations when it comes to exercises, the combatant commands of which often 'conduct training in a relatively benign cyber environment which is unlikely to exist … [that] provide the warfighter with a false sense of confidence about the scope and magnitude of the cyber attacks facing the Department'.[13] Exercise Trident Javelin 2017 was a breakthrough exercise in this respect, where the Cyberspace Domain achieved a great deal of prominence, and progress was also made in Exercise Trident Juncture 2018 where responses to Cyberspace incidents included a broad view of the entire Theatre and focused on Mission Assurance. But, this momentum must be maintained. Work is still required to better represent Cyberspace as a Domain and improve the Commander's understanding of the nature of Cyberspace operations and the implications of the integration in military operations.

Readiness: Alliance Teamwork

The V&S is intended to be comprehensive, to span the entire Alliance. There's no sense in having a few or even one member nation not aligned with this strategy since the security of the systems spanning NATO will only be as strong as its weakest link. The 'Cyber Defence Pledge'[14] agreed to at the Warsaw Summit, is addressing the requirement for member nations to defend their own networks, military systems and critical infra-

structure. Still, there are mechanisms in place now to facilitate mutual support if/when required (such as the NCIA-provided, Cyber Defence NATO Rapid Reaction Team) and NATO will work towards achieving greater coordination and linkages with member nations' incident and response options including intelligence sharing, military-civilian cooperation and collaboration with industry and academia. Member nations are encouraged to invest domestically to grow and develop talent at home and in order to assist NATO with addressing shortages of Cyberspace experts in the NATO Force Structure (NFS). Alliance nations will employ the NATO Defence Planning Process (NDPP) to guide the development of Cyberspace capabilities to meet NATO's requirements, once again leveraging the knowledge of industry, academic and civilian stakeholders by fostering unity of effort.

Centralized C2 of Cyber Forces

The second of the V&S' two guiding principles in the pursuit of adequate self-defence is that 'coordination of cyberspace operations … is best centralized'.[15] It should come as no surprise to Airmen that the structure for the most effective C2 over operations in the Cyberspace Domain would emulate the time-tested structure of that in the Air Domain where the span of control over forces is best exercised through the Joint Forces Air Component Commander. Similarly, the creation of the Cyberspace Operations Centre (CyOC)[16], as part of the adapted NATO Command Structure, will establish the equivalent of the Cyber Component staff for the theatre. It will strengthen defences by providing operationally-focused 'incident management, situational awareness and Command and Control'[17] and facilitate integrating the Cyberspace Domain into planning, execution and coordination of exercises and operations.[18] CyOC staff will liaise with Nations and coordinate the integration of sovereign Cyberspace effects provided voluntarily by Allies in AOM. This level of integration demands a high level of situational awareness of our own networks/systems. Having a clear picture of the state of Alliance Cyberspace, its defences and C2 platforms in order to coordinate activities is a must and will be accomplished through Cyberspace Situational Awareness Tools. Considering investment/procurement, getting the right tools for the job is critical to achieving the proper Situational Awareness and must be done without the complications that have hounded and delayed other large programmes in the recent past; without it, centralized C2 of Cyberspace forces will be irrelevant and the consequences severe.

Conclusion

Digitization and hyper-connectivity of our society in this Internet era presents a challenging battlefield for NATO. The Alliance must protect its information, networks and systems during peacetime, crisis and conflict. The potential targets are wide-ranging and span the entire spectrum of our modern, digital society (civilian and military), strikes against which can achieve operational and strategic effects while remaining below the traditional thresholds for crisis and conflict. The direction and guidance in the V&S applies not only for those formulating the appropriate doctrine and policy, but for those that influence planning operations and exercises in the Joint Air Environment and for the successful execution of AOM and other core tasks. Commanders must be provided the authorities and resources to carry out the associated tasks along with the tools necessary to provide the appropriate SA. To this end, the V&S is a sound flight plan to support the development of Cyberspace doctrine, policy and capabilities in a multi-domain approach that serves to maximize the potential of Cyberspace Forces. With this in mind, the V&S will only be successful with the full support of the member nations and their personnel in all levels of command.

Another important milestone will be reached when the official NATO Cyberspace Doctrine is approved by the NAC. While the AJP 3.20 Cyberspace Operations Doctrine was drafted in January 2016, it is in its third iteration and it is hoped we will see this ratified before the end of 2019. Though drafted before the V&S, in its current form, AJP 3.20 reflects the V&S's key elements. ●

1. North Atlantic Treaty Organization (NATO), MC 0665 Military Vision and Strategy on Cyberspace as a Domain of Operations, 12 Jun. 2018, p. 4.
2. NATO Communications and Information Agency, Customer Services Catalogue, Application Services [cited 25 Oct. 2018]. Available from https://dnbl.ncia.nato.int/Pages/ServiceCatalogue/CPSList.aspx#; Internet.
3. NATO Communications and Information Agency, NCIO 2017 Annual Report, 14 May 2018, p. 7.
4. Cooperative Cyber Defence Centre of Excellence (CCD COE), 'NATO Won Cyber Defence Exercise Locked Shields 2018' [cited 23 Sep. 2018]. Available from https://ccdcoe.org/nato-won-cyber-defence-exercise-locked-shields-2018.html; Internet.
5. CCD COE, 'The Largest International Live-Fire Cyber Defence Exercise in the World to be Launched Next Week' [cited 23 Sep. 2018]. Available from https://ccdcoe.org/largest-international-live-fire-cyber-defence-exercise-world-be-launched-next-week.html; Internet.
6. DeFazio, Alexander and Kalivoda, Michal, Defending NATO's Aviation Capabilities from Cyber Attack, JAPCC Journal Ed. 23, Autumn/Winter 2016, p. 106.
7. Ibid. 6, p. 108.
8. Nakashima, Elle, 'Confidential Report Lists U.S. Weapons Systems Design Compromised by Chinese Cyberspies', Washington Post, 27 May 2013, [cited 24 Sep. 2018]. Available from https://www.washingtonpost.com/news/worldviews/wp/2013/05/28/the-u-s-weapons-systems-that-experts-say-were-hacked-by-the-chinese/; Internet.
9. United States Government Accountability Office, Report to the Committee on Armed Services – US Senate, WEAPON SYSTEMS CYBERSECURITY – DOD Just Beginning to Grapple with Scale of Vulnerabilities, GAO-19-128, Oct. 2018.
10. Giles, Kerr. Handbook of Russian Information Warfare, NATO Defence College, Rome, Nov. 2016, p. 68.
11. This is what makes it impossible to make a direct comparison between NATO's Vision and Strategy and another nation's. For example, while NATO's V&S aligns in some respects with the US DOD 2018 Cyber Strategy of Sep. 2018 (secure networks/infrastructure, integrate with other Domains, operate in a contested environment, collaborate with industry, exercise/cultivate talent) it is void of any references to offensive cyber effects (pre-emptive action, defend forward, proactive engagement, offensive action, amplify military lethality).
12. NATO, 'NATO's flagship cyber exercise begins in Estonia' [cited 23 Sep. 2018]. Available from https://www.nato.int/cps/en/natohq/news_149233.htm; Internet.
13. Office of the Director, Operational Test and Evaluation, DOT&E FY 2017 Annual Report, 'Cybersecurity', p. 315 [cited 3 Oct. 2018]. Available from https://www.dote.osd.mil/pub/reports/FY2017/pdf/other/2017cybersecurity.pdf; Internet.
14. NATO, Cyber Defence Pledge [cited 26 Sep. 2018]. Available from https://www.nato.int/cps/en/natohq/official_texts_133177.htm; Internet.
15. North Atlantic Treaty Organization (NATO), MC 0665 Military Vision and Strategy on Cyberspace as a Domain of Operations, 12 Jun. 2018, p. 4.
16. NATO, TAB B to APPENDIX 1 TO ANNEX C TO ENCLOSURE 5 TO SH/SAG/OACM/18-320541 5000-TSC-PPX-0010/TT-180332/Ser:NR0014, dated 25 Apr. '18.
17. Ibid. 14, p. 8.
18. NATO, 'Speech by NATO Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference (Ecole militarie, Paris)' [cited 26 Sep. 2018]. Available from https://www.nato.int/cps/en/natohq/opinions_154462.htm; Internet.

Lieutenant Colonel (RCAF) Paul J. MacKenzie, MSM (US), CD

A Communications and Electronics Engineering (Air) Officer in the Royal Canadian Air Force, he examines Cyberspace as it relates to NATO Joint Air Power and from a defensive perspective through to the potential in exploiting offensive effects. He holds a Master's of Science degree in Computer and Information Technology (System Engineering), is a graduate of the CF Joint Command and Staff Program and has over 30 years of experience in the provision of IT/CIS to operations. His senior appointments include Director of Operational Support (CIS) – CANOSCOM HQ (Ottawa), Chief of the A6 Staff – NATO AWACS Airbase (Geilenkirchen), CO Canadian Contingent (Technical Element) NATO AWACS and Director of the A6 Staff – 1 Canadian Air Division (Winnipeg). He was Chief OPFOR (Cyberspace) for Exercise Trident Javelin 2017.

Is NATO Ready for Galileo?

How the Combination of GPS and Galileo could Increase NATO's Resiliency in PNT

By Lieutenant Colonel Tim Vasen, DEU A, JAPCC

Picture 1: GPS-III satellite.

Introduction

NATO operations rely significantly on space support services given by the member nations. One of the most essential is the Positioning, Navigation and Timing (PNT) service[1], provided by the United States' Global Positioning System (GPS) constellation.[2] GPS, as defined by the Memorandum of Understanding IV, is to be used by all NATO nations.[3] GPS has become a global utility comparable to the internet and does not 'just' provide positioning data. The most important civilian use, which is also important for the military community, is the timing signal which synchronizes communication and encryption for financial transactions worldwide; from cash withdrawals to stock exchange markets, where changes in the currency have wide impact.[4] While the USA has formulated first requirements to strengthen the resiliency of GPS, NATO has additional options to improve resiliency by integrating the Galileo constellation, operated by the European Union (EU).[5] This article will focus mainly on the military implications of these two

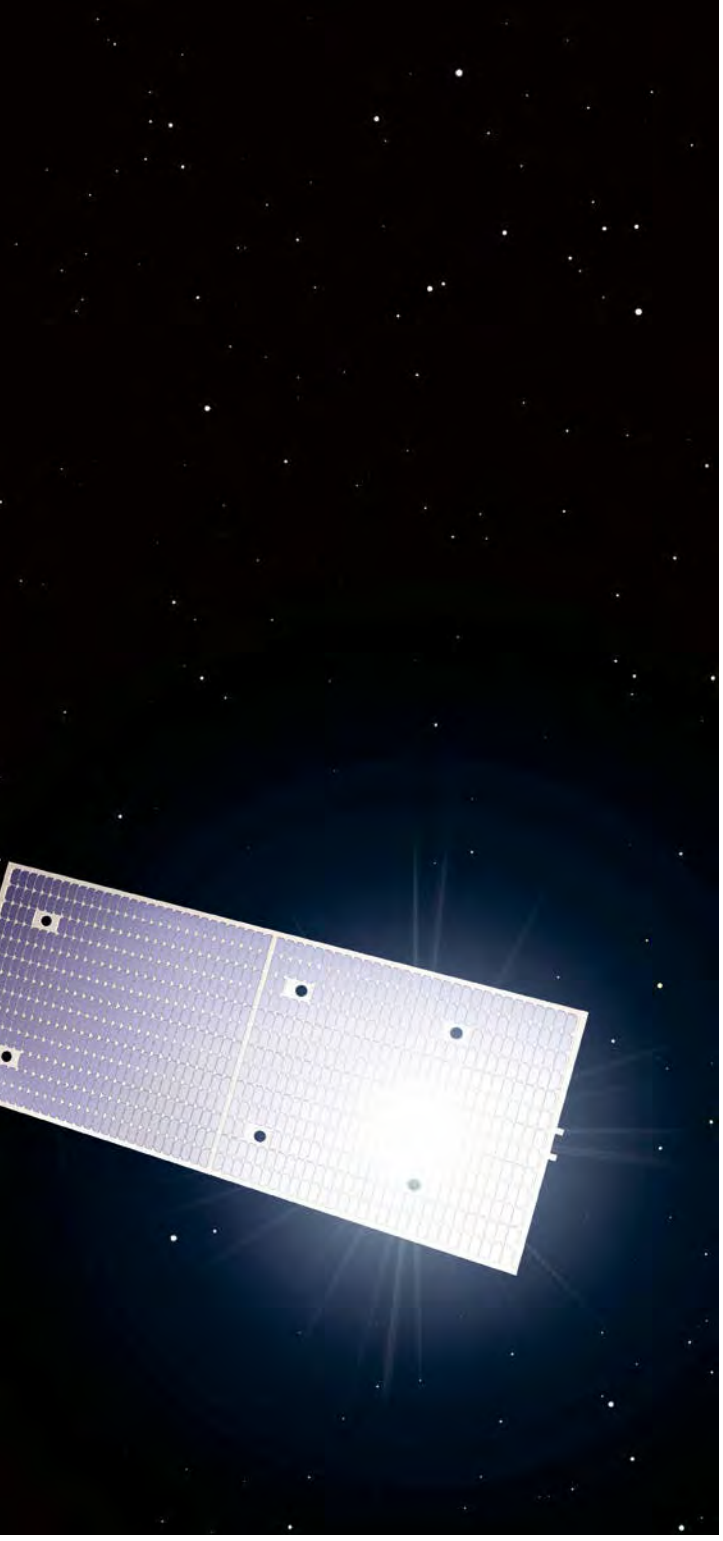
Galileo logo.

Picture 2: Galileo satellite.

Global Navigation Satellite Systems (GNSS), to ensure NATO members and policymakers are informed concerning the PNT options available to the Alliance. This article will first address the various threats to PNT services before looking at the idea of utilizing PNT receiver equipment capable of utilizing signals from multiple GNSS in combination. Secondly, it will address various technological and policy challenges facing the combination.

Threats to PNT Services

If NATO loses its PNT support it will have huge impacts on NATO military operations. However, an opponent who does not rely on GPS services may not be adversely affected. A low tech opponent may not be reliant on PNT data so he might be least affected by a denial of service. A peer opponent may operate its own PNT system, which, if intact, provides



an advantage against NATO (see Table 1). This will last until NATO counters the adversary's service with a corresponding PNT denial. These kinds of PNT warfare are summed up under the term Navigation Warfare (NAVWAR). According to Russian doctrine, for example, a highly capable PNT jamming component is included at least on the brigade level (land forces) and Russian forces are trained to fight in a degraded PNT environment.[6]

PNT services can be affected by jamming of the transmitted signals between satellites, ground stations and user segments within the broader spectrum of counter-space actions.[7] Jamming is the intentional interference with receivers by additional signals sent from opponents' transmitters. The aim is to overpower the satellite signal with a 'noise signal' strong enough that the receiver is not capable of receiving the original signal anymore. Jamming attacks are typically reversible attacks.

To jam PNT services, there are a large number of different, mainly military-developed jammers available. All worldwide available space-based navigation systems are operated by the military, except Galileo, and have at least one secured frequency, reserved for governmental and military use. To jam the full service of a system requires a wideband jammer, or several jammers. Nevertheless, this means an opponent could jam the NATO GPS system, while relying on another system (see Table 1). This could cause non-usability of PNT services for NATO, while the opponent has full service. Highly capable stationary and mobile PNT signal jammers exist, and are typically used for military purposes. The antenna size and electrical power of the jammers define the range. Even very small, Commercial Off-The-Shelf (COTS) jammers, down to the size of a cigarette-box, allow short range (up to a few kilometres) jamming of at least one frequency.[8] Manuals to build these kinds of systems can be found online, and the technical parts can be purchased at a regular electronics store. PNT jamming effects can also have major impacts on civilian life. PNT services are not only used in navigation devices or controlling traffic, as stated previously, they also support coordinating

EU	EU and NATO	NATO
AUT, CYP, FIN, IRL, MLT, SWE	BEL, BUL, CZE, DEU, DNK, ESP, EST, FRA, GBR*, GRC, HRV, HUN, ITA, LTU, LUX, LVA, NLD, POL, PRT, ROU, SVK, SVN	ALB, CAN, ISL, MNG, NOR, TUR, USA

*as of 31 May 2019
BREXIT decision pending

Table 1

global financial transfers. This implies that in a jamming environment, within the jammed area, the use of Automated Teller Machines (ATMs) and stock trading would not be possible.

A more specialised type of PNT jamming is referred to as 'spoofing', which describes the use of higher power suppressing the original signal and replacing it with a false one. 'Spoofing' is most effective in smaller areas where the difference in the position is difficult to recognize by operators while monitoring other navigational options. The new signal provides 'wrong' signal data, which causes incorrect position calculation and/or timing.[9]

Besides these man-made threats there are also environmental influences. The most critical environmental effects on PNT systems are caused by space weather phenomena.[10] While jamming can be overcome using countermeasures, space weather effects influence all GNSS services and may be more difficult to counter. Geographical and topographical factors could also affect signal reception by the user segments on the ground due to shadowing.

The Idea of a Combination[11]

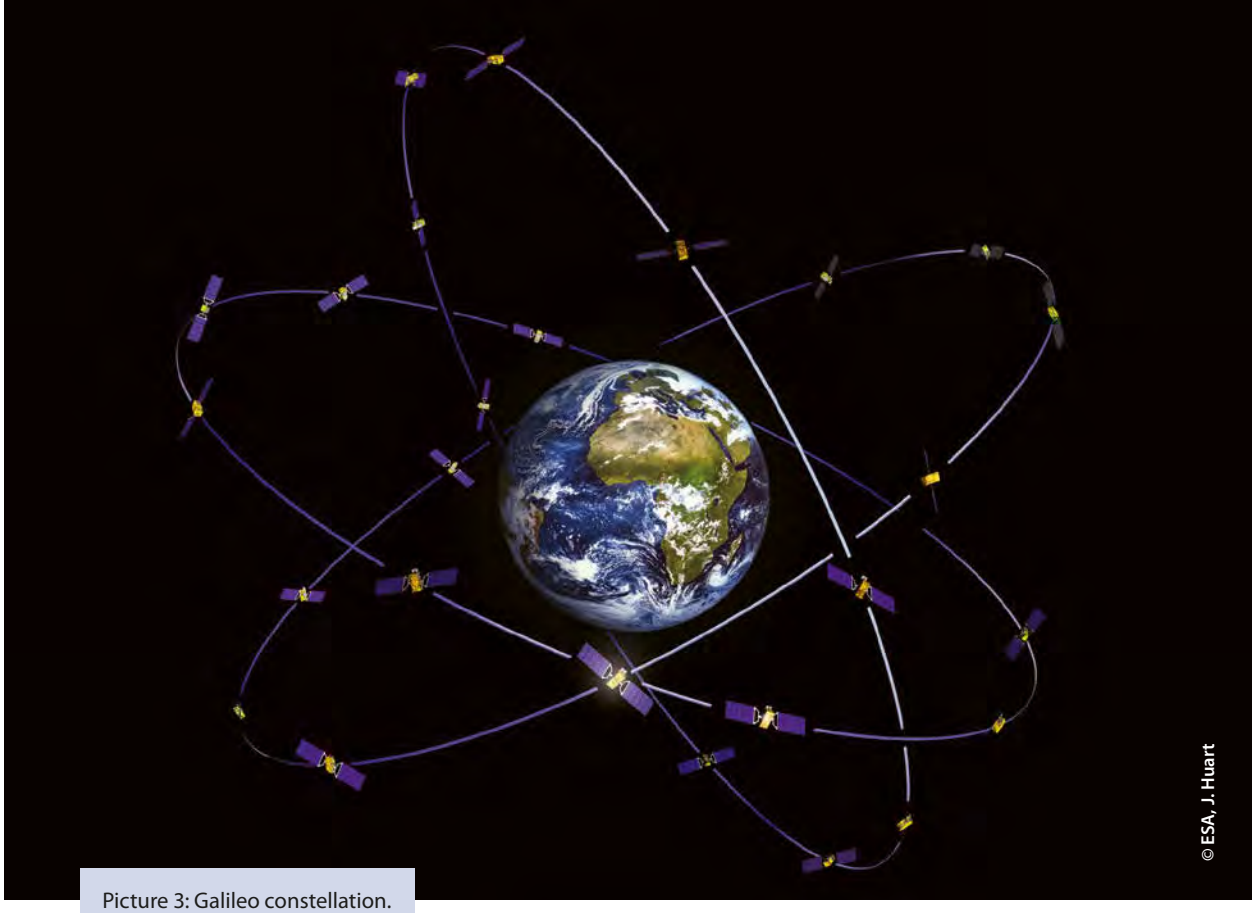
On the civilian side, the access to free receivable but unencrypted (and also unprotected) GNSS signals is quite easy. Most mobile phones are already using at least two or up to four different GNSS. The US and the EU are continuing negotiations to licence civilian services provided by Galileo on the US market.[12] The resulting advantages of using more frequencies have been recognized, improving the overall PNT service.[13] The Transatlantic makeup of NATO already provides the Alliance with the option to use both GNSSs and take advantage of them.

Advantages of a Combination

A combination could provide greater access to GNSS, even in urban or mountainous areas where shadowing of the PNT signals is commonplace. Modern commercial PNT receivers are built to use GPS, Russia's GLONASS and in some cases the Chinese BeiDou as well as the EU's Galileo. Regionally there are Space Based Augmentation Systems (SBAS) integrated into local PNT Networks that supply additional correction signals. A combination of only GPS and Galileo will not increase the position accuracy, due to the very similar geometry of both systems (GPS and Galileo).[14] Also, the usable area, especially north and south of 75° latitude will not be extended. Based on the fact that both systems are very similar, but rely on specifically designed reference frames, the data computation has to be done by a software solution. However, the ability to utilize both systems provides enhanced resiliency, so it is worth the effort.

Military receivers rely on protected signals. In the case of GPS, the military uses the Precise Positioning Service (PPS), based on the so-called P(Y) code, which can use two different frequencies. Galileo is protected by the Public Regulated Service (PRS) and uses two frequencies as well, different from the GPS frequencies. To gain advantages of both systems, receivers are needed that are not just able to receive both signals and calculate navigation data in parallel, but also able to combine them (e.g. position calculated out of two Galileo and two GPS satellite's signals). On the civilian side, multiple receivers have been successfully developed for the free signals which opens the opportunity to pursue combination also in the protected military or governmental services.[15] But even the option to use both of the free constellation services in parallel will increase the hardening against external influences. Parallel use of both systems could also be used as a 'spoofing' indicator as it always cross-checks simultaneously, and in parallel calculates positions of both GNSS. If one gets spoofed the other detects this effect and warns the user. Simultaneous 'spoofing' of two different GNSSs has not yet been observed and is technically more complicated. Detection of 'spoofing' research has been done by using an opponents' navigation signal as an indicator.[16] There is a definite need for a NATO PNT Warfare Playbook to specify measures and countermeasures.

According to the threat assessment, a combination of GPS and Galileo will increase the jamming resistance. An opponent will either have to use more



Picture 3: Galileo constellation.

jammers to affect the additional frequencies or concentrate on specific geographic areas or sectors to jam PNT signals. An area-wide jamming campaign will be harder to achieve and sustain over a long period of time.

Challenges of a Combination

To achieve a combination within a given receiver system may require additional antennas or receiver channels to accommodate the increased number of available PNT signals. The hardware of the receivers has to be adjusted, because current military PNT receivers, opposed to civilian receivers, are either only equipped with a GPS or a Galileo receiving device. Future receivers (able to use the GPS PPS as well as the Galileo PRS signal) need both receiving and decryption devices within a single system.

Additionally, every EU nation that uses the Galileo PRS signal is required to establish a Competent PRS Authority (CPA) which is responsible for the licensing of users inside the nation.[17] Users are defined as governmental and security agencies (e.g., police, firefighters, and paramedics). By national definition, an operator of critical infrastructure could be a potential licensed user. The EU could also allow so-called third parties, non-EU nations or international organizations the use of the PRS. This decision has to be made by the whole EU in consensus. If a nation is licensed, it then has to establish its own CPA for further licensing inside the country.

In comparison to GPS, where a single nation is responsible for all security licensing procedures, Galileo has 28 responsible nations and may add even more (depending on the non-EU nations) in the future. Galileo PRS security modules must be physically produced inside the EU, licensed external production is not allowed. They are designed as a 'Black Box' that includes a tamper function to prevent any attempt to gain insight into the security module, either hardware or software, if breached. This regulation and function can hamper the implementation especially inside of precision-guided ammunition by national regulations or concerns of the PGM providing nation. Besides the licensing for PRS, the interoperability or standardization process has to be ongoing to implement the services in systems. It implies sustainable willingness and a lot of negotiations, and paperwork, on both sides (EU/USA) has to be done.

