Transforming Joint Air and Space Power

The Journal of the JAPCC

Edition 31, Winter/Spring 2021

PAGE 6

The Need for Speed

More and Better Military Tools are Not Enough

PAGE 32

Cybersecurity Challenges

Leverage New Technologies in Modern Battlefields

PAGE 80

Italian Bio-transport During COVID-19

Blueprint for the Alliance

As I near the end of my five years in Kalkar it is