Summary

From the operational and technological perspective, it would be a massive improvement in PNT resiliency if both GNSS could be integrated into the NATO system. The fact that Galileo is not operated by a single nation creates challenges in the use of the PRS as well as in security issues. It will be a question for the future whether the US will modify its security standards to fully integrate Galileo inside their military receivers and into NATO Operations. The EU nations have to decide if NATO or specific NATO nations can be integrated as a 'third nation entity' or if only the members of NATO and EU will use Galileo PNT as a national fall back. This indicates that in the midterm perspective presumably only national 'island' solutions will improve the PNT resiliency. If this will not be a show stopper in standardization and interoperability and positive negotiations either in the Galileo or the GPS licensing process are done, it will be an effective and successful option on the long term, either for the whole alliance or for several nations. For future challenges and threats to NATO, it seems to be crucial to understand the technological and policy options available. ●

GPS	is a military system, operated by the US military. It consists of minimum 24 satellites on six orbital planes. There are several spare satellites to create a robustness in case of technical issues. The inclination is 55° (https://www.gps.gov/) (Picture 1).
Galileo	is civilian system operated by EU. It consists of minimum 24 satellites on three orbital planes. There are at least one spare satellites per orbital plane planned. The inclination is 56°. GALILEO offers with the PRS a military usable service (https://www.gsa.europa.eu/) (Picture 2 and 3).
GLONASS	– Globalnaja Nawigazionnaja Sputnikowaja Sistema –, GNSS system operated by the Russian Space Agency Roscosmos, financed by the military (https://www.glonass-iac.ru/en/).
BeiDou-II	– Regional Navigation Satellite System (RNSS) – operated by the Chinese military. Currently in the build-up phase for a GNSS (BeiDou-III), ETIC 2020 (http://en.beidou.gov.cn/).
NAVIC	RNSS operated by the Indian Space Agency (also known as IRNSS), officially claimed as a civilian system (https://www.isro.gov.in/irnss-programme).

Table 2

1. For further details see NATO Space Handbook, published 23 Aug. 2017, NATO restricted.
2. MC 0139/3, Policy on Satellite Navigation services for NATO Military Operations, 25 Aug. 2016.
3. ANP-03 'The NATO Satellites Navigation Warfare (NAVWAR) Framework, NATO Restricted, Nov. 2004.
4. Joan Johnson-Freese 'Space Warfare in the 21st century – Arming the heavens', Routledge 2017.
5. https://fedtechmagazine.com/article/2018/05/defense-department-moves-augment-gps-alternatives, seen on 11 Jan. 2019.
6. Roger N. McDermott, 'Russia's Electronic Warfare Capabilities to 2015', Report from International Centre of Defence and Security of Estonia, Sep. 2017.
7. Cass, Stephen, 'How to kill a satellite', published in Discover, vol. 28, Issue 12, p. 56–57, Dec. 2017.
8. CHIP online 4 Aug. 2013, http://www.chip.de/news/GPS-Jamming-Zunehmende-Stoerung-echter-Signale-63473441.html, seen 15 Jan. 2018.
9. Jafarnia-Jahromi, Ali; Broumandan, Ali; Nielsen, John; Lachapelle, Gerard, 'GPS Vulnerability to Spoofing Threats and a Review of Anti-Spoofing Techniques', published in International Journal of Navigation and Observation Volume 2012, May 2012.
10. According to US Joint Doctrine, Space Weather is 'the conditions and phenomena in space and specifically in the near-Earth environment that may affect space assets or space operations'. DoD Dictionary, p. 214.
11. To find a wording solution in this article 'combination' is used. It could also be contributing, merging, etc.
12. The EU also negotiates with Norway the use of the encrypted PRS service.
13. https://in.reuters.com/article/us-usa-fcc-gps-europe/fcc-to-vote-to-allow-u-s-devices-to-use-european-navigation-system-idINKCN1MY2X6, seen on 11 Jan. 2019.
14. All technical parameters of space systems were taken out of https://janes.ihs.com/, seen on 17 Jan. 2019. Further discussions were held with the exercise support Team of the USA Joint Navigation Warfare Centre at the NATO JWC Stavanger during Exercise Trident Juncture 2018.
15. German military Geospatial Institute. Geodetic Receivers are built by Leica, Trimbl, Ashtec, etc. https://www.gpsworld.com/quad-constellation-receiver-gps-glonass-galileo-beidou/, seen on 11 Jan. 2019, http://www.navigationsolutions.eu/product/septentrio-polarx3g-dual-frequency-gpsgalileo-receiver/, seen on 11 Jan. 2019.
16. Damian Miralles, Gabriel F. P. Araujo, 'Robustness Improvements for the PVT solution via consideration of GLONASS in a GNSS software defined receiver', published in 'Inside GNSS', Jul./Aug. 2018.
17. Decision 1104/2011 of the European Parliament and of the Council dated 25 Oct. 2011.

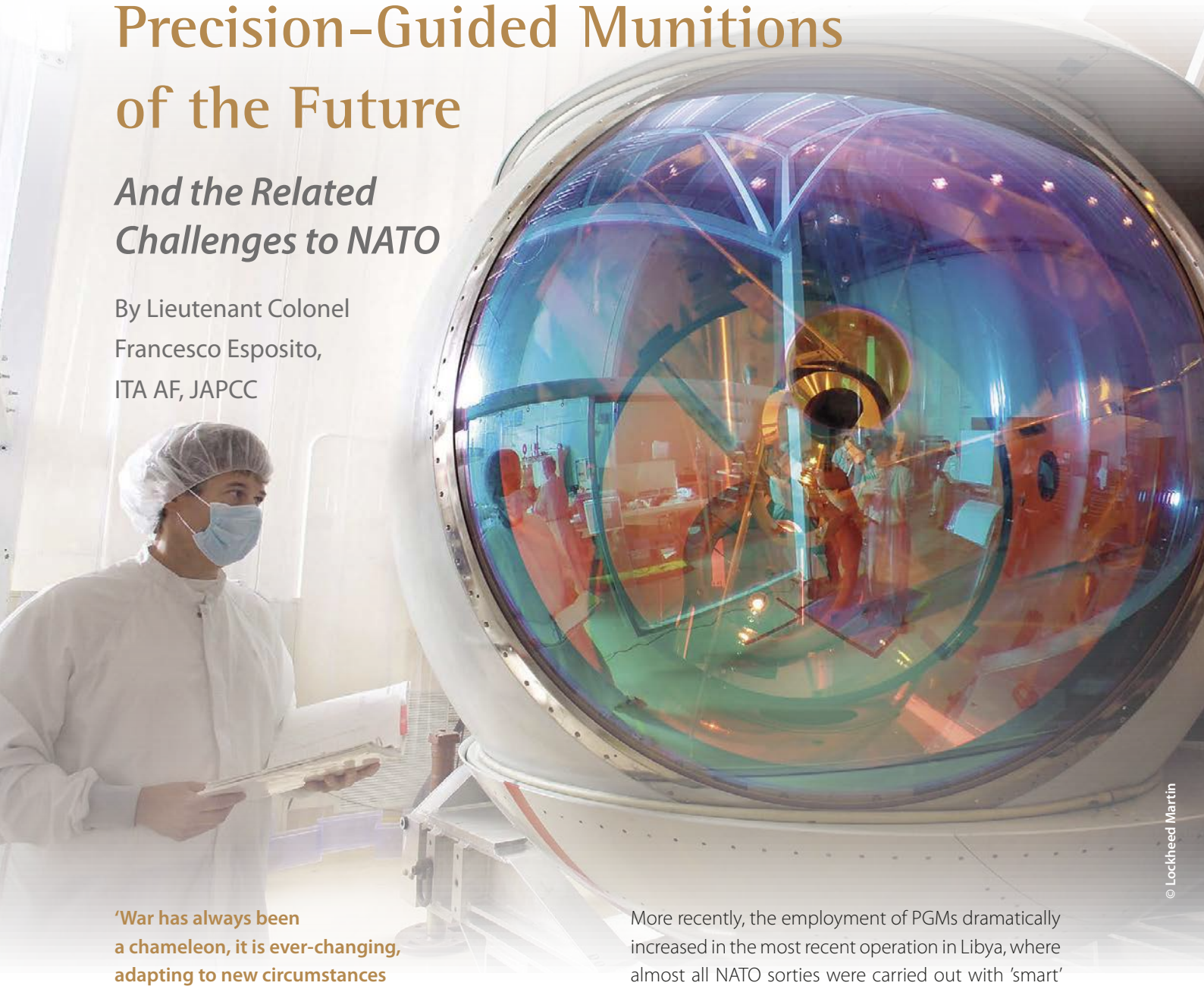
Lieutenant Colonel Dipl.-Ing. Tim Vasen

began his military career in July 1994 as a conscript. After his officer training he served for several years in commanding and staff positions within the artillery branch, including a deployment to KFOR as company commander of the DEU ISTAR-company. After 2005, he took over positions as an intelligence officer, responsible for IMINT planning and technical assessments, including positions in the office of military studies as a senior analyst for Space systems. From 2013 to 2017 he was part of the German Space Situational Awareness Centre (GSSAC) responsible for Space intelligence. Since October 2017 he has served in the role of a Space SME at the JAPCC.

Precision-Guided Munitions of the Future

And the Related Challenges to NATO

By Lieutenant Colonel
Francesco Esposito,
ITA AF, JAPCC



© Lockheed Martin

'War has always been a chameleon, it is ever-changing, adapting to new circumstances and camouflaging itself …'
Carl von Clausewitz (1780–1831)

Introduction

There has been a remarkable acceleration with the use of guided weapons since Operation Desert Storm, where unguided dumb bombs were the norm. After Operation Desert Storm, NATO members increased the use of Precision-Guided Munitions (PGMs) in Bosnia-Herzegovina, Kosovo and later in Afghanistan. More recently, the employment of PGMs dramatically increased in the most recent operation in Libya, where almost all NATO sorties were carried out with 'smart' bombs, providing the Alliance with positive and significant results, in terms of accuracy and minimizing collateral damage.

The 'why' is relatively easy to understand. Most significant among the reasons were decreasing tolerances for collateral damage. Developments in PGM-enabling fields like aerodynamics, laser technology, and electronics have brought Air Power close to a 'surgical strike' capability, which is deemed essential for modern warfare. In 2012, a study commissioned by the European Defence Agency (EDA) highlighted that 'the demand

for precision has grown, both to increase the effect against the opponent and to avoid casualties among friendly forces and non-combatant third parties.'[1]

In addition, Operation Deliberate Force showed, for the first time, an attempt to provide a tactical effect of almost a one-to-one ratio of bombs dropped to targets destroyed (about 700 precision-guided bombs dropped on about 400 Bosnian Serb targets). This gave an additional economical aspect to the 'why' of using precise weapons. 'The relationship of precision guided munitions to operational planning implies precision in terms of economy of force.'[2]

Today, despite a post-cold war economic situation where NATO member states have been forced to cut their military budgets, there has been further modernization in military technology, with nations focusing on things like protection, survivability, and precision-guided munitions. Indeed, multi-domain threats, which NATO is currently facing, dictate a priority to modernize weapons in precision, range and their ability to combat unconventional capabilities. Further, the need to fight in urban environments, to acquire targets far from the frontline, to utilize weapons in all weather conditions and in a joint effort, together with the already mentioned obligation to minimize collateral damage, are the common elements which characterize current PGMs and the platforms carrying them.[3]

Nevertheless, what political and military trends will drive the technology of precision weapons of the future? What will the PGMs of the future look like and what possible challenges regarding PGMs might NATO face fighting the next war?

Evolving Demands

General political trends and requirements are guiding technological developments of PGMs. Current political and geopolitical trends, such as uncertainty, financial constraints, manpower limitations, and no/low collateral damage requirements, are among the most important ones. The 'uncertainty' of an adversary, its offensive and defensive capacity, and the unknown battlefield, are pushing PGM research towards the requirements of more flexibility and versatility, greater adaptability, as well as multi-role and multi-purpose solutions.

Limited budgets and cutbacks to military and non-military spending are forcing nations to consider the affordability of new systems, including Commercial off-the-shelf (COTS) and 'Plug and Play' solutions, and act as catalysts for interoperability, modularity and upgradability. In the same way, manpower constraints will likely require reduced manning solutions, such as automated surveillance and remotely controlled systems; these come with their own attendant costs.

PGMs of the Future

Future 'high-tech' weapon systems are likely to have versatile characteristics and be employed across multiple domains and platforms. 'A conflict will not be limited to only one domain at any one time. On the contrary, actors will be likely to shift between domains, trying to leverage those that give them the most advantage or where they have superior capabilities.'[4]

Indeed, the next generation of PGMs will likely be carried and operated by both conventional manned platforms and autonomous Unmanned Aerial Vehicles (UAVs). These weapons will be required to have lethal and non-lethal capabilities and be able to operate in a physical environment while controlled in a virtual one. PGMs of the future might be released in cooperation with other platforms and weapon systems while retaining the possibility to be employed in individual modes; also their stand-off ranges will be extended and the manoeuvrability and precision enhanced (for employment within visual range and Close Air Support). Examples of this concept can be seen in new

© SAAB/2005

air-to-air missiles, including the AIM-120D Beyond Visual Range (BVR) air-to-air missile, which features a much greater range than the already extended range version AIM-120C, and the multinational European missile METEOR, which has an operational range of more than 300 km.[5] It is notable that the METEOR can also receive mid-course guidance updates from other aircraft and Command and Control (C2) nodes participating in the mission, providing increased degrees of manoeuvrability and precision.

Defence companies, in collaboration with nations, have already embarked on projects to design a new generation of PGMs. Raytheon Industry's laser-guided version of its 'Excalibur Projectile' (Excalibur S)[6] and Israel Aerospace Industries 'fire and forget' autonomous drone (HARPY NG)[7] are recent examples. This new generation of weapons is increasingly precise, yet flexible. Follow-on 'precision' munitions, such as hypersonic weapons and powerful laser systems are already becoming a reality.

In a recent interview, Russian President Vladimir Putin claimed a successful test of a hypersonic cruise missile. Although an interview does not validate his claim, the recent US Air Force award of a 480 million dollar contract to Lockheed Martin to develop a second hypersonic weapon prototype shows that platforms and weapons, which can travel at least five times as fast as the speed of sound, are no longer a distant mirage.[8]

Network-Enabled Weapons

A PGM which can communicate with other systems is inherently flexible and encapsulates one of the future PGM key elements. 'It is the ability to integrate and share information between platforms and systems in a timely manner that will give the Australian Defence Force a distinct edge,' said the Australian Minister for Defence, Kevin Andrews in 2017.

Network-Enabled Weapons (NEW) can fill existing gaps among the targeting cycle phases. The ability to find, track, and engage a target will be faster than before, as will be the damage assessment. This will help in de-conflicting operations, avoiding duplication of effort, reducing the potential for fratricide, and increasing the possibility of hitting the target in a timely manner.[9] These weapons will have the capability to exchange information between themselves and the nodes linked to the network (e.g. delivery platforms, C2 centres, and Intelligence, Surveillance and Reconnaissance [ISR]/satellite platforms). The result will be a weapon that collaboratively interfaces with the network, adjusts its trajectory in-flight to enhance accuracy, and provides real-time impact assessment. Information will be provided to the weapon by the most timely and accurate source available. Target coordinates will be updated and incorporated in real time into the guidance system, regardless of the weather conditions.[10] With NEWs, the physical and digital worlds are linked and provide new opportunities for employment and probabilities for success.

'However, as the warfighter moves forward and develops these weapons, a proper balance between technology and creating effects on the battlespace must be maintained to prevent an over-reliance on technology.'[11]

Achilles Heel of Future PGMS

In recent years, NATO has benefitted from being technologically superior to many of its rivals. While not a given, in future scenarios, it is unlikely that an adversary will be able to compete with a NATO aircraft which will have the degree of stealth of an F-35. It is also unlikely that an adversary will have the ambition to challenge and defeat the NATO Integrated Air and Missile Defence System (NATINAMDS). However, while the outcome of a conflict between a numerically superior force versus a technologically developed force could theoretically favour the smaller, more-advanced actor, such a result is not a foregone conclusion.[12]

In reality one of the Alliance's greatest strengths, its technological progress, might be one of its greatest weakness. Any part of this future complex network, such as a sensor, a C2 facility, or a weapon system, could be neutralized or subverted by opposing forces. It is also possible that an opponent might disable one or more of the enabling United States (US) and/or European satellites, as well as crucial radio links and critical data-managing computers.


© US DoD

In this case, the opponent will most likely use the full range of 'hybrid warfare tools' such as conventional explosives, cut cables, jammed transmissions, '[…] and anything else that comes to mind"…from little green men to big green rockets over fake news and cyber and electronic attacks…' as a speaker at the 2018 JAPCC conference mentioned.

If this happens, there might be no space-based ISR, no Global Positioning System (GPS) or Galileo positioning, no Link 16, no JCHAT (encrypted communication means), and limited computer-based mission planning. This could effectively pave the way for future NATO Air campaigns to be fought with 1980s technology, with severely 'maimed' PGMs, wherein heavy losses and 'collateral' casualties are to be expected.

Balance is the Solution

The new generation of airmen, who are skilled experts when training and operating in a perfect environment (precise Rules of Engagement, availability of GPS, Link 16 and C2 nodes), are not often trained in a technology-degraded environment, leading the training itself to a point of limited effectiveness.

Therefore, while moving forward with PGM development, NATO would be wise to implement exercises with new training events more tailored to a conflict in a 'degraded environment.' In this realistic environment member nations would be forced to operate without Link 16 or GPS. A recent interview with General Paolo Ricco', Commander of Italian Army Aviation advocates this thesis 'To increase our level of training […] we created a scenario which forces our crews to operate with minimized radio communications and without the use of GPS signals, forcing use of onboard backup systems […].'[13] Indeed, to safeguard the Alliance's military advantages, NATO must vigilantly prepare for the loss of some of the technology that helped make it so great.

On the other hand, it is possible to maintain advanced hardware and to fight with a technological advantage. To achieve this, NATO and nations must harden their own military relevant facilities and equipment against expected attacks by securing the links between the systems and the C2 nodes both in the air and on the ground, and by developing backup infrastructures. There is a persistent need to ensure effective and efficient resilience, not only of military forces but also of civilian infrastructure, by strengthening frameworks (physical and virtual) and systems against potential disruption or attack, including against kinetic and non-kinetic (cyber and electronic warfare) threats. The increased complexity of the decision-making process requires trustable information provided to commanders, at the strategical and tactical level.

Conclusion

The evolution of PGMs has provided NATO commanders with increased resilience and accuracy in air-

to-ground. Before PGMs, air-to-ground weapons had a certain degree of inaccuracy, which forced Air Tasking Order (ATO) planners to compensate with a large number of aircraft carrying heavy bomb loads. Modern PGMs allow more precise planning to hit one target with one bomb. In addition, requirements such as fighting in an urban environment, striking a target deep in an enemy defence system, and deploying weapons in all weather conditions, define current and future PGM characteristics.

Political parameters provide guidelines for new military options offered by technological developments. Future capabilities are therefore driven by political trends such as financial constraints, manpower limitations, and no/low collateral damage requirements.

Among various weapons, the future is likely to include a network-enabled PGM which can communicate with the systems present on the battlefield. The exchange of information between delivery platforms, ISR/Satellite assets, and C2 structures, will be essential to accomplish the mission with accuracy and with precision.

However, while technology is a significant factor, it does not always guarantee success. Technological advantage is important, but it must be clear that what is an advantage today is the standard of tomorrow. Therefore, the Alliance must fight complacency and continue to innovate.

To maintain a certain degree of superiority over adversaries, NATO has to be able to fight a so-called 'old style' conflict, especially if faced with the loss of the technological advantage. On the other hand, the Alliance has to defend this technological advantage by being prepared to keep its own systems and infrastructure intact and functional while rendering opposing systems and infrastructure inoperative.


© Cynthia Vernat, HQ Aircom PAO

Both solutions include positive and negative aspects. NATO, which has the ambitious task of being able to address the full spectrum of current and future challenges and threats from anywhere, and in every environment, must be able to train its personnel in all domains and in all conditions. Paradoxically, that means that the Alliance must stay at the forefront of technological innovations of PGMs while, at the same time, preparing to fight without them. ●

1. Taal, P., and Tsiamis, V., 2012. Roadmap and Implementation Plan on Precision Guided Ammunition. Available online at: https://www.eda.europa.eu/info-hub/press-centre/latest-news/12-0307/Roadmap_and_Implementation_Plan_on_Precision_Guided_Ammunition, accessed Nov. 2018.
2. Sine, J., 2006. Defining the 'Precision Weapon' in Effects-Based Terms. Air & Space Power Journal article.
3. Dilanian, A., and Howard, M., 2018. Readiness for the 21st Century: An Interview with Gen. (ret.) David McKiernan. Available online at: http://www.alu.army.mil/alog/2018/SEPOCT18/PDF/210106.pdf, accessed Oct. 2018.
4. Kepe, M., et al., 2018. Exploring Europe's capability requirements for 2035 and beyond. Available online at: https://www.eda.europa.eu/docs/default-source/brochures/cdp-brochure---exploring-europe-s-capability-requirements-for-2035-and-beyond.pdf, accessed Oct. 2018.
5. Smith R., 2018. MBDA's Meteor – The Most Advanced Beyond-visual-range Air-to-Air Missile in the World. Available online at: https://exoatmospheric.wordpress.com/category/weapons/air-launched-weapons/, accessed Jan. 2019.
6. Raytheon website. Excalibur Projectile. Available online at: https://www.raytheon.com/capabilities/products/excalibur Accessed Nov. 2018.
7. Israel Aerospace Industries Website. HARPHY NG. Available online at: http://www.iai.co.il/2013/36694-16153-en/Business_Areas_Land.aspx, accessed Nov. 2018.
8. AGM-183A Air-Launched Rapid Response Weapon (ARRW).
9. Koudelka, B., 2005. Network-enabled Precision Guided Munitions. Available online at: http://www.au.af.mil/au/awc/awcgate/cst/bugs_ch03.pdf, accessed Oct. 2018.
10. Ibid.
11. Ibid.
12. Gen. HR McMaster, comments made at RUSI Land Warfare Conference, 2015.
13. Rossetti, L., 2019. Italian Army Aviation; Current Situation, Vision and Planned Developments to meet future NATO challenges.

Lieutenant Colonel Francesco Esposito

joined the Italian Air Force in 1990, joining the Italian Air Force Academy in Pozzuoli (Italy). He was trained with the US Air Force SUNT program in Randolph AFB (TX) and subsequently graduated as a Tornado Navigator/Weapon System Operator in Cottesmore (UK) in 1996. As an aircrew with 156º Tornado Sqn, and as an instructor with 102º Tornado OCU Sqn he participated in the flying Operations in Bosnia and Kosovo. Between 2008 and 2012, he served as ATO Coordinator and Chief Strike cell in the Combined Air Operation Centre in Uedem (Germany) contributing, as an ATO Coordinator, to the Operation Unified Protector in Libya. Currently, he serves as JAPCC Precision Guided Munition Expert.

Improving NATO Air Training

An Outlook to Future Tactical Air Training

By Lieutenant Colonel Juan Cánovas, ESP AF, JAPCC

'Si vis pacem, para bellum'[1]
Publius Flavius Vegetius

To many military professionals, being well prepared for war means, among other things, one has the best equipment, updated doctrine and optimum training for a spectrum of future conflicts. Indeed, once there is a formulated idea of the future environment, NATO can, and should, update its next-generation training strategy. In regards to Tactical Air Power Training, this entails a review of the future operating environment and then a critical look at how the Alliance should adapt to prepare its aviators for the future.

Future Operating Environment

Based on the Framework for Future Alliance Operations[2], factors such as technological advances, new concepts of operation (Global Strike, Hybrid and Cyberspace operations) and shifts in the geopolitical landscape will greatly influence the future security environment. In addition, armed conflicts may be characterized by increased interconnectivity across the recognized domains of warfare (land, sea, air, space, and information environment) and, among other things, by small units fighting over greater distances.

Another takeaway from these estimations of the future is that, for the first time since the end of the Cold War, the Alliance has to be able to conduct operations against a peer-state actor. Therefore, the future operating environment may be one in which air superiority can neither be assured at the onset of operations nor, once obtained, be assumed an enduring condition[3]. As a result, during the 2018 NATO Summit, the Heads of State and Government agreed on a Joint Air Power Strategy (JAPS) which '… will strengthen our Integrated Air and Missile Defence, and guide our aerospace capabilities to operate together jointly, more swiftly, and effectively in peacetime, crisis, and conflict'.

In a future joint fight, 5th generation aircraft, like the F-35, with their sensor fusion capabilities and enabling connectivity, should be able to share a network with other service assets, such as air defence frigates or land-air defence battalions, and direct them to engage targets out of their sensor range limit with the best available weapon[4]. This symbiosis, or full integration in a joint and combined environment, may entail a transformation of pilots into Joint Mission Commanders (JMCs) in a multi-domain scenario. Potentially, these JMCs would have the

3rd, 4th and 5th generation aircraft can train together.

MATC Training Simulation Centre, Pardubice.

capability to exercise distributed Command and Control (C2) of the air battle in their designated area, while simultaneously protecting other assets and assuring air superiority.

While the possibilities are tantalizing, to actually realize such a 'multi-domain' future, it is important that the Alliance carefully considers Tactical Air Training of tomorrow. Furthermore, it will require appropriate Education, Training, Exercise and Evaluation (ETEE) at all levels, from individual to organizational, to include joint competencies, to work together and to do so effectively[5].

Flight Training: Live, Virtual and Constructive

Now that F-35s are attaining Initial Operation Capability (IOC) in many NATO countries, there is an urgent need to introduce the next generation of flight training to get a cost-effective and integrated solution for the users. This integrated training should be comprised of an equilibrium of Live, Virtual and Constructive (LVC) training scenarios and exercises[6], including live adversary air and ground threats, from Operational Conversion Units, (OCU) to Fighter Squadrons. In this context 'Live' stands for a pilot training in an aircraft; 'Virtual' refers to a pilot training in a flight simulator; and 'Constructive' refers to computer (or human) generated entities or effects that support the 'Live' or 'Virtual' domains.

With the introduction of LVC networking between training devices and aircraft, the possibilities for more complex and diversified tactical training have risen exponentially as more entities, team players, simulated threats and Weapon Engagement Zones (WEZ) can be included in training scenarios. Indeed, modern trainers use embedded LVC-type constructs to present the students with radar data and situational awareness in a way similar to what they will see in future cockpits. For example, the F-5, which entered service in Spain in 1970, has been capable of providing Beyond Visual Range (BVR) training through networked system updates. The upgrades include an embedded radar and a warning receiver using data link and, among other safety characteristics, a collision avoidance system. The Live-Constructive employment of advanced features in early assets preserves highly valuable flight hours in the OCU of modern fighters.

Distributed Mission Training via Simulation

The advent of simulation technology has enabled Mission Training via Simulation (MTS) to provide one of the best opportunities to combine future, multinational and advanced tactical training events. As an example, the Multinational Aviation Training Centre (MATC)[7], located in Pardubice, Czech Republic, is a Mission Training Simulation centre driven by a Memorandum of Understanding (MOU).[8] A networked

system of Virtual-Constructive (VC) participants includes eight high fidelity stations with roll-in/roll-out interchangeable throttle and stick controls and configurable displays that can simulate different platforms and enable high-intensity tactical training. The locally networked cockpits replicate either the Saab Gripen or other configurable options for different airframes. Scenarios include VC threats and WEZs for training pilots and Ground Control Intercept (GCI) controllers, ranging from basic two-versus-two BVR to more complex four-versus-many scenarios.

When linked together, Mission Training through Distributed Simulation (MTDS)[9] allows a network of multiplayer and multisite training opportunities, from individual and team participation to full-theatre battles. Mission C2 can be exercised by participants from Combined Air Operations Centres (CAOCs) that can play as training audiences. GCI controllers, Joint Terminal Attack Controllers (JTACS), Duty Officers or even Air Defence Commanders can be involved in large-scale, synthetic scenarios from multiple locations, in real time.

MTDS is a great tool to develop multi-domain unity of action and interoperability through integral, realistic and comprehensive training. Furthermore, simulation may be used as a laboratory for tactical dilemmas, like Anti-Access/Area Denial (A2AD), or for current and/or off-region scenario war gaming, like Baltic Air Policing. If simulation is coupled with Artificial Intelligence (AI), multiple benefits can be obtained. One example of this is an intelligent tutoring system that can generate an event template library. This library, in turn, facilitates the extraction of information about the tactical behaviour of an entity.[10] Additionally, while practicing various tactical mission sets (e.g. Suppression of Enemy Air Defence (SEAD), Ground Attack, Offensive Counter Air (OCA)), the system can gauge the performance of the weapon/sensor combination or effect, such as Electronic Attack, and generate Measures of Effectiveness, (MOEs) related to tactics, shot validation, shot doctrines and Probability of Kill (PK) criteria.

Opposition Forces

NATO live air training is accomplished through major flying exercises, such as Red Flag in the United States, Dissimilar Air Combat Training (DACT) in the Canary Islands, and Iniochos in Greece, as well as through the Tactical Leadership Programme (TLP) course at Albacete Air Base in Spain.[11] These avenues provide unique opportunities for Blue forces to train against advanced, simulated, Red forces. However, opportunities for NATO aircrew to participate in TLP and other air exercises are limited. Moreover, the presence of burgeoning 5th generation aircraft fleets in some of the TLP nations may cause disruptions in the current training community because of aircraft and pilot availability, flight hour costs, security issues and other support factors. These issues will likely impact future multinational training, based on dissimilar platforms, more seriously than today's training among 3rd and 4th generation platforms.

Currently, advanced training requires dedicated and capable opposition forces (OPFOR), which are usually a mix of Red Air and Ground Based Air Defence (GBAD). The TLP has started a dedicated OPFOR Training Program to improve the skills of tactical fighter aircrews in the replication of adversary tactics. The programme is available for those supporting TLP exercises as Red Air, and it is run by a dedicated team within TLP who specialize in OPFOR fighter tactics and GBAD employment (with support from Intel and Air C2 specialists)[12].

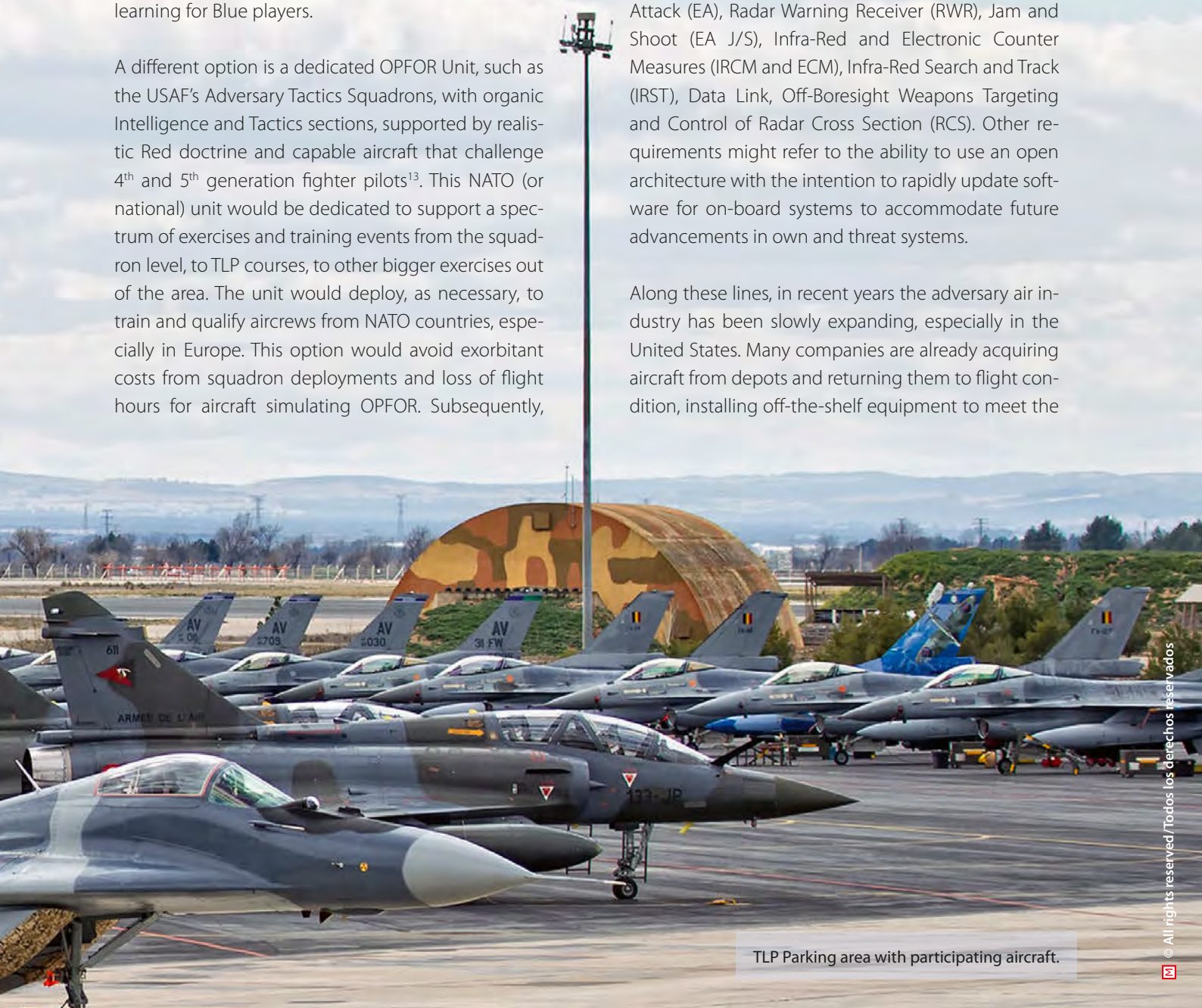
However, this option is not the most efficient solution since Red Air forces are ordinarily played by pilots who are going to attend the course as a Blue audience in the short term. Additionally, there is not always an actual dissimilar aircraft on the Red side, especially with appropriate, dissimilar electronic warfare equipment, which sometimes leads to negative learning for Blue players.

A different option is a dedicated OPFOR Unit, such as the USAF's Adversary Tactics Squadrons, with organic Intelligence and Tactics sections, supported by realistic Red doctrine and capable aircraft that challenge 4th and 5th generation fighter pilots[13]. This NATO (or national) unit would be dedicated to support a spectrum of exercises and training events from the squadron level, to TLP courses, to other bigger exercises out of the area. The unit would deploy, as necessary, to train and qualify aircrews from NATO countries, especially in Europe. This option would avoid exorbitant costs from squadron deployments and loss of flight hours for aircraft simulating OPFOR. Subsequently, OCUs and squadrons would retain the resources needed to concentrate on their assigned missions while the OPFOR Unit would standardize and replicate Red tactics suitable to the threat.

A third option is to outsource OPFOR through a contracted company that provides its own pilots and maintains its own aircraft. This option could be attractive to many Alliance nations because budget cuts, shrinking overall force size and the aging 4th generation fighter jets are limiting the amount of personnel and aircraft air forces have available to replicate Red Air.

Minimum requirements for simulated Red Air aircraft could be defined by users, depending on the fighter squadron to train (4th or 5th generation), but could include Active and Passive Detection systems, Electronic Attack (EA), Radar Warning Receiver (RWR), Jam and Shoot (EA J/S), Infra-Red and Electronic Counter Measures (IRCM and ECM), Infra-Red Search and Track (IRST), Data Link, Off-Boresight Weapons Targeting and Control of Radar Cross Section (RCS). Other requirements might refer to the ability to use an open architecture with the intention to rapidly update software for on-board systems to accommodate future advancements in own and threat systems.

Along these lines, in recent years the adversary air industry has been slowly expanding, especially in the United States. Many companies are already acquiring aircraft from depots and returning them to flight condition, installing off-the-shelf equipment to meet the



TLP Parking area with participating aircraft.

standards for a dedicated Red Air force at a minimum cost. Examples of these aircraft are the A-4K Skyhawk, Northrop F-5B, CF-5D and F-5 E/F, Mirage F1M, Aero L-159E Alca, Atlas Cheetah C and the Kfir.

Conclusion

NATO is preparing for contested environments where a multi-domain approach is required to have the advantage over our adversaries. To that extent, 5th generation aircraft are going to have a decisive impact on the way Air Power is delivered, especially when interoperability issues are resolved. As 5th Generation aircraft enter service in many NATO countries, an advanced and cost-effective training solution will have to be standardized in their Air Forces without sacrificing resources or operational capabilities.

Through common architectures, using machine to machine communication, a virtual operational environment can be embedded to replicate things such as radar, WEZs or data link information of joint and opposition forces. LVC synthetic training has the potential to enhance the quality of training and ensure seamless pilot transitions into 5th generation aircraft. In the near term, these tools can reduce the demand for live F-35 training missions and preserve its costly flight hours for operational use.

Multisession simulation will have to be employed extensively to facilitate advanced integration and joint training, but to get there, we need to have multi-national secure networks in place. Meanwhile, it is beneficial to create centres of MTDS in key training bases to complement and support Tactical Air Training.

Lastly, training in contested environments requires an integrated OPFOR, 'air and surface threat representative', with a standardized doctrine and capable support, dissimilar aircraft, electronic warfare means and dedicated aircrews, all in a cost-effective solution. If developed, future OPFOR should incorporate multi-domain operations, in which Red cyber and space actions influence Blue training in realistic ways. A NATO solution could consist of a new, dedicated 'Red squadron' or a contractor. In the end, the future of our Tactical Air Training will depend largely on how well the Alliance leverages LVC opportunities and how effectively it trains our aircrews against realistic, advanced threats. ●

1. 'If you want peace, prepare for war', Publius Flavius Vegetius. Written in his Epitoma *rei militaris* in the late 4th century AD, is the motto of many NATO squadrons.
2. NATO, Framework for Future Alliance Operations 2018.
3. NATO, Joint Air Power Strategy.
4. Bronk, Justin, 'Maximum Value from the F-35', Whitehall Report 1-16, London: Royal United Services Institute for Defence and Security Studies, (2016).
5. Ibid. 3.
6. Harrigan, J and Marosco, M, 'Fifth Generation Air Combat: Maintaining the Joint Force Advantage', The Mitchel Forum, No. 6 (2016).
7. https://matc.vavyskov.cz/
8. Four nations are the signatories of the MOU; Hungary, Czech Republic, Croatia and Slovakia.
9. Mission Training through Distributed Simulation (MTDS) is a Tier I project to establish a persistent NATO/Multinational MTDS infrastructure to support distributed tactical training through simulation.
10. Interview.
11. The mission of the TLP is to increase the effectiveness of Allied Air Forces through development of leadership skills, mission planning, briefing, tactical air operations and debriefing skills and conceptual and doctrinal initiatives: https://www.tlp-info.org/home/
12. Ibid.
13. Morrison, Brian, 'Is Red Air Meeting Your Needs?' The Journal of the JAPCC, Edition 17, Spring/Summer (2013): p. 63–67.

Lieutenant Colonel Juan Cánovas

joined the Spanish Air Force in 1988 and is a qualified F-18 and F-5M Instructor Pilot. He completed Basic Pilot Training in Spain in 1992, Undergraduate Pilot Training at Vance AFB, United States, and Fighter Weapons course at the 23rd Wing in Spain. He has been assigned as Instructor Pilot in the Fighter Weapons School, 23rd Wing, in Talavera Air Force Base. He also served in the 122 Squadron, 12th Wing at Torrejón AFB, where he flew the EF-18. He has worked in NATO ACC Izmir HQ, TACEVAL Division, as a GBAD and Flying Forces project officer and evaluator. Following the Armed Forces Joint Staff course he was assigned as a Materiel Group commander and Academics and Flying Group commander in the Fighter Weapons School, 23rd Wing, prior to his assignment to the Joint Air Power Competence Centre where he is in the Combat Air Branch as a Manned Air Expert. He has experience in several NATO operations as a pilot and as a battle Staff member.

Iniochos 2019. The quantum leap in air power, the F-35, in a mixed formation with 3rd and 4th generation aircraft, is flying a low pass over the symbol of democracy, the Acropolis of Athens, Greece.

INIOCHOS

The Largest International Military Exercise in Greece for NATO Allies and Partner Nations

By Colonel Konstantinos Zolotas, GRC AF,
Hellenic Air Force Air Tactics Centre (HAFATC) Commander

'I am delighted to be back in Andravida and very proud that we have the U.S. Air Force again participating so significantly in Iniochos '18. This has become an important multinational exercise with broad participation from across Europe and the Eastern Mediterranean, which reflects our vision of Greece as a builder of bridges, as a pillar of regional stability …'
Mr Geoffrey R. Pyatt
United States Ambassador to Greece[1]

The 'Charioteer of Delphi'[2]

The 'Charioteer of Delphi' statue (470 BC), also known as 'Iniochos' (Greek: Ηνίοχος), the rein-holder, depicts the driver of the chariot race at the moment when he presents his chariot and horses to the spectators in recognition of his victory. Despite the importance of the moment, the youth's demeanour encapsulates the moment of glory, and the recognition of his eternal athletic and moral stature, with abundant modesty.[3]

At its inception dating back to the 1980s, 'Iniochos' was established as an annual Hellenic Air Force (HAF) small-scale tactical-level exercise. It was designed to create a realistic training environment for the Hellenic fighter aircraft squadrons tailored to the necessity for training in Composite Air Operations (COMAO) in accordance with Hellenic national defence policy, doctrine plans and tactics.[4]

However, recent decades' battlefield fighting conditions, the emergence of new traditional and non-traditional threats, the effects of globalization, technology advancements, scarcity of resources and climate change, as well as the control of and access to natural resources are some of the factors that are shaping the future physical environment.[5] Identifying the emerging challenges that will dictate the next generation fighter pilots' training needs, and may be driven by the battlefield situational descriptors of complexity and congestion, HAF transformed the 'Iniochos' exercise design in accordance with contemporary battlespace needs. Amongst the many facets of 'Iniochos', this article focuses on the evolution of the exercise overtime by highlighting the key components that make it an essential and unique Invitation Exercise (INVITEX) across Europe and the Eastern Mediterranean.

Docking the Pillars

To provide a 'true' warfighter training for the combat aircrews on a modern, reactive battlefield environment, the HAF developed the design, planning, execution and evaluation of the exercise, inspired by previous lessons learned. From inception to 2013, the exercise execution, and Command and Control (C2) were decentralized, allowing air platforms to operate from both their home bases and remote airfields.[6]

In the last decade, potential adversaries of the Alliance were developing robust Anti-Access/Area Denial (A2/AD) capabilities in response to NATO capabilities.[7] At the same time, many NATO members reduced their defence budgets. Experiencing the effects of defence cutbacks, the HAF was searching for effective solutions for their aircrew training, without sacrificing the quality and maintaining combat training tailored to the new emerging battlefield environment. In 2013, the 'Single Base Operations (SBO) Concept' was adopted. The exercise was upgraded to simulate medium scale Joint Air Power (JAP) operations, including missions across the full spectrum of the air operating domain, and established a demanding exercise battle rhythm to simulate as many 24/7 air warfare operations as possible.

Iniochos 2016. A formation of US Air Force F-15 and Hellenic Air Force F-16s is flying over the Rion – Antirion Bridge (Charilaos Trikoupis), in Patras, Greece.

Single Base Joint Air Operations

The new concept was tested in 2014 in HAF-only format and in April 2015, the HAF decided to launch the exercise as an INVITEX. The invited participants were the Israeli Air Force (IAF), the United States Air Forces in Europe (USAFE) and US Special Operations Forces (SOF) that supported the training with Joint Terminal Attack Controllers (JTACs).

In the past four years, the exercise was held as a two-week INVITEX at the HAF Air Tactics Centre (HAFATC) in Andravida Air Force Base (AFB). It constitutes very significant training event among Allies' & Partners' armed forces, in which JAP operations are launched in a battle rhythm of 24/7, providing a significant Air Level of Effort (Air LoE). The LoE ranges close to 1,000 sorties over the two week period, mainly operating from Andravida AFB.

In order to allow participants to increase joint interoperability, national and international assets from the land and maritime operating domains have also been combined into the exercise.

The 'Chameleon' Concept

After sharing knowledge and gaining considerable experience with high profile Air Powers, the HAF stakeholders identified the need for training in contested airspace operations. The vision of the HAF is to design a 'chameleon' exercise concept, which could be adapted to the training needs across the JAP spectrum while maintaining the individuality and integrity of its exercise.

Air operations are taking place in the Athens Flight Information Region (FIR). The 'chameleon' concept is based on a campaign scenario, which will be adjusted every year according to the current military advancements/developments and threat projection. Additionally, the feedback from participating forces, as well as the lessons learned from previous exercises are consolidated and applied with each iteration.

The scenario is an escalation from a localized crisis over territorial disputes and hybrid warfare to a full-scale international conflict. Consequently, a large flying force will be tasked to operate with maritime and land forces jointly. These will be supported by assets of non-physical operating domains (e.g. electronic warfare and information operations).

The Exercise Key Components

During the 2016 Warsaw Summit Communique, it was described the necessity of NATO developing training and exercises with more realistic, full-spectrum, deterrence focused scenarios by engaging all levels of command – from political to tactical level – employing, as

© Hellenic Air Force

Iniochos 2019. An Italian F-35 is taxing in Andravida Air Force Base in order to depart.

well, tactical live flying.[8] 'Iniochos' stakeholders increased their efforts towards exercise realism investing in better threat presentation, dynamic scenarios and thoroughly precise event assessments which are now key elements of 'Iniochos'.

Realism is augmented through a demanding and high tempo daily battle rhythm, which starts before sunrise and ends after midnight. This allows tactical units to exercise on time-restricted planning and execution, along with their ability to meet the required scenario timeline. Realistic attrition rates are achieved among challenging scenarios which consist of multi-domain threats, real Surface-based Air Defence and live injects. The goal is to replicate the 'Friction of War' effect with the presence of complexity, congestion, degradation, contesting, deception, dispersion, confusion and concealment.[9]

Clausewitz defined 'friction as the only conception that distinguishes real war from war on paper'.[10] The HAF applies the concept by creating a battle environment characterized by imperfect information and constant contention. 'Friction' is the element, which dominates the modern battlefield, stimulating human physical and psychological strengths.

The desired effect is supported by a thorough and precise exercise event assessment which is fulfilled by the qualified instructors of the HAF Fighter Weapons School (FWS), who are employing their expertise along with specialized debrief software. Every mission is reconstructed, and every event is assessed using multiple data sources (on- and off-board sensors, digital data, Global Positioning System [GPS] trackers, Link 16) and specifically designed shot assessment software. The accurate debrief closes the loop of participants' feedback by delivering a reliable and valid training outcome.

The Exercise Descriptors

Increasing realism, combat readiness, and sharing knowledge are the core values of 'Iniochos'. The aforementioned are described by the exercise objectives:

- *Realistic Training employing the most modern and latest updated tactics, in a multi-domain air warfare, enriched with 'live' Surface/Ground-to-Air threats combined with robust Air-to-Air adversaries.*
- *Maximizing the participating aircrews' combat readiness along with their platforms' survivability.*
- *Giving the opportunity to participating aircrews of sharing their background experience, ideas and concerns.*

The missions are supervised by the HAF FWS, which assures that the planning, execution and debriefing phases meet the objectives of the exercise. Missions are executed within a 20-hour daily battle rhythm, in

'Iniochos' simulates the challenges that an Air Expeditionary Force (AEF) faces thus preparing aircrews for a real-world force deployment. Training includes:

- OCA (Offensive Counter Air);
- DCA (Defensive Counter Air);
- ASuW/APCMO (Anti Surface Warfare/ Air Power Contribution to Maritime Operations);
- IADS (Air Ops against Integrated Air Defence System);
- AI (Air Interdiction);
- DT/SCAR/CAS/TST (Dynamic Targeting/ Strike Coordination and Reconnaissance/ Close Air Support/Time Sensitive Targets);
- ISR (Intelligence & Surveillance & Reconnaissance);
- HVAA (High Value Airborne Asset);
- CSAR (either Immediate or Pre-planned).

which three main flying waves and two side missions take place to test Allies' and Partners' physical and psychological strengths.

Figuring 'Iniochos' Importance for Allies and Partners

Apart from the SBO Concept, exercise design also creates a unique training environment for the following reasons:

- *Flying missions are executed in a Notice to Airmen (NOTAM) reserved airspace, which is covered by large areas of high terrain, coastal and deep blue sea in a contested environment with air-to-air and/or fixed or mobile ground/surface-to-air threats, protecting either an area or a route (pop up threats).*
- *Adversaries are Advanced Medium-Range Air-to-Air Missile (AMRAAM) aware 4th gen aircraft employing Beyond Visual Range (BVR) tactics and carrying modern Electronic Warfare and RADAR capabilities.*
- *Opposing forces are always presenting a multilayered Integrated Air Defence System (IADS) employing at the same time long or medium range Surface-to-Air Missile (SAM) Systems, as well as a considerable number of Short-Range-Air-Defence (SHORAD) systems.*
- *Participants train in medium and high threat contested Close Air Support (CAS) and Dynamic Targeting scenarios.*

The campaign scenario is supported by a dynamic flow of information, interconnected events and interdependent missions to promote interoperability, coordination of effort and synergy. By prioritizing and addressing the operational needs to overcome any high threat scenario, the exercise prepares and trains the participants to observe – orient – decide – act and defeat the enemy according to George S. Patton's motto 'you fight like you train'.[11]

British Ambassador to Greece Kate Smith said in a tweet …[12]

'The Iniochos 2018 multinational air force exercise "strengthens the relations of allies and friends". Second day of the multinational exercise Iniochos 2018, including British Typhoons of the Royal Air Force for the first time. British pilots with their colleagues from six countries in an exercise strengthening the relations of allies and friends.'

1. Geoffrey, Pyatt, In 'Ambassador Pyatt's Remarks during "Iniohos 2018" Multinational Exercise'. [US Embassy & Consulate in Greece, News, 2018]. Available at: https://gr.usembassy.gov/ambassador-pyatts-remarks-iniohos-2018/
2. Delphi (formerly also called Pytho), is famous as the ancient sanctuary that grew rich as the seat of Pythia, the oracle who was consulted about important decisions throughout the ancient classical world. Moreover, the Greeks considered Delphi the navel (or centre) of the world, as represented by the stone monument known as the Omphalos of Delphi. It is now an extensive archaeological site, which occupies an impressive site on the south-western slope of Mount Parnassus, overviewing the coastal plain to the south and the valley of Phocis, Greece.
3. Sakoulas, Thomas, 'Charioteer of Delphi', in Ancient-Greece.org, 2019. Available at: https://www.ancient-greece.org/art/chiarioteer.html
4. Hellenic Air Force (HAF), 'History of Iniochos Exercise', in haf.gr, 2019. Available at: https://www.haf.gr/en/structure/htaf/air-tactics-center/iniohos/#hist
5. Allied Command Transformation (ACT), 'Strategic Foresight Analysis', Virginia, Norfolk, 2017. Available at: http://www.act.nato.int/images/stories/media/doclibrary/171004_sfa_2017_report_hr.pdf, (accessed Dec. 2018).
6. Ibid. 3.
7. Schmidt, Andreas, 'Countering Anti-Access/Area Denial'. In: The Journal of the JAPCC, (Ed. 23), Kalkar/Germany, 2016: p. 69–77.
8. Lt Gen Wundrak, Joachim, et al, 'Joint Air Power Following the 2016 Warsaw Summit: Urgent Priorities'. An Allied Command Transformation Headquarters Study conducted by the Joint Air Power Competence Centre, Kalkar/Germany, 2016. Available at: https://www.japcc.org/portfolio/airpowerafterwarsaw/
9. Clausewitz terms 'friction' the 'only concept that more or less corresponds to the factors that distinguish real war from war on paper'. Friction is caused mainly by the danger of war, by war's demanding physical efforts, and by the presence of unclear information or the fog of war (http://www.au.af.mil).
10. Carl von Clausewitz. 'On War', by Michael Howard and Peter Paret (Princeton University Press, 1976). Available at: http://clausewitz.com/readings/OnWar1873/BK1ch07.html
11. The OODA loop is the cycle observe – orient – decide – act, developed by military strategist and United States Air Force Col John Boyd.
12. Kate, Smith, 'British ambassador comments on RAF participation in Iniochos 2018 multinational exercise'. In ERT International news, AMNA, 2018. Available at: http://int.ert.gr/british-ambassador-comments-on-raf-participation-in-iniochos-2018-multinational-exercise/

Colonel Konstantinos Zolotas

is the Commander of the Hellenic Air Force Air Tactics Centre (HAFATC). He graduated from the Hellenic Air Force Academy (HAFA) with a BSc in Aeronautics in 1989. Colonel Zolotas is also studying 'European Civilization' towards a BSc course at the Hellenic Open University (HAP) and is a graduate of the HAF Air Tactics Centre A-G Operations course. He is an F-16 instructor and functional check flight pilot, and he is a command pilot with more 2,500 flying hours in the F-104 and F-16 aircraft. He has served as a director of operations and as commander subsequently in the 347 Fighter Squadron from 2005 till 2009 and 115 Combat Wing's Director of Operations from 2014 till 2016. Prior to assuming his current position, the Colonel served as a staff officer and Head Department at the A1 – Operations Planning Division of the Hellenic Air Force General Staff (HAFGS).

© K_E_N/shutterstock

How can Modelling and Simulation Support Integrated Air and Missile Defence?

By Lieutenant Colonel Andreas Schmidt, DEU AF, JAPCC

Introduction

Modelling and Simulation (M&S) is nothing new, especially for training purposes in the military domain, although the extensive use of Information Technology (IT) has changed opportunities for the use of M&S. In order to be prepared for actual combat, soldiers need to train and exercise their skills to increase their chances of success. Since training with a real adversary is impossible for obvious reasons, simulations are used instead. In the information age, most people think of 'simulation' as computers, sophisticated mathematical equations and people in lab coats. But simulation is and can be so much more, that is, as long as the tools are correctly understood and used. The following article will look at M&S basics, how the military can benefit from simulation and why M&S tools need to be used quite carefully.

Figure 1: Generic development of a model.

What is Modelling and Simulation?

Simulation is realistic modelling, as much as is possible, of events in reality[1]. In order to better comprehend simulation, it is beneficial to have a good understanding of the terms 'modelling' and 'system'. According to P. Sanchez (2007)[2], a 'system' is a set of elements interacting with each other, and a 'model' is a system which can be used as a surrogate for another system. Therefore, simulation is the process of using a model or models to study the behaviour of a system or system of systems. A system could be an aircraft or Surface Based Air and Missile Defence (SBAMD) unit, and an M&S equivalent could be an F-35 flight simulator or an S-400 mock-up[3]. There are numerous reasons why the use of models has advantages over using the original system. In terms of training, flight simulators are cheaper to operate than real jets, and S-400 mock-ups are easier to purchase and employ than the real system. However, there are also various reasons why we need to be careful in using these models. The development of a model follows a very deliberate path, and we need to know which demands the model needs to satisfy to qualify as a realistic model (see Figure 1). Hence, the use of the model outside of these demands will very likely not produce the desired results.

The three framing parameters of model development are[4]:

- *Resolution:* The degree of detail and precision used in the model;
- *Aggregation:* The ability to group entities while preserving the effects of entity behaviour and interaction while grouped;
- *Fidelity:* The accuracy of the model.

Obviously, a model system cannot represent 'all possible' requirements, otherwise it would be the real system. The real and full experience of flying a Eurofighter can only be achieved by flying a Eurofighter, but perhaps the model only needs to satisfy a certain subset of 'all possible' requirements, like realistically representing switches and displays of an F-35 or PATRIOT engagement control station. Thus, the creator of a model needs to have, and be aware of, the finite set of requirements necessary to develop a satisfactory product. Consequentially, the resulting system model can only be successfully used to service these requirements. Any use of the simulation outside of these specifications will likely cause an unrealistic and unsatisfactory result. Worse yet, if unaware of the initiating requirements, it could provide an incorrect interpretation of the results. This, in turn, might result in erroneous conclusions or an unwarranted mistrust in simulation tools. So, simulation is an outstanding tool when used as intended, and within its design parameters.

Although a 3D model of an F-16 for a wind tunnel test or sandbox wargames technically qualify as a 'simulator' for M&S purposes, in the following paragraphs we will focus on characteristics of IT-aided simulations. In general, there are several taxonomies for classifying models and simulations. One of the most common categorizes the level of interaction with a human[5]:

- *Live:* A simulation involving real people operating real systems;
- *Virtual:* A simulation involving real people operating simulated systems;
- *Constructive:* A simulation involving simulated people operating simulated systems. Real people stimulate such simulations, but are not involved in determining the outcomes.

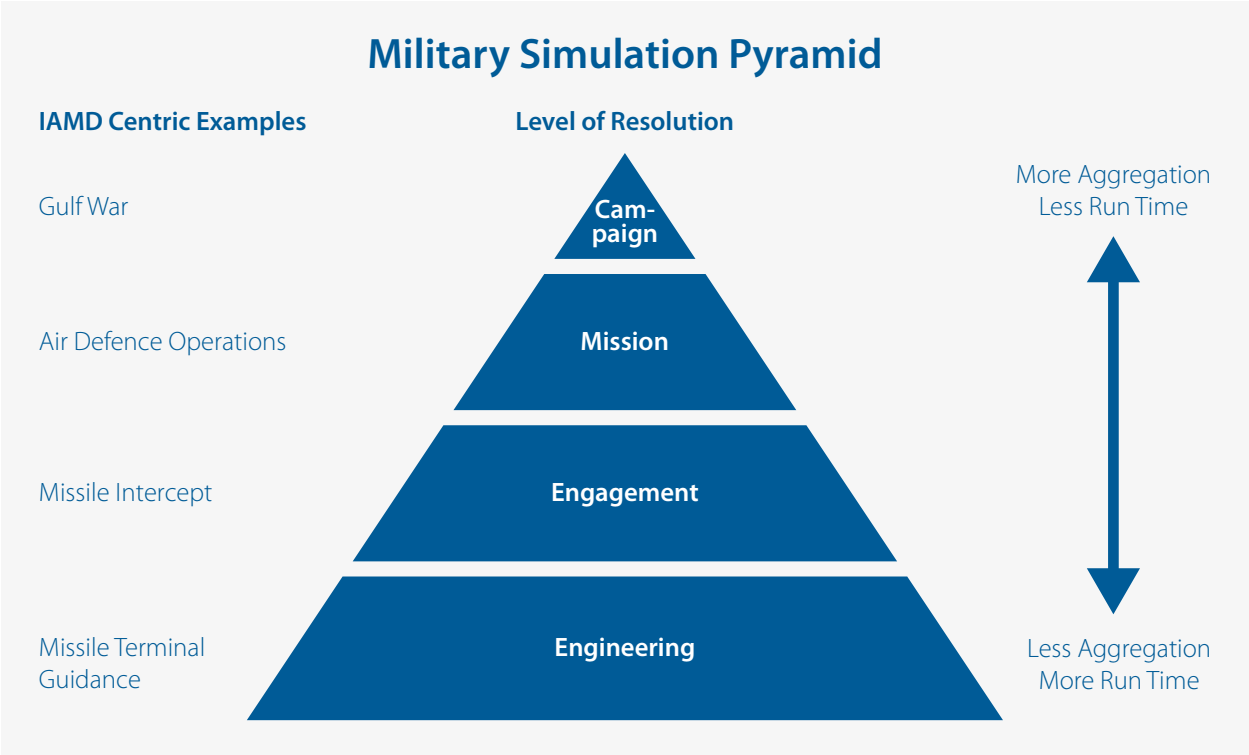


Figure 2: Reflection of IAMD on the military M&S pyramid.

In execution, there can be mixed variants of all three of these categories to satisfy set demands. Simulations using Hardware in the Loop (HWIL) constructs[6] are a hybrid of Live and Virtual, exploiting the benefits of both categories. Another way of distinguishing simulations is by the level of resolution. Figure 2 shows an exemplary projection of Integrated Air and Missile Defence (IAMD) on the military modelling and simulation pyramid.[7] Higher levels on the pyramid allow for more aggregation, and lower level tend to show higher resolution.

Some simulations can be executed in a continuous and dynamic fashion in real time, representing regular operations, while others are done in a more analytical fashion (e.g. using the Monte Carlo method[8]) mostly in non-real-time with little observability. For that, it is essential the simulator adequately process all qualitative and quantitative inputs necessary to produce an output with the desired value. All parts of the simulation need to be fine-tuned to achieve the desired result. The inputs must match the model's resolution and fidelity to achieve usable outputs.

Another distinguishing parameter of many simulators is their capability of being embedded in a network with other simulators, or used in a standalone fashion. For NATO IAMD, highly networked operations are inherently crucial. Hence the capability of accurately portraying that capability in an M&S environment is essential. To be able to connect multiple simulators, some of their input/output and means of transmission need to be standardized. Obviously, operational Data Links (e.g. Link-16[9] or JREAP-C[10]) are available, but a data exchange format is also necessary that allows a gainful stimulation of all connected simulators. Currently, two standards are widely used: Distributed Interactive Simulation (DIS) (Distributed Interactive Simulation v7 IEEE Standard 1278.1) and High-Level Architecture (HLA) (High Level Architecture IEEE Standard 1516). DIS was developed in the early 1990s and was supposed to be succeeded in NATO by HLA in 1998. Instead, DIS was amended for new demands in 2010 (e.g. Direct Energy effects or Mode 5 Identification Friend or Foe [IFF]) and is still in use by the Alliance. Regardless of which standard is used, the simulation link needs to be able to support all current

and future demands, so it has to be updated continuously so that the simulations will not be stifled by an out-of-date interface.

A conglomerate of simulators working together can also be seen as one big simulation with high resolution and low aggregation, but bound by the same fundamental question. Does this 'super' simulation fulfil all requirements to achieve sufficient accuracy for the anticipated product? Just because it is technically feasible, does not mean it warrants the effort to do so, when a different simulator might give better results. For campaign-level analysis, constructive models with a higher level of aggregation and statistically portraying lower level units are more suitable than large networks of individual simulators.

Also, and especially with military simulators, the classification of input/output data and the model itself are fundamental aspects which will have a significant effect on how the simulator can be employed. For NATO, this requires information sharing agreements be in place before the whole effort can be initiated.

M&S in Support of NATO Education, Training, Exercise and Evaluation

The baseline education and training of national capabilities is the responsibility of each Alliance nation. NATO's concept of Education, Training, Exercise and Evaluation (ETEE) is a logical build-up from individual training to collective exercises, concluding with evaluations to reliably create and sustain the necessary joint and synergetic capabilities and capacities for NATO operations.

During this whole process, simulators can not only contribute significantly to save time and resources, therefore increasing overall efficiency, but also create new training options that would otherwise not be available. Simulation allows NATO to reduce ETEE efforts to necessary focus areas. This could be done with real systems that possess a simulation environment with all essential models and interfaces, or with dedicated simulation tools. If an operator needs to learn or improve his skill on his respective console, simulation tools can take care of everything behind the Human-Machine Interface (HMI). For example, for console training of a Tactical Control Officer (TCO) of a SBAMD unit, it is not necessary to use a fully-employed weapon system, and for a pilot, it is not required to have the HMI 10,000 metre in the air. For the console training of higher-level headquarters, it is not necessary to employ all subordinate units, as most units can be portrayed mainly with adequate simulators or models and reduced to a needed minimum.

One of the core paradigms of military training is 'train as you fight'. Since the ETEE environment should be a sufficient depiction of real-world circumstances, it should also reflect full NATO missions, or coalitions of the willing, with or without non-NATO nations. Here, classification issues become relevant very quickly. In other words, weapon systems, simulators and networks might need to be able to work in various classification environments. Currently, NATO has the option to use the Combined Federated Battle Laboratories Network (CFBL Net) for simulation purposes outside of the NATO secret network as a standing capability for IAMD training. A simulation tool which reveals information with higher classification or too many technical details might only be suitable for a small subset of audiences. This implies that not only national demands for models need to be met but also all potential networked arrangements as well. For an exercise like Joint Project Optic Windmill (JPOW), it is of little importance to have a high-fidelity, six-degrees-of-freedom depiction of an interceptor missile transposed on the Link-16 and DIS network. Lower fidelity (e.g. three degrees of freedom models, sanitized flight paths) with a statistical representation below a releasable threshold are sufficient and help the integration of all anticipated players. A portrayal of all entities in the same simulated threat environment is one of the main benefits. This also helps in designing the network required for such an exercise. Apart from simulation-specific issues, the integration design should reflect the actual mission requirements of such a player audience quite well, which should help when doing the same thing in a real mission. The connection of real and simulated systems in one distributed network will create the needed synergy without the need for a centralized system deployment. Furthermore, it reduces the need for real weapon systems, which are a scarce commodity, to a

© US Air Force, Airman First Class Michael S. Dorus

necessary minimum. Of course, the systems/simulators require network connectivity with adequate bandwidth, latency and encryption.

Depending on the ETEE audience (e.g. a Unit-level Force Evaluation or Joint Force Command Major Joint Operations exercise), it is essential to define the framework and focus of what needs to be simulated to find the appropriate model(s). If we are still in the phase of learning, improving or experimenting, simulation creates outstanding options for trial-and-error, learning-by-doing and step-by-step improvements in an environment of high attrition or overmatch. Besides, in a simulation, it is easier to change the circumstances (e.g. doubling the red forces or increasing/decreasing own resources) to give the training audience the broadest spectrum possible. This helps identify how robust certain procedures are, and to identify the need for contingency plans.

Not only can M&S representations of enemy forces be the easiest way of interfacing with them outside of the battlefield, but surely the most adaptable, so that these models can be used for a broad spectrum of use-cases. In general, it is much easier to portray adversary forces within a defined, controlled and repetitive environment. From testing and refining Tactics, Techniques and Procedures (TTPs), to simulations with a more experimental character, the following exemplary disciplines can be supported by M&S tools:

- developing policy;
- analyzing resilience of own capabilities;
- identifying capability gaps;
- optimizing defence plan/design robustness.

Also, a conflict with high attrition rates on both sides can only be trained within a simulated environment. Since peer, near-peer and proxy conflicts appear to be or become the current focus, an M&S environment seems to be the safest, cost-effective and best way of evaluating such situations.

Other Areas M&S can Support and Create Synergy

As stated before, simulation is nothing new and is already present in current various NATO Air Command and Control (C2) processes. For IAMD, a simulator is

used to evaluate potential defence designs. As a recent example, for a current threat study, NATO used a campaign and mission level simulator to validate standing plans and identify potential gaps or weak points. A prevalent discussion in the M&S community is about what kind of weapon system data is needed (red and blue) to draw viable assumptions and conclusions. Since most defensive weapon systems and enemy weapons data underlie national disclosure restrictions, it is complicated to create a high-fidelity database for NATO simulations. However, just because the data does exist to support a certain degree of fidelity, does not imply that it is actually needed to create the desired output.

M&S can support the procurement process of new systems from the initial decision to its final integration. Integrating and optimizing a model, and reflecting identified military needs in a simulated operational environment with representative models of existing systems, can support refining the actual requirements. It has proven beneficial to have users hands-on during the development to stay true to these requirements. Also, through the use of simulators, the development of operational concepts and TTPs can be started before the hand-over of the system to the user occurs. By developing and amending such models right from the beginning, they can be used later on for other purposes mentioned above.

Simulation and Artificial Intelligence

Artificial Intelligence (AI) is one of the current buzzwords in computer science and one of the leading trends of ongoing global research. In the context of M&S, it can be described as a model for problem-solving and decision-making in various processes. The problems are not being solved based on predetermined algorithms, but rather based on a dedicated learning process that creates a model for optimized decision-making. Of course, M&S environments can serve to train certain AIs. Currently, NATO is discussing how to incorporate AI in AirC2. Once it is incorporated, it must be reflected in any model or simulation of NATO AirC2. Otherwise, the model will rarely produce realistic results. For the portrayal of adversary forces, AI could be trained to reproduce adverse behaviour in a controlled fashion, which could, for example, reduce the need for large red force player groups during exercises. Since it

can be assumed that potential adversaries are also developing AI for their military purposes, and the employment of AI might create a new paradigm in warfare, this also needs to be reflected in our M&S to have a successful depiction of the enemy.

Conclusion

M&S is much more than just another beneficial tool for *affordable and realistic* IAMD training. It is a keystone element for the overall mission success of NATO and the gateway for affordable and realistic training. The proper use of M&S can support various IAMD facets; from system procurement to operational evaluations. For the Alliance, to be able to use M&S to a maximum extent, several things need to be available:

- A clear understanding, on all applicable C2 levels, of simulation requirements and/or possibilities:
  - resolution, aggregation and fidelity;
  - quality/quantity of input/output, observability;
  - thorough description of model accuracy, limitations and possibilities.

- Flexible and adaptable simulation environments:
  - data link networks and up-to-requirement simulation link networks;
  - options for distributed simulation and integration.

- Up-to-date NATO simulation standards:
  - simulator network interfaces;
  - standards for input and output formats.

'Modelling and Simulation is much more than just another beneficial tool for affordable and realistic IAMD training. It is a keystone element for the overall mission success of NATO and the gateway for affordable and realistic training.'

- Information sharing concepts, tailored to simulation demands:
  - What is needed?
  - What can be provided?

In general, the use of M&S tools for NATO has to be a coordinated effort between NATO, NATO nations and industry. Also, knowledge about the general use, benefits and limitations of simulation needs to be broadly spread throughout NATO to increase the correct usage of M&S, and to take full advantage of its benefits. For NATO ETEE alone, it could create a more cost-effective, streamlined environment, always moulded for the respective training audience. ●

1. Gabler Wirtschaftlexikon 19 Feb. 2018: https://wirtschaftslexikon.gabler.de/definition/simulation-43833/version-267158
2. https://www.informs-sim.org/wsc07papers/007.pdf
3. A full-sized structural model built to scale chiefly for study, testing, or display.
4. US DoD Modelling and Simulation Glossary, 1 Oct. 2011.
5. Ibid. 4.
6. E.g. Integration of real PATRIOT weapon systems in the exercise Joint Project Optic Windmill (JPOW).
7. Modelling and Simulation at APL, James E. Coolahan, 2003.
8. https://mathepedia.de/Monte-Carlo-Methode.html
9. https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1235/MR1235.chap9.pdf
10. https://www.airforce-technology.com/news/newsusaf-evaluates-new-joint-range-extension-applications-protocol-c-system-4182741/

Lieutenant Colonel Andreas Schmidt

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

Improving Ballistic Missile Defence Interoperability

By Cadet Richard King,
US Air Force Academy

Introduction

NATO leaders announced at the 2010 Lisbon Summit that the Alliance would expand its Active Layered Theatre Ballistic Missile Defence (ALTBMD) capabilities 'to provide full coverage and protection for all NATO European populations, territory, and forces'.[1] This shield will eventually span all NATO European territory and must be capable of reacting to threats on extremely short notice. It would include a few NATO owned capabilities, such as the Ballistic Missile Defence Operations Centre (BMDOC), connected to a multitude of nationally owned sensors and interceptors, including land-, maritime-, and space-based systems. Furthermore, NATO Ballistic Missile Defence (BMD) and Theatre BMD (TBMD) is only one part of the Alliance's Integrated Air and Missile Defence (IAMD) mission, meaning these wide-ranging BMD capabilities must be able to operate within the NATO IAMD System (NATINAMDS) as well. Considering these issues, interoperability in BMD is critical for crisis management and the collective defence of the Alliance.

© MDA Photo

Aegis Ashore Missile Defense Complex in Devesulu, Romania.

This article begins by outlining the desired end state for NATO BMD interoperability, continues by exploring the current state of the capability, and finishes by recommending some ways in which NATO can evolve to achieve this end state. NATO BMD has already declared Initial Operational Capability (IOC) and is slowly growing as more nations contribute sensors and interceptors, and interoperability is key for effectively utilizing these platforms. NATO BMD will develop better if the Alliance focuses on the three dimensions of interoperability: technological, procedural, and human. First, member states should purchase platforms that can technologically interoperate with other NATO IAMD platforms and should emphasize the multinational procurement of new BMD assets. Second, NATO should incorporate more strategic level BMD considerations into multinational IAMD exercises and should standardize procedural aspects of BMD, especially the coordination with TBMD. Third, NATO should facilitate the acculturation of BMD personnel through BMD and IAMD courses, summits, and conferences. By focusing on these areas, NATO can move from its current state to an end state that ensures a BMD system that maximizes the effectiveness of platforms under its command and operates as a key contributor within NATINAMDS.

Desired End State

The 2016 Warsaw Summit Communiqué reaffirms the aim of NATO missile defence in general as 'full coverage and protection for all NATO European populations, territory, and forces.'[2] However, this article focuses specifically on the interoperability aspect of NATO BMD. The end state for this particular context has not been comprehensively defined by NATO; however, one can conclude that it must be flexible enough to match the improving capabilities of NATO BMD as the Alliance moves closer to full coverage and that it must be appropriate for the current and near future BMD-related threats in an IAMD environment. That being the case, this article defines the desired end state as a NATO BMD system mature and robust enough to fully utilize all available sensors and interceptors and operate fluidly as part of NATINAMDS.

Current State

Command and Control

Announcements within the past decade about the NATO BMD Command and Control (C2) structure

provide one element by which to gauge the current state of BMD interoperability. While C2 is important for all operations, it is particularly vital for BMD to properly function, as sensors and interceptors are nationally owned and spread across vast geographical distances. At the 2012 Chicago Summit, just two years after announcing the decision to pursue Alliance-wide BMD coverage,[3] NATO leaders announced that Interim Ballistic Missile Defence Capability had been achieved. Part of this achievement included the installation and testing of C2 capabilities at Headquarters Allied Air Command in Ramstein, Germany.[4] Four years later at the Warsaw Summit, Alliance leaders announced that NATO BMD had reached IOC, part of which would include the transfer of C2 for the new US Aegis Ashore site in Romania to NATO.[5] Additionally, Spain currently hosts four US Aegis ships, Turkey hosts a US missile defence radar system, the Netherlands and Denmark have decided to procure radar-equipped frigates, the UK is investing in a ground-based radar system, and Poland has agreed to base a US Aegis Ashore system.[6] Each of these contributions are currently part of or planned to be part of NATO BMD.

Interoperable Technology

Another area of concern for NATO BMD is the procurement of interoperable technology. To better provide for crisis management and collective defence, Allies should ensure their BMD platforms have the technical ability to interoperate as part of NATINAMDS. Most NATO members have continued to purchase sensors and interceptors that can work as part of the Alliance BMD structure. Even systems intended for national use can also be used by NATO when needed, and interoperable systems simplify this process. For example, since 2013 Germany, Italy, Spain, the Netherlands, and the United States have all provided short-term augmentation to NATO BMD capabilities in Turkey by providing PATRIOT and ASTER SAMP/T batteries, which are plugged into Allied Air Command at Ramstein, to defend against Syrian short- and medium-range ballistic missile threats. These assets are provided temporarily, and will afterwards return to national use.[7] NATO leaders have recently raised alarm, however, about Turkey's purchase of four S-400 batteries from Russia. Unlike the PATRIOT or ASTER SAMP/T, the S-400 will likely not be allowed to integrate into the NATO missile defence structure. This raises concern over the implication of NATO members procuring platforms that will not be permitted to plug into NATINAMDS and has led to unease among some NATO members.[8]

Multinational Exercises

A third element comprising current BMD interoperability is the relevance of exercises conducted by NATO or by groups of member states. A number of exercises related to BMD currently exist, some of which include Joint Project Optic Windmill (JPOW), Steadfast Alliance, Steadfast Armor, and Nimble Titan. JPOW is especially notable because it offers the opportunity to experiment and develop new methods of employing missile defence, which has led to the development of new tactics, techniques, and procedures (TTPs) and NATO doctrine.[9] These exercises, however, are mainly limited to the tactical and operational levels of conflict and lack strategic focus, despite BMD being a primarily strategic mission.

Lines of Effort

NATO doctrine defines three dimensions of interoperability: technological, procedural, and human.[10]

Technological

One way to improve interoperability is for nations to purchase systems that are technologically capable of interoperating with one another. This does not mean that all member states must acquire the same equipment, as NATO doctrine clarifies, 'Interoperability does not necessarily require common military equipment. What is important is that this equipment can share common facilities and is able to communicate with other equipment'.[11] As mentioned previously, Turkey's purchase of S-400s from Russia has raised concern among Allies, particularly the United States. Analysts worry that connecting the S-400 to other Turkish platforms, such as the F-35 could expose vulnerabilities.[12] While nations are free to procure whatever military equipment they see fit, logic dictates that it is more

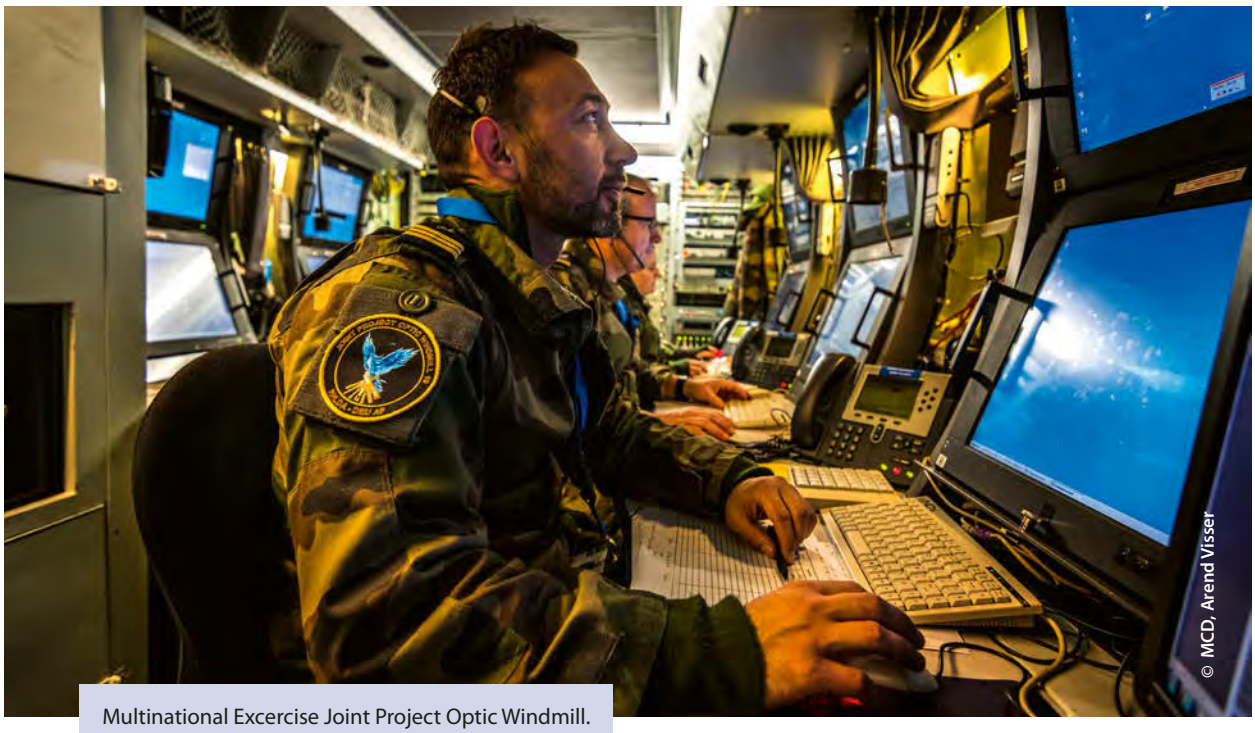
beneficial for collective defence if Allies procure equipment with the ability to technologically interoperate within NATINAMDS.

Multinational procurement offers another avenue by which to improve technical interoperability. NATO leaders included a paragraph in the 2014 Wales Summit Declaration: 'We note the potential opportunities for cooperation on missile defence, and encourage Allies to explore possible additional voluntary national contributions, including through multinational synergies in planning, development, procurement, and deployment.'[13] Multinational procurement splits the research and development costs of expensive systems among Allies, and by working together to acquire and operate missile defence technology, involved parties can maximize usage and share technical expertise.

Procedural

Procedural interoperability could be improved by developing an IAMD exercise that incorporates multinational BMD personnel at all levels of conflict. Although JPOW and other exercises involve multiple NATO and partner-nations and are effective at training multinational personnel to work together at the tactical and operational levels, they do not receive enough consideration from the upper levels of military-political leadership. BMD is primarily a strategic problem, meaning leaders at that level must also get involved during relevant multinational BMD exercises.[14] One useful avenue to gain this experience are BMD Distinguished Visitor programs, which are currently conducted to inform and educate political and military leadership.

From threat identification to interceptor firing, the BMD mission involves all levels and incorporates both NATO and national systems. The ability to seamlessly transition thus requires standardizing aspects of procedural interoperability, such as shared TTPs and a common language. Exercises, JPOW in particular, have led to the development of TTPs, but care must be taken to ensure these remain up-to-date and applicable to the most current threat assessments determined by NATO. To better integrate BMD throughout Alliance IAMD, NATO must develop sufficient guidance and publish Standardization Agreements (STANAG) to allow for better integration and a list of common acronyms related to BMD. Doing so will simplify interoperability and thereby reduce friction during BMD operations.[15]



Multinational Excercise Joint Project Optic Windmill.

Human

Human interoperability is critical for ensuring those serving in BMD positions can work together while spread across the entire NATO European territory. Acculturation into the BMD mission allows personnel to better operate with one another. NATO needs to increase opportunities for BMD personnel to attend exercises, summits, and courses, such as the NATO Ballistic Missile Defence Course and the Surface Based Air Defence course at the NATO School in Oberammergau. Providing opportunities for NATO to come together can enable better communication and understanding of how different nations operate. Two researchers at the US Army War College Strategic Studies Institute warned that 'given differing threat perceptions and declining defence budgets, it seems very likely that tangible Alliance contributions, in the form of sensors and interceptors, in particular, will remain minimal over the next decade.'[16] Better communication and understanding can help bridge this gap in perceptions, thus allowing NATO BMD to interoperate more effectively through the Alliance.

Conclusion

NATO BMD is currently in a phase of expansion, as Allies continue to contribute sensors and interceptors until full coverage is achieved. Interoperability is key for proper function of NATO BMD due to its unique nature, as defined by the geographical dispersion of platforms, the national ownership of hardware, and BMD's role within NATO IAMD. By focusing on the technological, procedural, and human aspects of interoperability, NATO can improve the efficiency and effectiveness of its BMD assets. Specifically, this should involve the purchase of technologically interoperable systems as well as increasing multinational procurements. Additionally, member states should ensure the strategic level is appropriately involved during BMD exercises. Also, the Alliance should publish more guidance to procedurally standardize NATO BMD. Lastly, NATO leadership should support providing means, such as courses and exercises, to acculturate personnel into the NATO BMD mission. Doing so will drive NATO BMD interoperability to the point that the Alliance is maximizing the utility of its platforms and seamlessly operating within NATO IAMD. ●

1. Lisbon Summit Declaration. 20 Nov. 2010.
2. Warsaw Summit Communiqué. 9 Jul. 2016.
3. Lisbon Summit Declaration.
4. Chicago Summit Declaration. 20 May 2012.
5. Warsaw Summit Communiqué.
6. 'Ballistic Missile Defence,' (15 May 2018), https://www.nato.int/cps/en/natohq/topics_49635.htm, accessed 6 Jul. 2018.
7. NATO Public Diplomacy Division, 'Augmentation of Turkey's Air Defence,' (Jan. 2017), https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_01/20170113_1701-factsheet-patriot_en.pdf, accessed 9 Jul. 2018.
8. Reuters Staff, 'U.S.'s Pompeo Presses Turkey on S-400 Missiles Purchase from Russia', Reuters (27 Apr. 2018), https://www.reuters.com/article/us-nato-foreign-usa-turkey/pompeo-presses-turkey-on-s-400-missiles-purchase-from-russia-idUSKBN1HY2A6, accessed 4 Jul. 2018.
9. Andreas Schmidt (JAPCC Ballistic Missile Defense Subject Matter Expert) in interview with author, 5 Jul. 2018.
10. NATO Standardization Office. 'NATO Standard AJP-01 Allied Joint Doctrine' (Feb. 2017).
11. NATO Public Diplomacy Division. 'Backgrounder: Interoperability for Joint Operations' (Jul. 2006).
12. Valerie Insinna. 'US Official: If Turkey Buys Russian Systems, They Can't Plug into NATO Tech,' Defense News, (16 Nov. 2017), https://www.defensenews.com/digital-show-dailies/dubai-air-show/2017/11/16/us-official-if-turkey-buys-russian-systems-they-cant-plug-into-nato-tech/, accessed 6 Jul. 2018.
13. Wales Summit Declaration, 5 Sep. 2014.
14. Interview with Andreas Schmidt.
15. Ibid.
16. Steven Whitmore and John Deni, NATO Missile Defense and the European Phased Adaptive Approach: The Implications of Burden Sharing and the Underappreciated Role of the US Army (Carlisle Barracks, Pennsylvania: United States Army War College Press, 2013).

Cadet First Class Richard King

is currently attending his final year at the US Air Force Academy in Colorado Springs, Colorado, where he is majoring in Military and Strategic Studies and minoring in German. He spent summer 2018 at the JAPCC conducting interviews and doing research about the role of NATO IAMD in Alliance cohesion. During the course of researching this article, he met with representatives from the Competence Centre for Surface-Based Air and Missile Defence, US Air Forces – Europe, the European Integrated Air and Missile Defense Center, 10 AAMDC, NATO Allied Air Command, CTF-64 and the 603rd Air Operations Center.

The Rise of Consumer Drones Threat

By Dr. Claudio Palestini, Emerging Security Challenges Division, NATO HQ

Introduction

Unmanned Aircraft Systems (UAS), more commonly referred to as drones, have been one of the most rapidly advancing technologies developed in the last decade. While remotely-piloted aircraft have been traditionally used by the military and, on a lower scale, by other professional communities and aero-amateurs, UAS technology has experienced an incredible commercial momentum gain over the last five years. This is due to extraordinary technological advances, the rise of sophisticated but low-cost products and the emergence of a vibrant community of users, as well as businesses that are developing new applications in this field.

As a result, the UAS market has grown exponentially in the recent years, from USD 4.5 billion in 2016, to USD 17.82 billion in 2017 and to the expected volume of USD 100 billion by the year 2020.[1] The US Federal Aviation Authority has estimated that there will be more than 1.2 million drones by the end of 2018 in the US, with an annual growth rate of around 40 %.[2] In Europe, experts from Airbus predict that, by 2035, the skies above Paris will be filled with around 20,000 UAS per hour.[3] From the technology point of view, new trends like swarming, autonomy, better endurance and higher payloads, night vision and more integrated and compact sensors are on the horizon.

While these technologies open outstanding possibilities, these developments have not gone unnoticed by criminals, who have started to use this technology for illegal purposes. Even more threateningly, terrorists have increasingly misused consumer and recreational UAS to plan, prepare and execute attacks on Allies and partners' forces. For example, several open-source reports have proven the capability of terrorist groups, like the Islamic State (IS), to customize Commercial Off-The-Shelf (COTS) technology and to weaponize both fixed-wing and rotary-wing UAS.[4] On the civilian side,

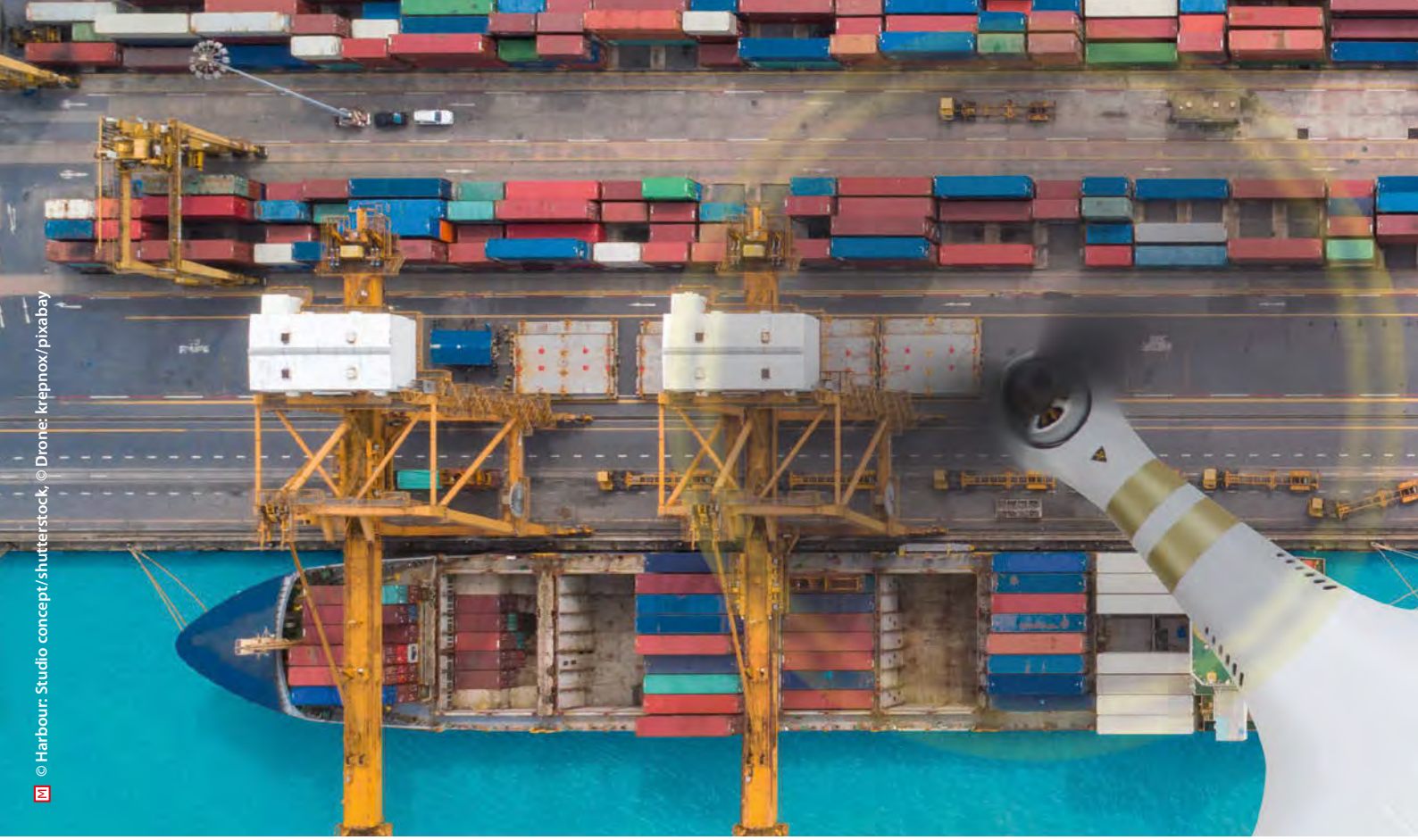
recent events at Gatwick Airport demonstrated the capability of a small commercial UAS to induce a complete shutdown of an airport, causing the cancellation of several flights and the loss of tens of millions GBP. At the same time it generated vast media attention.[5]

Challenges to Allies and Partner Nations

Terrorist misuse of UAS poses a number of challenges to Allies' and partner nations' preparedness both in theatres of operations and in their own homelands. These challenges stem from the asymmetric nature of the threat and can be grouped in three main areas: technological challenges, cost-effectiveness and rules of engagement.

Technological Challenges. From the technological point of view, coping with this threat encompasses a number of challenges throughout the entire kill chain (detection, identification, tracking, engagement and finally exploitation of any information extracted from the captured UAS for intelligence purposes). From the detection point of view, traditional radars are typically designed to target large and fast-moving objects and are ill-suited to detect Low, Slow, Small (LSS) UAS, which are filtered out due to their low radar cross-section. Additionally, low-altitude UAS can escape detection by hiding within the environment and behind buildings, trees or other objects. Finally, radio-frequency detection systems are based on libraries of known UAS signatures, but these can become ineffective in case of UAS with customized command and control features. The advent of the Internet of Things (IoT) and 5G technology, which will open up the possibility to operate UAS via the internet from everywhere in the world, will make radio-frequency detection techniques useless and the detection challenge even more complicated.

From the engagement point-of-view, radio-frequency countermeasures, like jammers, could turn out to be ineffective in cases where UAS fly with automatic flight patterns and use inertial navigation systems or visual aided navigation. Furthermore, consumer UAS, as well as other commercial-based technologies, are progressing at a pace faster than traditional military capability development, making it difficult for military forces to ensure the availability of effective countermeasures in a timely fashion. In this scenario, only a scalable, integrated, multi-layered system of systems is likely to be effective.



© Harbour: Studio concept/shutterstock, © Drone: krepnox/pixabay

Cost-Effectiveness. On the other hand, considering cost effectiveness, challenges arise as these Counter-UAS (C-UAS) systems are typically much more expensive than the threat itself, making unpractical the widespread adoption of sophisticated and expensive capabilities to counter low-cost and fast-evolving threats.

Rules of Engagement. Finally, defining rules of engagement for countering misuse of UAS is also an issue, as there is a need to consider a number of risks when operating these systems: potential collateral damage, coordination with civilian agencies and sharing of responsibilities with host-nation authorities. This is especially important in urban environments where use of countermeasures could impose risks on the civilian population.

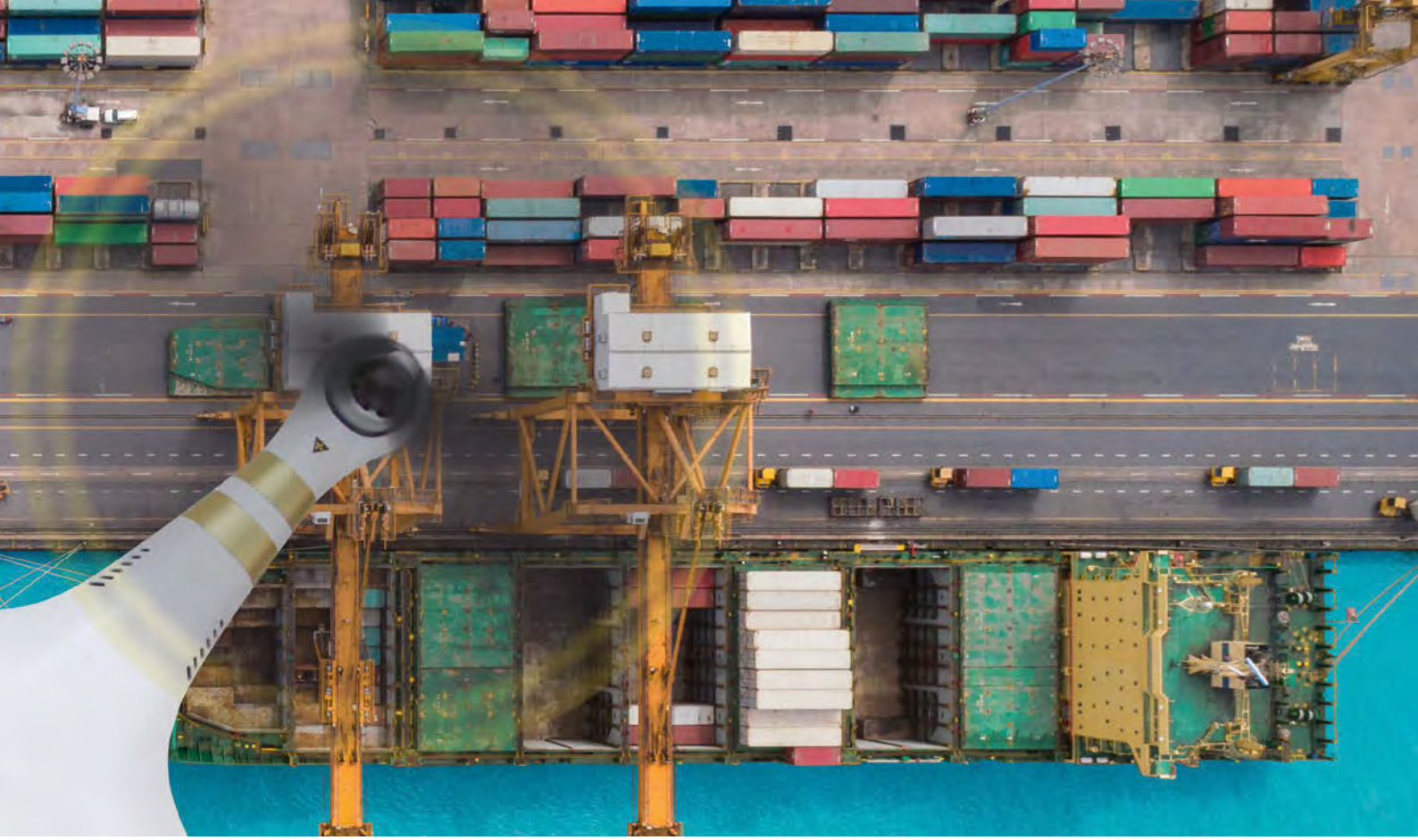
Recommendation

Accordingly, development efforts are needed in several areas, including testing and deployment of innovative capabilities to cope with the challenges above. These efforts should span across the full spectrum of Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities and Interoperability (DOTMLPFI) and should consider the entire kill chain. It is clear that such an effort would require access to several areas of expertise and different communities within Allied nations. For this reason, a cross-dimensional approach has been proposed within NATO and recently endorsed at Defence Ministerial level.

Conclusion

Recognizing that preventing, protecting, and recovering from such attacks requires a coherent and holistic approach, NATO Defence Ministers have endorsed at their meeting in February 2019 the establishment of a practical framework to C-UAS with the objectives of supporting the development of capabilities by Allies and bringing coherence to NATO's current ongoing efforts.

The practical framework is intended to be developed in a short time frame to cope with a very rapid technological lifecycle and aims to include a continuous



effort of research, development and exercises, leveraging national, multinational and NATO ongoing activities. This will allow personnel to be trained to experiment and exercise countermeasures with detection, identification, tracking and engagement systems in field conditions. Ultimately this will ensure interoperability and serve as a proof of concept for fielding an integrated and comprehensive C-UAS capability.

The Emerging Security Challenges Division in NATO is managing the Defence Against Terrorism Programme of Work (DAT POW) and is supporting the execution of this framework with a number of initiatives and exercises to be carried out in the near future. These include the comparative analysis between non-lethal and lethal effectors to counter LSS UAS, the demonstration of an integrated system for the management and detection of cooperative and non-cooperative UAS, and the demonstration of a new cognitive radar technology to improve detection in urban areas.

1. https://www.dronethusiast.com/commercial-drone-market/
2. https://www.faa.gov/data_research/aviation/aerospace_forecasts/media/Unmanned_Aircraft_Systems.pdf
3. https://www.unmannedairspace.info/uncategorized/airbus-launches-blueprint-utm-roadmap-predicts-19269-drones-hour-paris-2035/
4. http://time.com/5295586/drones-threat/
5. https://www.standard.co.uk/news/uk/cost-of-gatwick-drone-chaos-expected-to-run-into-tens-of-millions-a4030751.html

Claudio Palestini

is working as a Counter-Terrorism Officer at NATO Headquarter, within the Emerging Security Challenges Division. He deals with topics such as countering terrorist misuse of technologies and manages projects in the Science for Peace and Security (SPS) Programme and Defence Against Terrorism Programme of Work (DAT PoW). Before joining NATO, he has worked in European Union institutions, dealing with the satellite navigation programme Galileo and the Single European Sky ATM Research (SESAR) Deployment. He holds a PhD in telecommunication engineering from University of Bologna (Italy).

Future Command and Control of Electronic Warfare

By Major Erik Bamford, NOR A, Norwegian EW Centre
By Commander Malte von Spreckelsen, DEU N, NATO Joint Electronic Warfare Core Staff

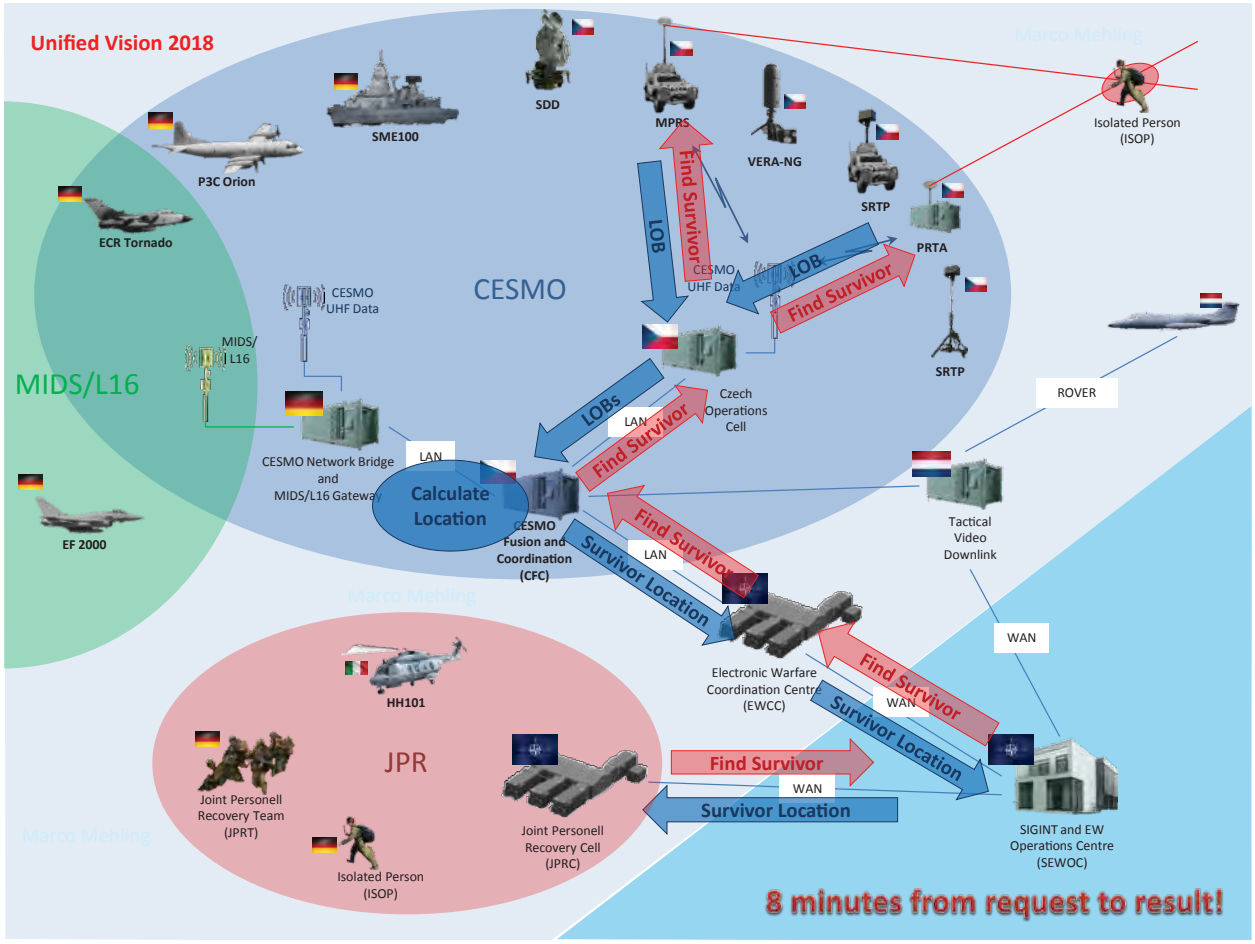
New Functional Services are on Their Way to Enhance NATO's Ability to Effectively Command and Control Electromagnetic Operations.

Introduction

During a NATO-led operation, a helicopter crashed due to a malfunction. The helicopter crashed well within a contested area. Unfortunately, the pilot was not able to transmit his last position prior to the crash. This event changed the daily routine within the NATO Combined Joint Task Force ELBONIA staff who immediately initiated the contingency plans for personnel recovery in hostile-controlled areas. Without loss of time, the Commander reviewed the latest known geolocation of the helicopter and made the rescue of the downed crew his top priority.

All available assets and sensors were tasked to search for, identify and geo-locate the downed crew within the defined search area. The chief of the Electronic Warfare Coordination Cell (EWCC)[1] tasked his available Electronic

Warfare (EW) assets to focus on any electromagnetic emissions related to the crash by issuing an updated Emission of Interest (EOI) list. The updated EOI covered call sign, combat identification last recorded transmission (time/space) and emergency beacon search priorities. The radio frequencies for the downed pilot's personal AN/PRC-112[2] Survival Radio were uploaded via the Cooperative Electronic Support Measure Operations (CESMO)[3] Fusion Cell (CFC). Instantaneously all CESMO equipped assets received the updated EOI to sense for the requested frequencies. The basic concept of CESMO is to increase NATO-led formations' collective exploitation through the benefits of using multi-platform intercept data. The collected multi-platform intercept data is shared in near real-time and supports the need for rapid geo-location of targets/EOI from different locations (altitude and azimuth) and orientations. Near real-time sharing enables rapid and accurate geo-location and the ability to defeat threats in a matter of seconds. It also provides the ability to geo-locate and link up with allied forces who find themselves beyond the reach of established command systems.



© DEU Air Force/Cdr Malte von Spreckelsen, DEU N

Figure 1: EW reporting chain at Unified Vision 2018 for the personnel recovery event.

The sensor network available on the day of the crash consisted of two Tornados,[4] a P3C Orion[5] and some ground-based surveillance vehicles. Eight minutes after the crash the Chief of EWCC reported the triangulated position of the AN/PRC-112 to the operations centre. Immediately thereafter an available aircraft with video downlink capability was tasked to investigate the signal and verify the position. The helicopter and crew were found, and the rescue mission could proceed.

This scenario took place during NATOs Joint Intelligence, Surveillance and Reconnaissance (ISR) Trial Unified Vision 2018. The eight minutes from the initial incident to the successful localization and identification of the crashed crew could be rated as a great achievement. However, it should be noted that the software, tools and systems used in the EWCC to coordinate the search in the spectrum were not at all advanced or highly sophisticated.

The NATO Emitter Database (NEDB)[6], as a reference database, still runs its queries within a Microsoft® Access Database and the CFC was not connected with the rest of the NATO Trial Network. Information was manually moved between the different systems to overcome the lack of connectivity and interoperability. The current processing, including manual movement of information, requires additional staffing. This example highlights NATO's need for new tools and functional services to ensure proper Command and Control (C2) of Electromagnetic Operations (EMO). Command and Control (C2) of EW is designed to provide this.

Electromagnetic Operations

NATO forces are required to operate within an increasingly complex Electromagnetic Environment (EME)[7],

Figure 2: C2 of EW related word cloud.

which is defined as an operating environment[8] by NATO. Commanders are tasked to attain the level of superiority required to enable effective friendly forces' use of the EME while simultaneously exploiting, preventing or reducing the adversary forces' EME usage. EMO consists not only of EW but several other disciplines which operate in the EME, such as navigation warfare, spectrum management, and signal intelligence. As EW has evolved from isolated operations in the EME at the tactical level towards joint EMO at the strategic and operational level, EW remains the combat discipline of EMO.

NATO doctrine recognizes that NATO operations are complicated by an increasingly congested and contested EME.[9] All modern forces conduct operations that depend on the use of the EME. The recognized need for military forces to have access to and utilize the EME creates vulnerabilities and opportunities for EW. Today's communication, sensing and guidance devices, whose function depends upon electromagnetic energy, are increasingly used both alone and in networked arrangements by civilian and military organizations.[10]

Command and Control of Electronic Warfare – A Project

EMO demands a level of coordination and synchronization which is impossible without specialized capabilities that support EME situational awareness, coordination and priority of actions.

Command and Control of Electronic Warfare (C2 of EW) describes the development and implementation activities associated with the supporting functional services.

The C2 of EW project will be implemented incrementally. The first increment will replace the legacy fielded NEDB as the foundational data provider for C2 of EW. The second increment should fulfil the Minimum Military Requirements (MMR) for planning, coordinating and managing EW activities focused on mission execution. Future increments, including support to EW, integration for threat assessment, planning and coordination of force employment, operational reporting, Navigation Warfare and Spectrum Management related tools will follow as well as cueing to/from other functional services. An agile acquisition approach to C2 of EW should ensure the timely fulfilment of the highest prioritized requirements. This approach should also allow for added functionality as NATO EMO evolves.

An information exchange requirements working group is currently reviewing and updating existing NATO EW messages to ensure their relevance and actuality. As a result, the NATO Common Electronic Order of Battle (C-EOB) exchange format will be introduced.

The C2 of EW supports NATO's exploitation of the EME from stabilization or humanitarian operations through to major combat operations, ranging in scope from a single radio-controlled improvised-explosive device incident to operations against sophisticated Integrated Air Defence Systems (IADS). C2 of EW is by design intended to enhance the knowledge of the EME and inform Commander's decisions with the ultimate goal being to achieve EMS superiority.

NATO Emitter Database Next Generation

The NATO Emitter Database (NEDB) was established as a NATO database and information sharing tool on electromagnetic systems over 25 years ago. It is NATO's primary platform for EW mutual support and exchange of the best emitter data available in both peacetime and periods of crisis. Therefore it is one of the most important sources of information to enable C2 of EW. Since its inception, the NEDB has been continuously expanded to facilitate the description of new electromagnetic systems and associated platforms.

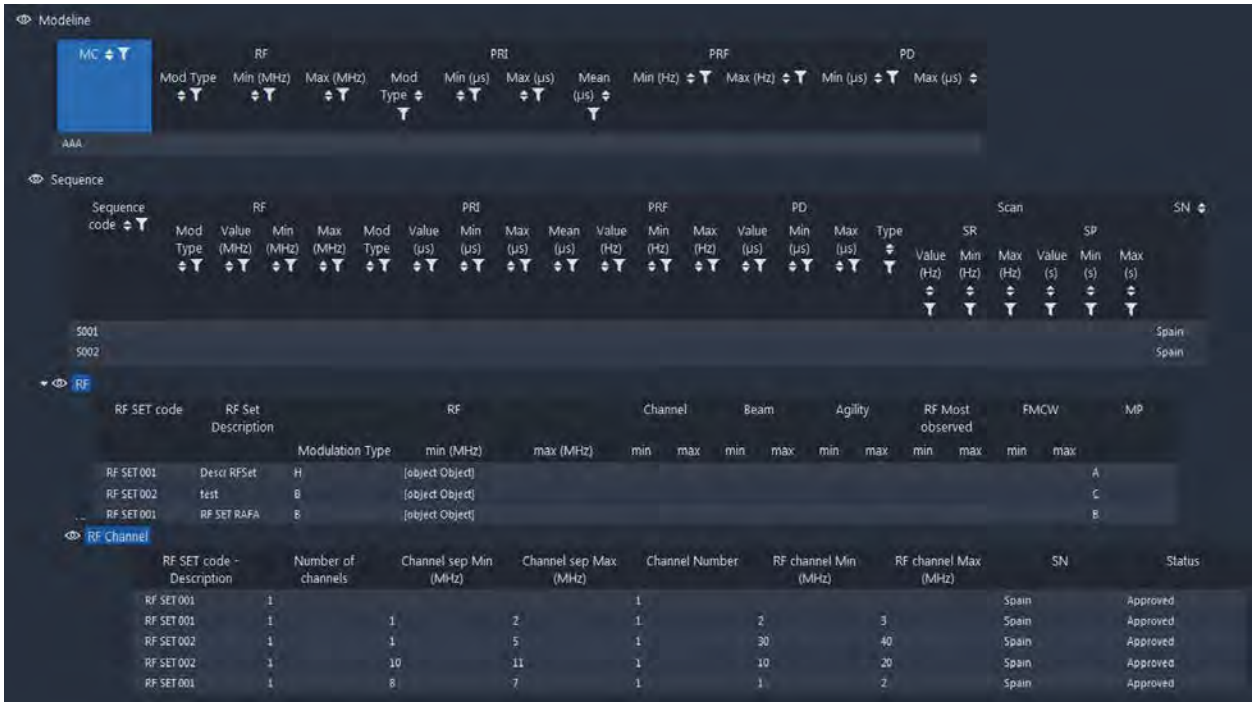
Recent operational requirements and technological developments triggered a technology uplift of the NEDB into the NATO Emitter Database Next Generation (NEDB-NG). The existing database does not effectively address NATO's emitter data management processes, network security policies and lacks automation and integration with other information capabilities. There is also a requirement for a more complex data model that can adequately describe the complex modern emitters which continue to proliferate within the electromagnetic environment.

The NEDB-NG will be delivered during the first increment of C2 of EW. It was developed as a web-based capability, with advanced data storage and near real-time data-sharing capabilities, which can be deployed in a federated infrastructure of a system of systems. All existing NEDB data will be migrated into NEDB-NG which will be available and run on the NATO Secret Wide Area Network. It will also be accessible through Battlefield Information Collection and Exploitation Systems (BICES) networks to all NATO nations. Each NATO nation may also have national instances of NEDB-NG running on their own National networks.

An innovative, agile methodology has been adopted for developing the NEDB-NG, and the user community is directly involved in the design and development process. The Initial Operational Capability (IOC) is planned to be delivered in 2019 with full service expected in 2020.

NATO Recognized Electromagnetic Picture

The NATO Recognised Electromagnetic Picture (REMP) aims to visualize EM activity in time and space (3D tracking) in a manner that is relevant to enhance situational awareness and the effective conduct of Allied EMO. NATO REMP seeks to compile all EOI for own, adversarial and neutral entities within the Joint Operations Area (JOA). The NATO REMP will utilize NATO Core Geographical Information Services (NATO Core GIS) to visualize geographically referenced EM information for dissemination and storage. As such it will



© NCIA

Figure 3: NEDB-NG Mock-up used to support the design of the Database Reader View. The image shows the filters available at the mode line level.

provide a seamless sharing of the REMP into the NATO Common Operational Picture (NCOP), increasing the awareness of EMO across the Joint Force.

The NATO REMP will be a core function of NATO's future C2 of EW and will support the full range of features required for NATO EMO including planning, directing, monitoring and assessment of the EMO. Key to the support of planning and assessment of Allied EMO is the monitoring of near real-time universal EM activities to direct own forces' EM actions and capabilities in a congested and contested Electromagnetic Spectrum (EMS). Additionally, the NATO REMP will visualize the Electronic Order of Battle (EOB), showcasing the full EMS capability of platforms or force elements within the required area. The planning function of the NATO REMP will support the identified need for an agile approach to EMO. Modern military operations require constant refinement of own EMO. Own EMO will be planned and assessed through digitalized modelling and propagation of EM sequences for each operational phase and account for the relevant terrain. The NATO REMP will facilitate reduced Electromagnetic Interference (EMI) within the Joint Forces through a shared understanding between the EW and Spectrum Management communities.

The NATO REMP enables the visualization of the EME by bringing together NATO's EMO capabilities in a unified and coherent way. It will support NATO's wider EMO community of interest well beyond EW.

Conclusion

With C2 of EW functional services in place, the recovery scenario could continue up to the point of a successful extraction of the crew and recovery of critical materials like crypto and other technological advances which keep allied forces ahead of the adversary. The EWCC would provide an overview of threats and other activities in the EME for the overall mission planning and execution. Based on available data, EW sensors and self-protection equipment on the extracting assets could be updated to meet the current threats. This however also demands the near real-time collaboration with national EW reprogramming units. The joint restricted frequency list would be updated and prioritized to optimize the undisrupted Command, Control and Coordination of own forces. All completed with increased accuracy of information, speed and agility in the employment and integration of EMO.

The NATO EW community has developed a very mature set of criteria for C2 of EW based on an in-depth study of command and control in general and the C2 of EW specifically. The EW study includes a full review of NATO's EW information flow, formatting and usability. With these functional services, NATO will have a clear picture of the EME in the operational area, enabling effective EMO as another layer in the achievement of mission objectives and enabling the protection of own forces.

The future EME will require an advanced understanding of EME enabling exploitation, offensive and defensive EMO. NATO will be prepared by ensuring that the EMO community and EW Operators have the right tools to achieve EME superiority.

'EW has been a sleeping dragon, hidden away and forgotten for a generation. Now the awakened dragon needs to be controlled!'

1. AD 80-19 Directive for an Electronic Warfare Coordination Cell.
2. AN/PRC-112 device offers synthesized radio in the VHF and UHF aircraft bands. It is a PRC-112 modified to include a GPS receiver, allowing encrypted position information to be sent. Also has COSPAS-SARSAT (**Co**smicheskaya **S**istema **P**oiska **A**variynyh **S**udov – **S**earch **A**nd **R**escue **S**atellite-**A**ided **T**racking) beacon.
3. NATO STANAG 4658.
4. The Panavia Tornado is a family of twin-engine, variable-sweep wing multirole combat aircraft, which was jointly developed and manufactured by Italy, the United Kingdom, and West Germany. The Tornado IDS (interdictor/strike) version is employed as fighter-bomber.
5. The Lockheed P-3 Orion is a four-engine turboprop anti-submarine and maritime surveillance aircraft developed for the United States Navy and introduced in the 1960s.
6. STANAG 6009.
7. MC 64/11 'NATO recognizes the Electromagnetic Environment (EME) as an operating Environment'.
8. According to NATO, Operating Environment (OE) is a composite of the conditions, circumstances and influences that affect the employment of capabilities and bear on the decisions of the commander.
9. AJP 3.6 'ALLIED JOINT DOCTRINE FOR ELECTRONIC WARFARE'.
10. Ibid. 9.

Commander von Spreckelsen

joined the German Navy in 1993 and holds an MA from Kings College London. He has a background in maritime aviation on BR 1150 Breguet Atlantic as a Mission Commander. During his career, Commander von Spreckelsen held command of different naval and joint EW units up to battalion size. In between he was posted at the Strategic Reconnaissance Command. In 2015 Commander von Spreckelsen resumed his present position as the Chief of Plans and Policy in the NATO Joint Electronic Warfare Core Staff. On this position in 2017 he was appointed as the Chairman of the NATO Electronic Warfare Working Group. During his career, Commander von Spreckelsen deployed several times on different NATO missions and has 2,500+ flight hours.

Major Erik Bamford

joined the Norwegian Army in 1995 as an Infantry Officer Candidate. Upon graduating the Norwegian Military Academy in 2002, Bamford changed from Infantry to EW. Through his career Bamford have served in several operational EW postings within the Norwegian Army including EW Branch Head at the Army TRADOC. Major Bamford has actively represented Norway in several NATO EW forums, including NATO Team of Experts on ECM for RCIED and NATO EW Working Group. Major Bamford has several deployments in EW and EW related positions in both Afghanistan and Iraq. In 2013 Major Bamford assumed the position with the Royal Norwegian Air Force (RNoAF)/ Norwegian EW Centre (NEWC) as SO EW – National Joint EW authority. Bamford currently co-chairs the Command and Control of EW sub-group within the NEWWG.

Satisfying ISR Requirements in Stabilization Missions – Is Contracting the Right Option?

A Reflection from a Robust UN Peacekeeping Mission towards NATO's Future Operations

By Major Michel Busch, DEU A, JAPCC

Introduction

The trend of outsourcing services and parts of businesses to third-party manufacturers or service providers has become more and more fashionable since the 1990s. One main reason is businesses wanting to focus on their own core strengths in high-tech aspects of the work, while leaving baseline work and services to others that specialize in that field, for short-term financial gains. Likewise, the military services have embraced similar ideas and practices. Since the end of the Cold War, but especially from the 2000s, non-core functions of militaries have been outsourced around the world, ranging from maintenance services of equipment and infrastructure to logistical support[1]. The gains envisioned were similar to civilian counterparts' and largely motivated by budgetary concerns[2].

However, despite early trends to limit outsourcing to so-called 'non-core services', core functions have also increasingly become outsourced. This paper will discuss outsourcing trends in the Alliance's Intelligence field and whether this trend is a worthwhile option, or perhaps even a necessity. In order to draw conclusions regarding NATO, another actor in the area of peacekeeping, the United Nations (UN), is used as a reference to debate the advantages and disadvantages of using non-military Intelligence, Surveillance and Reconnaissance (ISR) service providers in an actual mission area.

MINUSMA MALE ISR Assets

The UN Department of Peacekeeping Operations (DPKO) Multidimensional Integrated Stabilization Mission in Mali (MINUSMA), is currently utilizing two Medium Altitude Long Endurance (MALE) Unmanned Aircraft Systems (UAS) as its main theatre ISR collection assets. One is an Israel Aerospace Industries HERON 1 system provided, manned and employed by Germany as part of their ISR Task Force contribution to the mission[3]. The other UAS is an ELBIT HERMES 900 system provided, manned and employed by the private company THALES UK. Both systems share similar features with respect to their capabilities and both are tasked by the MINUSMA Force Headquarters (FHQ) U2[4] ISR cell for long-endurance mission sets. These missions include ISR collection in accordance with the Intelligence Collection Plan (ICP) and direct support to operations, including force protection. Another similarity of these systems is their embedded analytical capacity, both having imagery analysts who conduct first-level analysis on-site. Of note, the HERON UAS utilizes a reach-back component at the home base of the squadron in Germany for the 'level 2' analysis while Thales UK conducts all analytical work in theatre. Even though they operate from different Main Operating Bases (MOBs)[5], both UAS share the same overall constraints of state-of-the-art MALE UAS. Issues such as airspace integration, airspace risk management, weather limitations and a high dependency on the availability of satellite communication bandwidth are foremost areas of concern when employing either a military-owned or a contracted MALE UAS system. Nevertheless, how the employing unit/vendor deals with these inherent limitations can be quite different.

Role of the ISR Forces in a Peacekeeping Mission and NATO Stabilization Operations

Before delving into the advantages and disadvantages of different ways to provide this ISR 'service', one must consider the baseline role, considerations and assumptions of ISR air assets in peacekeeping operations (and their relationship to NATO stabilization operations).

The current Areas of Operation (AOO) of NATO and Coalitions fighting against terrorism, such as ISAF/Resolute Support, Operation Inherent Resolve (OIR) and UN missions such as MINUSMA, predominantly consist of large geographic areas with stakeholders and parties of multiple affiliations. Typically, the participants have limited numbers of both 'boots on the ground' and ISR resources to satisfy the Intelligence Requirements (IR) of Force and Mission leadership[6]. This is especially true given the dynamic and ad-hoc taskings that are derived from the need to have 'eyes-on' various situations on the ground, many of which overextend available capacities[7].

Notably, employing a MALE ISR asset in a mission requires a substantial effort by supporting elements and infrastructure to actually get the asset airborne.

More to the point, only a few nations have a MALE UAS capability in their inventory at all. Within NATO, only 11 countries have or are in the process of acquiring MALE-like systems, limiting the number of possible Troop Contributing Countries (TCCs). For UN missions, even though in theory there is a bigger pool of possible contributors (states), the actual number of nations contributing to UN missions, with contingents big enough to host a MALE UAS, are mostly limited to TCCs that do not have this capability available[8]. Therefore, to be able to satisfy even current ISR requirements, additional [non-military (or non-governmental or non-state)] providers of ISR capabilities often have to be considered.

© Drone: Bundeswehr, Sebastian Wilke
© Handshake: Africa Studio/shutterstock

As a result, this demand-that-exceeds-supply has given rise to various organizations that are able and willing to provide such capability and expertise. Specialized ISR know-how is now commonly available to commercial entities due to the employment of MALE UAS systems in military operations for the last 20 to 25 years and the military's subsequent loss of personnel to the civilian sector. Consequently, the experience gained in the field by operating MALE systems in diverse environments, such as the above described AOO, is harnessed by employing these former military operators and catalysed by utilizing a wide range of commercially available, or self-developed systems. Hence, a wide range of companies are now at the disposal of governments and multinational organizations and not only offer technical and logistical support, but an entire range of effects from employing the aircraft to analysing the data.

Considerations of Employing a Civilian Contractor

In order to derive an assessment and recommendation on the future use of civilian ISR contractors in NATO operations, their participation in the Tasking, Collection, Processing, Exploitation, and Dissemination (TCPED) process shall be examined with respect to the operational value of the two UAS in the MINUSMA mission. Due to the focus on the ISR results in this paper, the second major aspect of the topic, the legal dilemma of contracted civilians in armed conflicts, will not be evaluated[9].

Tasking: By their nature, UAV ISR missions are either deliberate, dynamic or ad-hoc. Deliberate missions entail detailed planning and subsequent tasking by analysing Requests for Information (RFI). Dynamic and

ad-hoc missions are completed by re-tasking UAVs that were conducting other assignments, such as deliberate missions. Still, all tasking types require the tasking authority to provide the asset with a detailed set of questions in order to answer the IR. With a civilian contractor, the challenge in this step lies in comprehending the tasking with regard to access and knowledge of the operating environment and situation. The main issue is the constant risk of missing available background information due to the lack of direct access and/or 'membership' in military Intelligence product distribution chains. Consequently, a higher degree of communication between tasking manager, requestor and asset is required, creating more workload at the Information Requirement Management/Collection Management (IRM/CM) cell and, potentially, less detailed analysis.

Collection: Considering the collection part of the ISR process, the overall environmental framework in which a contracted asset is operating is not much different from a military one as they basically use similar versions of UAS. However, when considering the actual availability of an asset, especially in cases of activation in ad-hoc or emergency situations, the contractual boundaries and framework of civilian assets do create constraints. For example, the focus of a civilian contractor will almost always be driven by economic circumstances, therefore minimizing available crew and assets and therefore costs within the contractual limits. Conversely, a military-operated asset is normally assessed to have greater flexibility and reachability, especially in crisis situations. For real-time viewing of collected information, connectivity to, and potential requirements for the training of units in handling of remote video terminal technology provided by the contractor needs consideration. It is considered to require more coordination to include external training to TCC units than from organic military assets but still this requirement needs to be included in military training efforts for units to reach Full Operational Capability.

Processing: The third step in the ISR process is considered a primary technical one. Still, permission to connect to the Command and Control (C2) systems of the mission could be a show-stopper for civilian entities. Even if it is not, the level of classification of the collected data, and the possible security concerns that arise when having a civilian contractor store the data on commercial drives, must be taken into consideration. Nevertheless, available framework concepts and NATO standards that provide reference to interoperability should be utilized at the early stages of the contract development to avoid challenges in this technical step.

Exploitation: Exploiting data that is collected is a time consuming and crucial step in the Joint ISR process. It requires access to sensitive reference data and is, therefore, an important factor in the decision to contract an all-inclusive (civilian only) package of the TCPED process. Both of the last steps of the process, exploitation and dissemination, include similar restrictions and considerations concerning operations security. These considerations lead to an assessment that either allows full access for the contracted analyst to get the highest quality product, or exploitation will otherwise inherently be limited to 'level 1'. If that limitation is imposed and in-depth analysis is left to military analytical capacity, monitoring of the efficiency of the tasking and collection, plus the quality of the first-level interpretation by any sensor operator, is to be considered most crucial and requires additional manpower to understand the 'why and how' of the collected information. This factor is also one of the main considerations of use (or not) of reach-back analysis units outside the theatre, as a 'break' in the chain between first and second level analysis is more likely.

Dissemination: Finally, the ISR results need to get to the right person and unit to be of value. Because this stage is closely linked to the tasking step, and assuming the C2 connection from the asset to the IRM/CM cell is working, it is considered to be as efficient as a military asset. Still, the requirements for ad-hoc and dynamic reporting is assessed to be more challenging when working with the contracted asset, especially when limited secondary methods of communication are established. This is largely due to the location of the asset and accessibility of communication equipment that is only available to the military requestor.

Additionally, factors beyond the TCPED process, like human factors and business models, have to be considered. A staff of civilian contractors posted to a remote location has different dynamics than a military unit deployed in the same area. In the author's experience, the relationship within a military unit, especially when working together as a team towards a military objective, is different to a collective staff of civilian individuals, each with different duty durations, leave days and working in a company-salary based system. It can be argued that the motivation of the latter 'to go the extra mile' to make a flight, mission and product happen is less than a functioning military unit.

Conclusion

Not all experiences from a UN peacekeeping mission can be transferred to NATO stabilization operations but both missions share similar ISR requirements. Therefore, with regards to experiences from MINUSMA, the following are notes and recommendations for NATO when contracting unmanned (or manned) ISR:

Contracting an ISR asset to deploy a full-service package, especially to austere locations, cannot be handled like any standard service contract. The architecture of how the system is supposed to function within the mission framework is crucial to success and requires detailed preparation and validation. Consequently, a high satisfaction rate can only be ensured by considering operational experience when negotiating the contract.

A contracted ISR asset is most valuable in a relatively static environment with a clear focus on recurring tasks and with a clear baseline of information. Contractors can fill gaps in an environment such as that and deliver satisfactory results, often because of their military backgrounds. Solely relying on them in a dynamic environment, especially when only very few overall sensors are employed, should be avoided as units completely embedded in the military structure proved to be more efficient.

© Erwan de Cherisey

Level 1 Interpretation:

Real-Time observation resulting in oral near real-time description and written summary of list of events.

Level 2 Analysis:

Deliberate IMINT analysis including cross-referencing and production of requested JISR result.

The emphasis for the future should then be on establishing more combined, multinational ISR units, each with NATO-owned systems, which can be accessed and deployed directly in a flexible manner within the NATO Command Structure.

In summary, with the constant and continuous growth of conventional threats, a sole emphasis on contracted ISR is not very practical but can assist in bridging gaps and satisfy basic requirements. Overall, a too great focus on contracting may limit the experience and counter the willingness of the nations in employing MALE ISR systems in missions and not deliver the best results possible.

1. Moore, Adam, 'U.S. Military Logistics Outsourcing and the Everywhere of War' 2015 [cited 31 Jan. 2019]. Available from SSRN: https://ssrn.com/abstract=2700879; Internet.
2. Petersohn, Ulrich, 'Privatizing Security: The Limits Of Military Outsourcing'. CSS Analysis in Security Policy No. 80 (2010): p. 1.
3. Interestingly, Germany is also using a third-party service provider for technical maintenance and support of the UAS but is employing a dedicated unit for the flying operations and ISR operations.
4. UN equivalent to a CJ2 branch at operational level.
5. HERON is deployed to GAO, while the HERMES 900 is deployed to TIMBUKTU.
6. Sloan, Elinor C., Modern Military Strategy, Oxon: Routledge, 2017 p. 50.
7. Wong, Kristina, 'US commander: Lack of intelligence assets slowing down ISIS war'. 2016 [cited 31 Jan. 2019]. Available from: https://thehill.com/policy/defense/282457-isis-air-war-commander-short-on-intelligence-assets; Internet.
8. See Ranking of contributions by country to UN led mission. Available from: https://peacekeeping.un.org/en/troop-and-police-contributors; Internet.
9. For more information on this particular subject see Haider, André, 'Contracting Civilians for Remotely Piloted Aircraft System Operations. Blurring International Law's Principle of Distinction?', JAPCC Journal No. 22 (2016).

Major Michel Busch

was commissioned to the German Army as an artillery officer in July 2003. His subject matter expertise comprises Unmanned Aerial Vehicles (UAV) and Imagery Intelligence (IMINT). He was recently deployed to the UN Peacekeeping Mission in MALI as U2 Deputy Chief ISR. In previous assignments, he was an Instructor for NATO Aerial Imagery Analysis and Head of the Full Motion Video Section at the German IMINT Training Centre. Major Busch holds a university diploma degree in Social and Political Sciences from the Bundeswehr Universität München and a Master of Business Administration degree from the University of Applied Sciences in Kempten.

© Toria/shutterstock

Command and Control in Digital Transformation

The Future of the Command Post

By Harold H. M. Vermanen, MBA, Business Director Public Sector, Microsoft Corporation

Threat Landscape is Changing

The Crimean crisis showed Russia's 'new generation warfare' capability or, as NATO described it, 'hybrid warfare' including propaganda, deception, sabotage and other non-military tactics.

These tactics were used before. The difference was in their level of intensity, scale and speed, all made possible due to available technology, which was a leading threat vector vice a supporting element as in the past.

According to the Multinational Capability Development Campaign (MCDC) in their report Countering Hybrid Warfare Project[1] '… our common understanding of hybrid warfare is underdeveloped and therefore hampers our ability to deter, mitigate and counter this threat'.

This is not a surprise, knowing that most of these hybrid elements, such as cyberattacks, are launched with the latest technology and include other hybrid elements, like deception and propaganda.

An effective response requires, therefore, new technologies and doctrines to achieve a rapid response and enable NATO to take the initiative before the adversary is able to execute its plan.

Getting Inside the OODA Loop

The OODA loop is an acronym for the cycle 'Observe – Orient – Decide – Act' as developed by the United States Air Force Colonel John Boyd, where they applied the concept to the combat operations process,

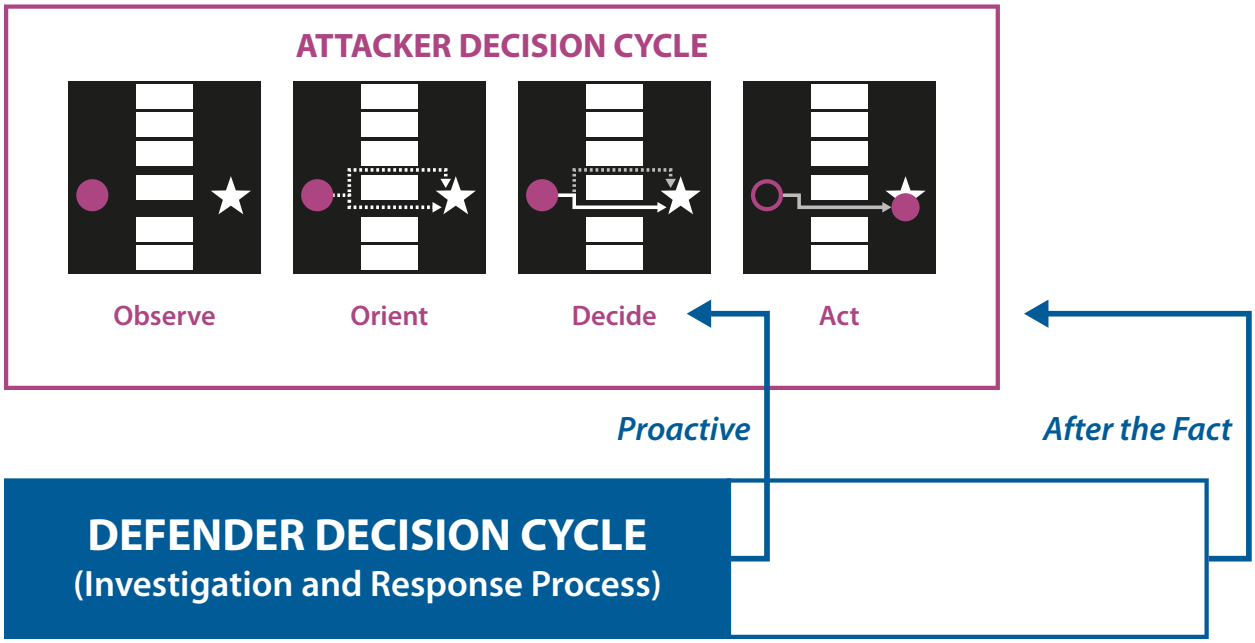


Figure 1: Getting inside the OODA loop of the adversaries. *Better and faster investigation and response decisions.*
(Source: Microsoft presentation at NATO C2 COE seminar, November 2018, graphic rebuilt at JAPCC.)

often at the operational level, during military campaigns.[2] The approach explains how agility can overcome raw power in dealing with human opponents.

By following that principle, the response to hybrid threats should be to make decisions better and faster in order to outmanoeuvre the adversary. This means getting inside the attacker's OODA loop will rapidly increase our chances to win by taking the initiative before the attack takes place. Knowing the hybrid attacks of various adversaries, there are lessons to be learned from the responses taken by commercial organizations to hybrid attacks. The 'hybrid battlefield' and cyberattacks in particular, are, as we know, not limited to military targets.

There are, of course, differences as commercial organizations are, by law, not allowed to initiate offensive actions. So, all effort is focused on defence. The objective for commercial organizations is to get inside the adversary's OODA loop by taking the initiative and make the costs for the adversary to attack the commercial organization so high, that the Return on Investment (ROI) is not attractive enough to proceed. This course of action means having an impact on the decision of the adversary before the attack (Act) is launched.

Information Dominance

Sun Tzu wrote 2,000 years ago in the 'Art of War'[3] about the importance of information dominance: 'If you know the enemy and know yourself you need not fear the results of a hundred battles.' This means that our analysts need to provide assessments better and faster to assist decision-makers to enable them to outmanoeuvre the adversary. The introduction of hybrid warfare with cyberattacks changed the thinking that manpower alone is enough to gain information dominance.

Skyrocketing volumes of data from more and more sensors expedited this requirement, as all the analysts in the world would not be enough to translate the volume of available information into predictions and help make the best decisions in time.

How Machine Learning can Support Command and Control

Machine learning (ML) is potentially a valuable way to analyse large data sources/signals and predict what is expected to happen, thus enabling organizations to take the initiative before an attack takes place.

© HQuality/shutterstock

With ML you can establish your own data model (algorithms) with specific instructions for performing a task. Predicting, for instance, an adversary's attack vector in such a way depends on the quality of the algorithm, and the volume and quality of the available data.

Computing power, in combination with ML, helps to overcome the human limitations of using large data sets because it:

- scales beyond the limits of human capabilities and expertise;
- shines a light in areas undetectable by humans (blind spots);
- helps staff automate routine tasks, avoiding wasted effort.

As with many disruptive innovations, ML presents risks and challenges that could affect authenticity of the information provided to commanders and the outcomes of processes and technologies that use it. ML algorithms basic risks may include:

- amplification of human bias;
- inadvertently reveals private/secret information;
- missing critical context and implications (e.g. confuse innocent 'John Smith' with another 'John Smith' with the same birthdate but a criminal record);
- feeding false/malicious data.

These deficiencies could undermine the decisions, predictions or analysis ML applications produce, subjecting us to legal liability and other harm. Some ML scenarios present an ethical dilemma like for example a form of small drones that are able to be deployed, and unlike current military drones, be able to make decisions about killing others without human approval based on a certain algorithm.

In an ideal world, we would have the best-designed algorithms (ML) to minimize these risks. In combination with the highest quality and volume of data, high computing power will enable us to provide the best predictions for organizations to affect Command and Control (C2) and to execute an effective OODA loop.

Nevertheless, the reality is that prediction depends on human adaptability to situations and the rationale/logic used for decision-making. Besides, the lack of

quality data and comprehensive algorithms require that humans evaluate and understand the more complex situations and possible attacks.

Making Better Decisions, Faster, from a Commercial Cyber Operation

ML can be a great value within the C2 process when done in the right way using an example of a commercial cyber operation that integrated ML successfully in their C2 process based on three doctrines:

1. **MAXIMIZE VISIBILITY** (minimize blind spots and ensure you have good coverage of sensors)

   Internal – Minimize internal blind spots by ensuring you have good coverage (as close to 100 % as you can manage) of all asset types. (e.g. identities, data centres, email).

   External – Ensure you have a diversity of threat feeds from sources that give insight and context about the external environment. (e.g. malware, compromised identities, attack websites).

2. **REDUCE MANUAL STEPS** (and errors)

   Automate and integrate as many manual processes as possible to remove unneeded human actions that lead to delays and potential human errors.

3. **MAXIMIZE HUMAN IMPACT**

   For the places in the process where it makes sense to have human interaction (e.g. difficult choices, new decisions), you should ensure that your analysts have access to extensive expertise and intelligence to make better decisions.

   Additionally, ensure learning is integrated throughout the process, up to and including consideration of when you would watch an attack unfold to learn its objective (long term value) versus blocking the attack (short term value) or a combination of the two by directing an adversary to a honey pot where the characteristics can be studied without causing harm.

Improving the Impact by Including Synthetic Data and Augmented Reality

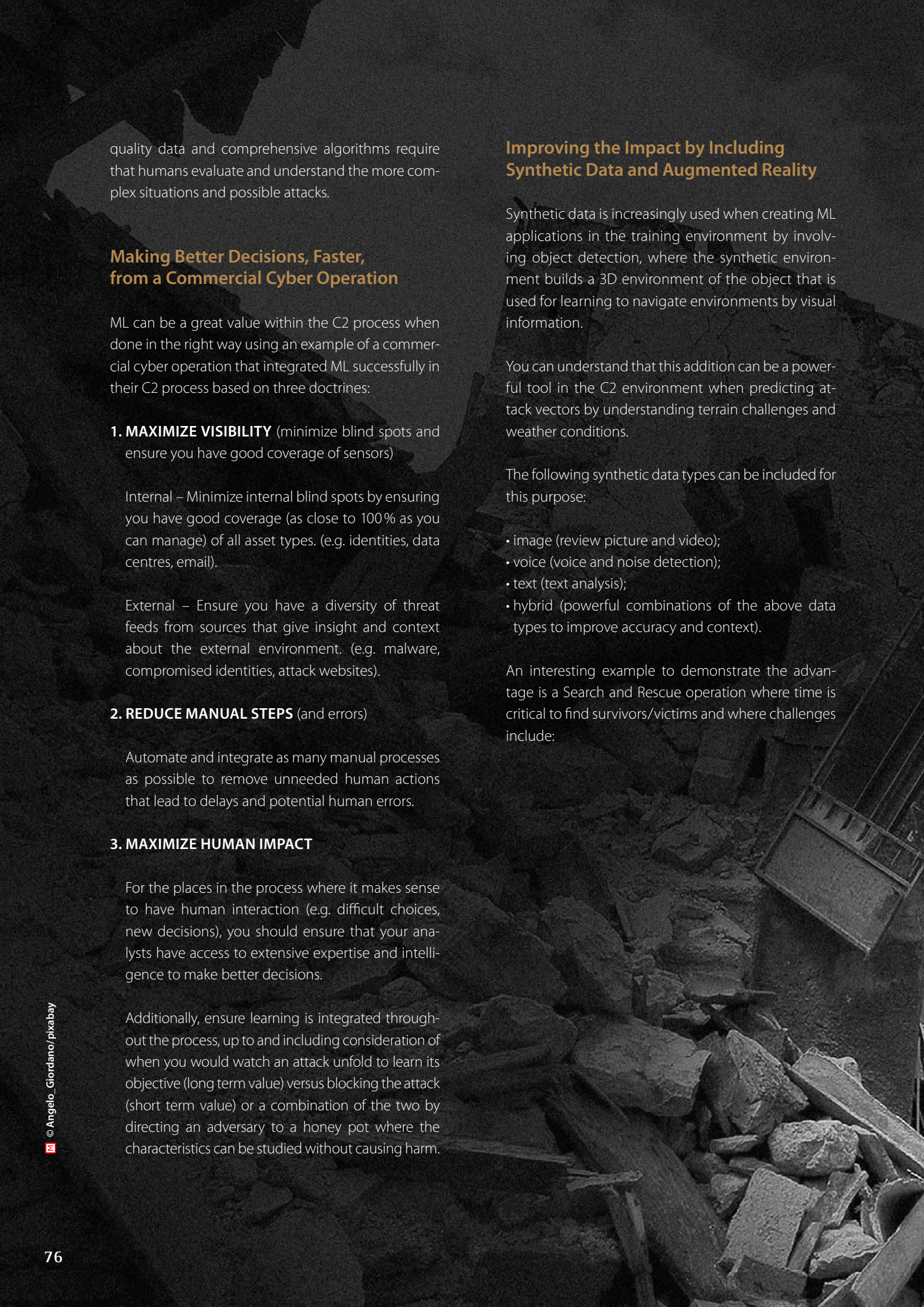
Synthetic data is increasingly used when creating ML applications in the training environment by involving object detection, where the synthetic environment builds a 3D environment of the object that is used for learning to navigate environments by visual information.

You can understand that this addition can be a powerful tool in the C2 environment when predicting attack vectors by understanding terrain challenges and weather conditions.

The following synthetic data types can be included for this purpose:

- image (review picture and video);
- voice (voice and noise detection);
- text (text analysis);
- hybrid (powerful combinations of the above data types to improve accuracy and context).

An interesting example to demonstrate the advantage is a Search and Rescue operation where time is critical to find survivors/victims and where challenges include:



© Angelo_Giordano/pixabay

- Difficulty finding survivors in rescue situations where low light, weather, or complex terrain are factors (i.e. forests and oceans).
- There is too much information for the human eye to process in a short time frame.
- Resource bottlenecks requiring creative solutions to maximize effectiveness.

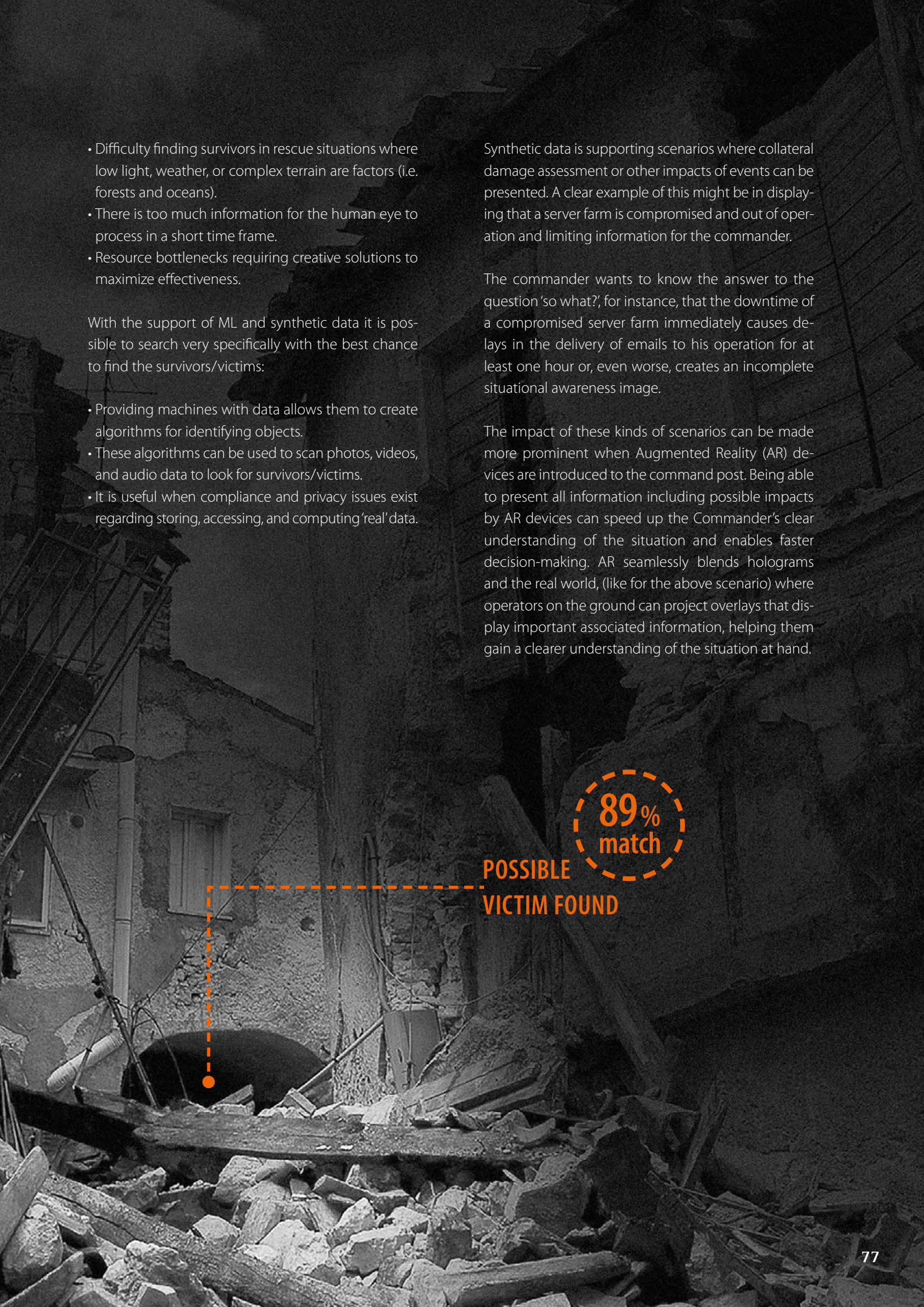
With the support of ML and synthetic data it is possible to search very specifically with the best chance to find the survivors/victims:

- Providing machines with data allows them to create algorithms for identifying objects.
- These algorithms can be used to scan photos, videos, and audio data to look for survivors/victims.
- It is useful when compliance and privacy issues exist regarding storing, accessing, and computing 'real' data.

Synthetic data is supporting scenarios where collateral damage assessment or other impacts of events can be presented. A clear example of this might be in displaying that a server farm is compromised and out of operation and limiting information for the commander.

The commander wants to know the answer to the question 'so what?', for instance, that the downtime of a compromised server farm immediately causes delays in the delivery of emails to his operation for at least one hour or, even worse, creates an incomplete situational awareness image.

The impact of these kinds of scenarios can be made more prominent when Augmented Reality (AR) devices are introduced to the command post. Being able to present all information including possible impacts by AR devices can speed up the Commander's clear understanding of the situation and enables faster decision-making. AR seamlessly blends holograms and the real world, (like for the above scenario) where operators on the ground can project overlays that display important associated information, helping them gain a clearer understanding of the situation at hand.



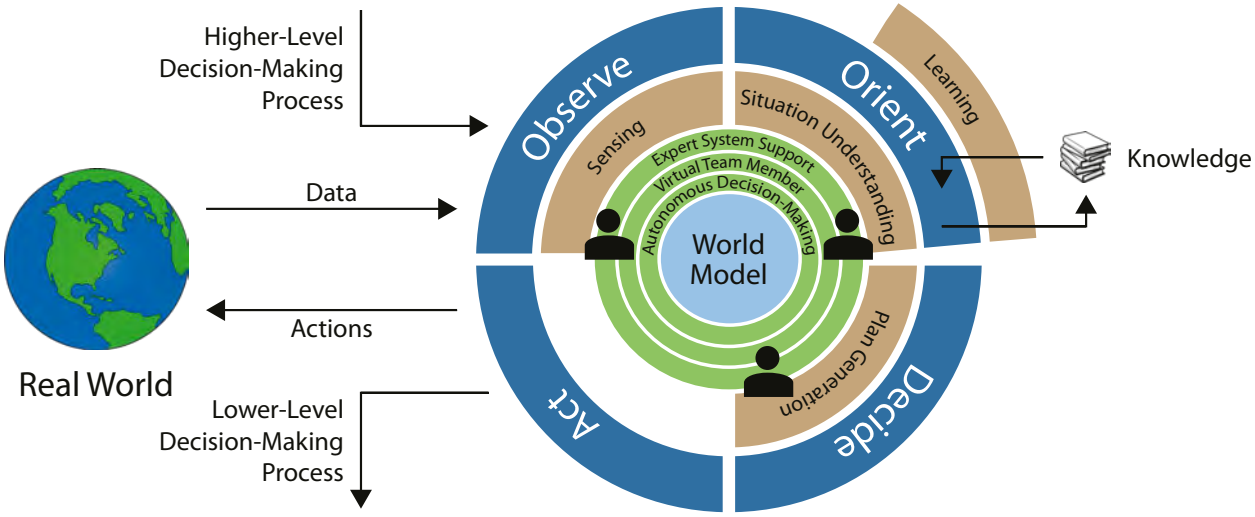


Figure 2: A system view of the OODA decision-making cycle supported by AI.
(Source: NATO Science & Technology Organization STO-MP-IST-160, graphic rebuilt at JAPCC.)

Reduce Time and Complexity in Decision-Making with Machine Learning and Augmented Reality

ML and AR will be able to provide the analysts and commanders additional Artificial Intelligence (AI) services that are unlocked by the usage of these new technologies. This will have a positive impact on the following parts of the C2 process:

- Course of Action options (more precise and much faster);
- analyze patterns and anomalies in data to take actions;
- improved force readiness by aggregating siloed and open source data for intelligence analysis;
- automatic classification and processing of visual data such as reconnaissance images or training video;
- automated translation and transcription for better interaction in multinational forces and expeditionary missions.

The question that arises is can AI take over the C2 process in the future?

For the near future, we will see ML driving a process which should always be managed by humans. In practice, this means that ML will drive the 'no brainer, very logical' decisions and execute them quickly, and, as always, under the authority and responsibility of humans. The more complex decisions will always require human agreement before execution, where ML can provide advice on what to do.

The quality of ML decisions continues to depend upon the availability, volume and quality of data and on the quality of the algorithms.

Evolution Trajectory of (Cyber) Command and Control

The main advantage that we see in the evolution of C2 is that the 'Mean Time To Remediation (MTTR)' decreases by optimizing expert human decisions in a faster way.

Below we can see Microsoft's expectation on this evolution where the evolution of C2 will continue and is expected to be brought to a new level by the introduction of AI bots and AR, which is expected to further decrease the MTTR.

Technology will continually improve as will the ability and speed at which analysts and incident responders detect and remediate incidents. The speed of evolution will be influenced by the ability of humans to accept and trust the outcome of the prediction algorithms in such a way that they will feel comfortable to make important decisions.

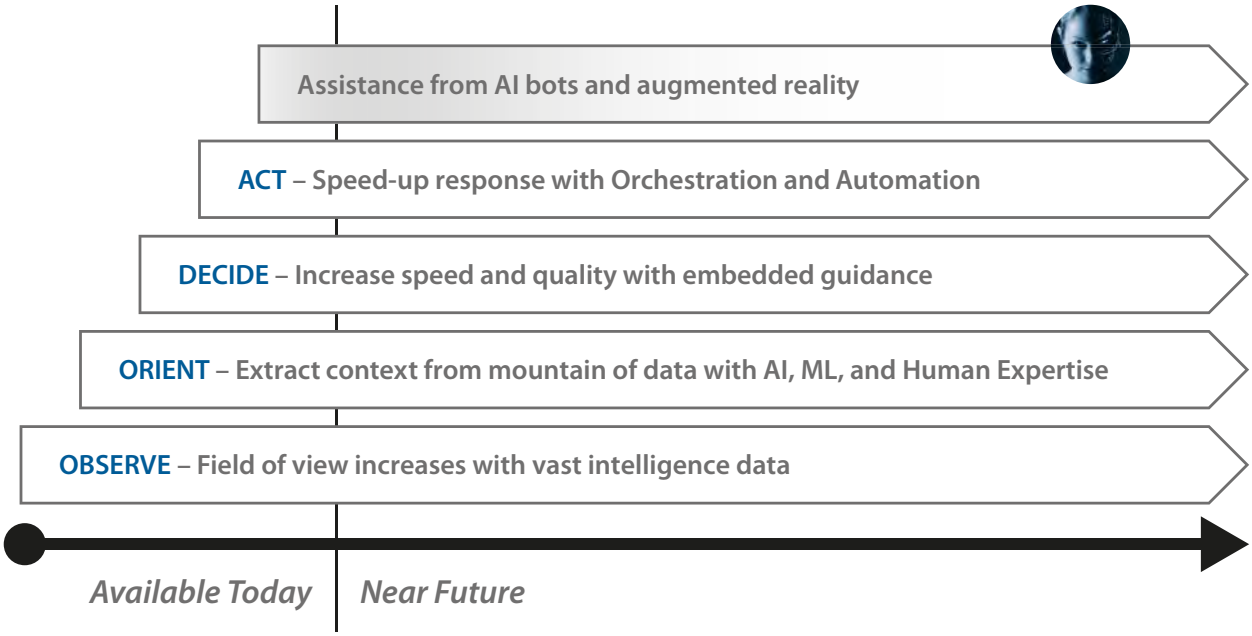


Figure 3: Evolution Trajectory of (Cyber) Command & Control. *Reducing Mean Time To Remediation (MTTR) by optimizing expert human decisions.* (Source: Microsoft presentation at NATO C2 COE seminar, November 2018, graphic rebuilt at JAPCC.)

The idea that, in a relatively short time, AI will become superior to human intelligence was popularized by the well-known futurist, Ray Kurzweil argued in his 2005 book *'The Singularity Is Near: When Humans Transcend Biology'*[4] that by 2045 'It may be true that new technologies are slowly replacing certain cognitive tasks, just like machines replaced physical labour during the Industrial Revolution'.

The future will tell us if the outcome of battles will depend on the best AI technology, therefore I would like to conclude my article with a quote from Microsoft's Chief Executive Officer (CEO) Satya Nadella on his perspective on how AI should develop:[5]

'We've seen how AI can be applied for good, but we must also guard against its unintended consequences. Now is the time to examine how we build AI responsibly and avoid a race to the bottom. This requires both the private and public sectors to take action.'

1. Multinational Capability Development Campaign (MCDC) report 'Countering Hybrid Warfare Project', published 27 Sep. 2017: https://www.gov.uk/government/publications/countering-hybrid-warfare-project-understanding-hybrid-warfare
2. Science Strategy and War, The Strategic Theory of John Boyd. Abingdon, UK: Routledge, ISBN 0-415-37103.
3. Art of War (Chapter 3, Attack by Stratagem) by Sun Tzu is an ancient Chinese military treatise dating roughly 5th century BC. Translated from the Chinese by Lionel Giles, MA (1910).
4. 'The Singularity Is Near: When Humans Transcend Biology' non-fiction book (2005) written by Ray Kurzweil about artificial intelligence and the future of humanity.
5. Microsoft CEO Mr Satya Nadella on Twitter (1:49 AM – 7 Dec. 2018).

Harold H. M. Vermanen MBA

Harold Vermanen (Netherlands) has worked in various roles within the technology industry with a focus on digital transformation of critical infrastructure for various national security customers like NATO and Defence organizations worldwide.

He has delivered presentations and contributed to panel discussions on many military conferences on topics related to Digital Transformation, Cyber Security, Command & Control and more.

He regularly writes blogs for Microsoft and is also a member of various advisory groups and boards for the public sector and other customers with the objective to secure the critical infrastructure. Harold started his career as an officer of the Royal Netherlands Army (RNLA), holds an MBA from Stanford University (US) and is the author of the essay 'Implementing Changes in Hectic Environments'.

Joint Air & Space Power Conference 2019

Congress Centre Essen-East, Germany

Shaping NATO for Multi-Domain Operations of the Future

8–10 October 2019

Contact and reserve your seat:

conference@japcc.org

www.japcc.org/conference

Joint Air Power Competence Centre

The JAPCC Annual Conference 2019

The JAPCC invites you to attend the 2019 Joint Air and Space Power Conference in Essen, Germany, from 8–10 October. The Director of the JAPCC will kick off the Conference and two Keynote Speakers will set the stage for panel discussions addressing this year's topic of **'Shaping NATO for Multi-Domain Operations of the Future'.**

What is a Multi-Domain Operation?

The first panel will explore a working definition of what constitutes Multi-Domain Operations (MDO) and will address prevailing environmental views from the Air, Land, Sea, Space and Cyber domains, in order to set a baseline for discussion of MDO and what distinguishes it from Joint-, Hybrid-, and Effects-Based Operations.

What Requirements Go Along with a Multi-Domain Operation?

The second panel will examine the foundational requirements associated with MDO. In this context the panel will discuss the legal and policy requirements for conducting multinational MDO to improve understanding of the role of political and military decision-makers. The panel will also look at the impact of MDO on the Airpower principle of centralized command and decentralized execution and control.

Which Challenges does NATO Face in Order to Meet the Requirements?

Panel Three will address the challenges NATO may face in order to meet the requirements discussed earlier, which may include educational, psychological and behavioural adaptations in order to ensure that the individual service members can cope with the increasing speed of operations and decision cycles. Other key issues comprise securing the Electromagnetic Spectrum and protecting the Space and Cyber infrastructure.

What are the Future Enablers to Cope with the Challenges?

The last panel will expand on new technologies such as Artificial Intelligence, Hypersonic Weaponry and Robotics, as well as mining, managing and exploitation of Big Data as potential key enablers for effective MDO. Finally, the panel will address the paradigm shifts required to effectively transition from traditional C2 to a truly joint and unified command relationship that will characterize future MDO. Top experts from the political, academic, military and media spheres will debate, in four themed panels, the threats and questions raised, and how the Alliance and its partners might best evolve and leverage Air and Space capabilities to enhance and sustain NATO's three core tasks of Collective Defence, Crisis Management, and Cooperative Security. This is your opportunity to hear from senior military and civilian leaders from across NATO and the nations on this topic of extreme importance, and to engage and contribute to a robust discussion aimed at strengthening and enhancing the Alliance. To register for the 2019 Conference and see additional information, please visit us online at: *https://www.japcc.org/conference* ●

Agenda

Day One

- Keynote Address
- *Panel 1:* What is a Multi-Domain Operation?
- *Panel 2:* What Requirements Go Along with a Multi-Domain Operation?
- *Panel 3:* Which Challenges does NATO Face in Order to Meet the Requirements?

Day Two

- Keynote Address
- *Panel 4:* What are the Future Enablers to Cope with the Challenges?
- Wrap-up and Director's Closing Remarks

Cooperation in Problem Solving and Solution Developing

Joint Air and Space Network Meeting and Think Tank Forum

Over the past six years, the JAPCC has successfully developed an engagement strategy of approaching the Alliance, the Nations and EU organizations to offer opportunities for cooperative and synergetic investment in more effective research and analysis. Two main pillars of this strategy are the two annual collaborative meetings (Think Tank Forum and Joint Air and Space Network Meeting), supporting and guiding the efforts of our Subject Matter Experts by leveraging their independent thought in their areas of Expertise in the Air and Space Power environment reaching out to their global network of experts with military, academic and industrial background.

On 5 and 6 December 2018, the NATO Joint Air Power Competence Centre hosted its 5th annual Joint Air and Space Power Networking Meeting in the JAPCC's home base in Kalkar, Germany. The event attracted defence-related NATO, EU and MOU organizations to discuss current programmes of work and areas of concern, and was aimed at identifying new opportunities to collaborate in the development of effective solutions. This year's event yielded several opportunities for immediate collaboration in areas such as: improving safe, secure and efficient NATO access to European airspace in peacetime; looking into how EATC can best support NATO during an Article V scenario;

Joint Air and Space Power Network Meeting.

Joint Air and Space Power Think Tank Forum

and ongoing challenges of integrating 5th Generation technologies into existing NATO and European force and C2 structures. All in all 12 such areas of common concern were identified.

This year the JAPCC welcomed representatives from NATO Headquarters, NATO Air Command (AIRCOM), the NATO Science and Technology Organisation (STO), the European Air Transport Command (EATC), the European Air Group (EAG), the Competence Centre for Surface-Based Air and Missile Defence (CCSBAMD), Air Operations Centre of Excellence (CASPOA) and the European Defence Agency (EDA) to the event. To facilitate continued collaboration throughout the year, the JAPCC provides a secure online collaborative workspace.

The main objective of the Think Tank Forum is to magnify multiplication of effect and decrease duplication of effort throughout Air Warfare Centres, Think Tanks and similar national organizations through sharing critical Air and Space Power advancement information between NATO nations and organizations. The forum aided discussion and continuance of providing innovative, timely advice and subject matter expertise to the Alliance and our Nations while identifying opportunities for cooperative problem solving, technology development and procurement.

The 2019 TTF was graciously hosted by Greece at the Hellenic Air Force Air Tactics Centre and increased awareness of key areas of effort across multiple organizations from ten nations, discussion of potential fields of cooperation, identification of solutions to common challenges and coordination of projects, to increase cooperation and collaboration. Furthermore, discussions and presentations during TTF made very clear that 2019 JAPCC Air and Space Power Conference theme is appropriately focused on Multi-Domain Operations, as all participants showed great interest in the area. ●

Political Guidance 2019

Verification of the Focus Areas and Projects

In February 2019, NATO's new Political Guidance 19 (PG 19) was approved by the Nations' Defence Ministers in their regular session. The Political Guidance, which is released every four years at the very beginning of each planning cycle, represents one of the key NATO Defence Planning Process (NDPP) documents. Considering the overall aims and objectives that have to be met by the Alliance, while taking higher strategic policy documents into account, JAPCC endeavours to ensure the coherence of all of its ongoing projects and activities with PG 19. Within the JAPCC structure, the regular monitoring and analysis of similar documents resides within the Assessment, Coordination and Engagement (ACE) Branch. The ACE Branch examined the new PG 19 and reconfirmed the relevance of the JAPCC Focus Areas to current Alliance priorities. The JAPCC supports more than 120 projects and objectives within 13 Focus Areas. All projects in which the JAPCC is currently engaged are in accordance with PG 19.

Active Engagement of the ACE Branch

The role of the ACE Branch is not limited to passively monitoring NDPP-related documents that arrive at the JAPCC. ACE Branch representatives participated in the meetings and workshops related to the PG 19 development and actively contributed during the PG 19 production phase. The ACE Branch regularly represents the JAPCC during the PG development process led by NATOs Allied Command Transformation (ACT) within the frame of Long Term Military Transformation (LTMT). Every four years the results of the work are published in two LTMT core documents: the Strategic Foresight Analysis and the Framework for Future Allied Operations. These documents directly support and inform the development of the before mentioned Political Guidance within the first step of the NDPP. In supporting ACT, the ACE branch Subject Matter Experts (SMEs) contribute by identifying capability requirements to fulfil the future Levels of Ambition. These are set out in the PG for the Alliance as a part of the next NDPP step – Determining Requirements. ●

JAPCC's Newest Publication

'The Implications for Force Protection Practitioners of Having to Counter Unmanned Systems – A Think-Piece'

The subject of the use of 'Drones' has become a 'hot-topic' not just in NATO but globally. This issue was brought into sharp focus in Europe by the disruption caused by what the media describe as the reported use of a 'Drone', in the airspace around Gatwick Airport over the period 19–21 December 2018. This think-piece seeks to explore the issue of the use of Unmanned Systems; not just Unmanned Air Systems (UAS) but, systems operating in the air, on the surface (both land and sea) and sub-surface, again, both land and sea – a true Multi-Domain phenomena but, is it a new one?

The idea of creating a think-piece, rather than a White Paper, was to explore the issue in a pragmatic way by asking while not necessarily completely (or indeed correctly) answering a series of searching questions. The think-piece starts by exploring why this subject has become the 'hot-topic' that it is – who is driving the agenda and to what end(s)? Underlying the stated question are the thoughts that even an Unmanned System has a human-in-the-loop somewhere and, what if anything, is unique about the threat from an Unmanned System?

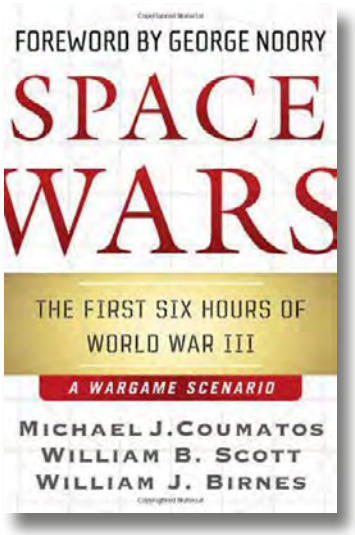
The think-piece progresses to highlight a series of well-established Tactics, Techniques and Procedures (TTPs) that if applied in the context of Countering-Unmanned Systems (C-US), will have a positive effect. The think-piece offers that in moving forward, the Alliance needs to adjust its thinking, particularly in terms of its ability to confront an intelligent, capable and adaptable adversary. The Alliance cannot have a written answer (doctrine) for everything. Human nature remains such that people will do stupid and ultimately dangerous things (e.g. fly drones around busy airports) and our adversaries will on occasion 'get lucky'! The position of the author and those that contributed, was that whilst there is a challenge to confront, is it really such a radical problem? Or, with the application of a little intellectual rigour and the resurrection of some tried and tested techniques (e.g. camouflage, concealment, dispersal etc.) and/or novel use of existing technologies, can the threat be effectively mitigated?

Ultimately, Unmanned Systems are just another threat and existing Counter-Threat methodologies can be applied successfully. Yes, new technology may provide an answer but, here again, how much new technology can our personnel realistically embrace? A new counter for every apparently new threat cannot be the answer. Rather, it is about incremental increases in capability, in step with emerging challenges but, capable of dealing with a full spectrum of threats. Otherwise, we risk dealing with the latest threat but, exposing or re-exposing ourselves to threats that have been around since Douhet was writing.* ●

*Gen Giulio Douhet (30 May 1869 – 15 Feb. 1930), Italian Gen and Air Power theorist.

E-Version: *https://www.japcc.org/portfolio/counter-uas-think-piece/*

‘Space Wars: The First Six Hours of World War III’



By Michael J. Coumatos, William B. Scott, William J. Birnes; Forge Books, April 2007

Reviewed by:

Lt Col Tim Vasen, DEU A, JAPCC

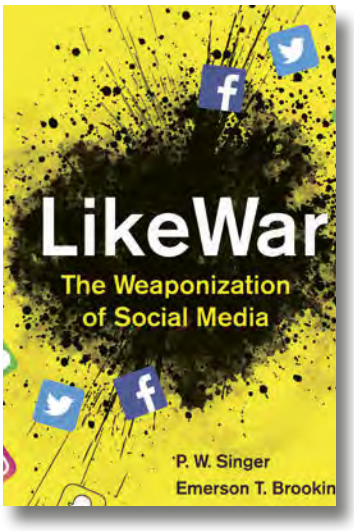
Space Wars is a nonfiction novel based on war-gaming findings. Set in the near future, a terrorist organization obtained access to a counter-space weapon that could cause irreversible damage to satellites. After disabling several western countries’ satellites, intelligence sources identified the weapon’s location, and a successful military operation neutralized the threat. The story explains the effects due to the degraded space services on the military, as well as on the civil environment. The book unveils critical vulnerabilities of, and dependencies on, space services, and describes the weakness of the security and safety environment of western nations. Other actors, rogue countries as well as criminal organizations, realized the weakness and tried to exploit it for their purposes. After analysing the situation, western countries execute several approaches to regain the common space services, including the use of spares, finding alternatives, or restoring capabilities. While these approaches return a semblance of normal life to the world, the story assesses how vulnerable the worldwide network of space-based services (communication, navigation, military applications) is, and how the dependencies (military and civil) are interconnected and interact. This book gives a broad and technically-proven overview on potential threats to space services, and the results of degradation on the life of mankind. All described technology to threaten satellites and to restore lost capabilities is realistic – i.e. either under development or already existing. One should view the book as a forewarning of possible future threats, either from terrorist organizations or international conflicts. ●

‘LikeWar – The Weaponization of Social Media’

Like War – The Weaponization of Social Media is an in-depth account of the ways in which social media has developed in to more than a means of communicating with our friends and family, into a weapon which takes information warfare to another level. Moreover, the realm in which social media exists, the internet, can now be considered a fully-fledged military operational environment.

Through a series of engaging profiles the authors, P. W. Singer and E. T. Brooking, explore the new reality and consequences facing each of us as we attempt to interact with the larger world via social media. Well organized with a vernacular easy to follow, Like War seeks to show us the hazards we are already encountering on a daily basis. The hope is we are better able to understand, and when necessary, arm ourselves with at least an appreciation of what is transpiring around us.

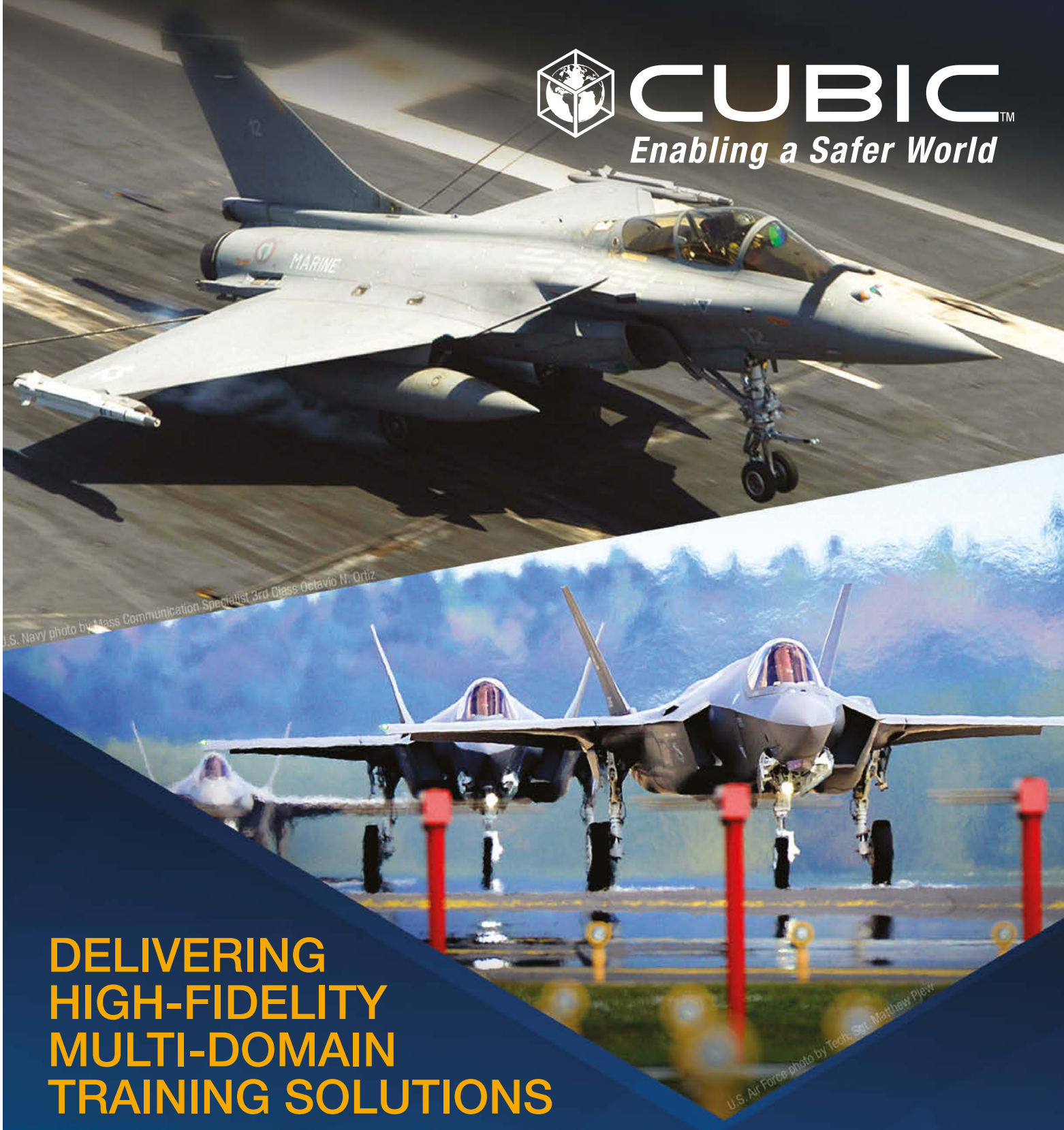
This is an excellent book for anyone regularly utilizing social media, in particular the modern warfighters seeking a better understanding of information warfare and the terrain in which it is fought. ●



By P. W. Singer and Emerson T. Brooking, Eamon Dolan/ Houghton Mifflin Harcourt, 2018

Reviewed by:

Lt Col Henry Heren, USA AF, JAPCC



CUBIC™

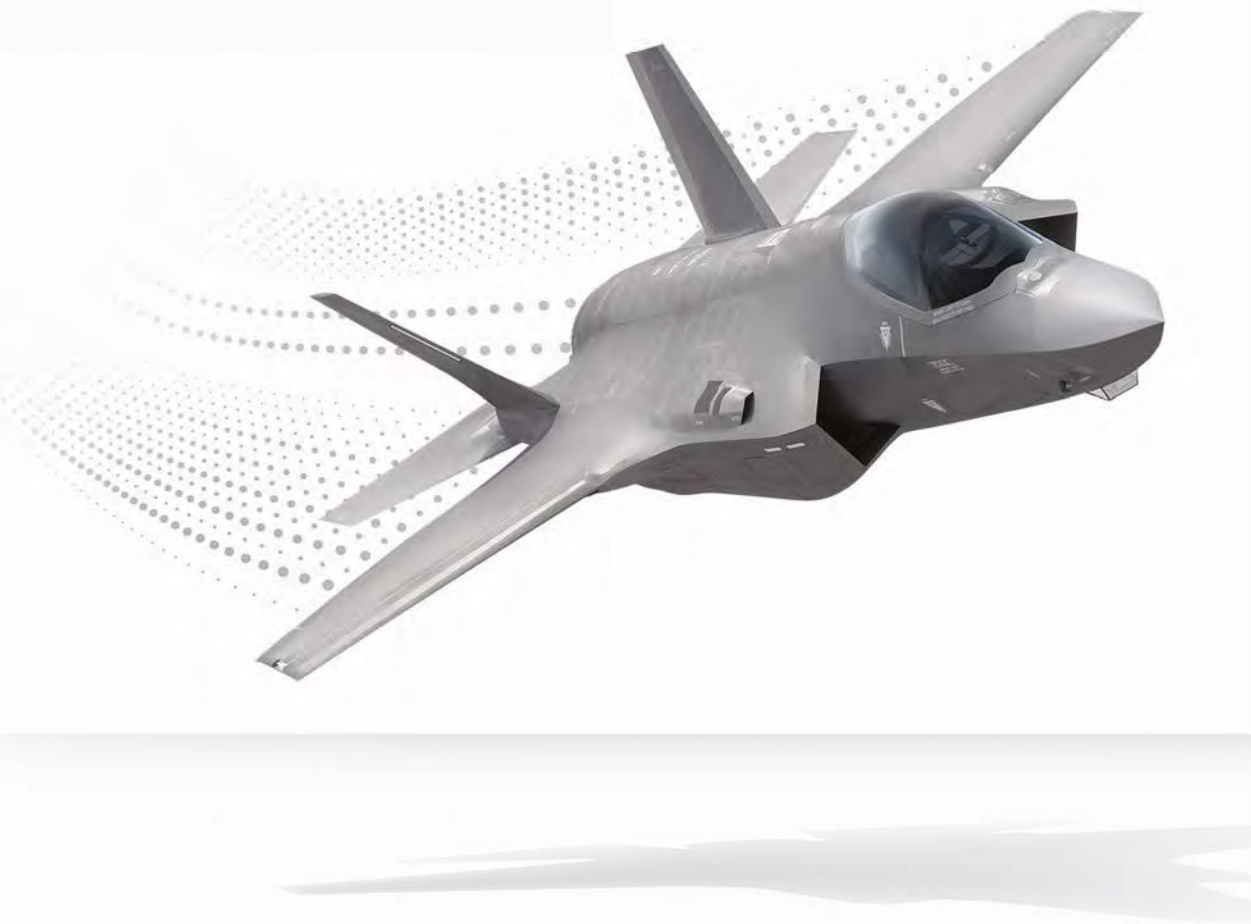
Enabling a Safer World

DELIVERING HIGH-FIDELITY MULTI-DOMAIN TRAINING SOLUTIONS

Cubic is proud to sponsor the JAPCC Joint Air & Space Power Conference. We are committed to providing innovative multi-domain training solutions that support NATO training and readiness efforts worldwide.

Learn more about our next generation of training solutions at **cubic.com/training**

The F-35, the United States and NATO: An alliance forged in excellence.



Both the United States and NATO are each propelled by a diverse set of goals. Inspired by them, we made it our mission to build the F-35. With stealth technology, increased range, weapons capacity and advanced sensors, the transformational F-35 is the most lethal, survivable and connected fighter in the sky. The F-35 gives our men and women an advantage against any adversary and any threat — today and for decades to come.
Learn more at F35.com.

Lockheed Martin. Your Mission is Ours.™

LOCKHEED MARTIN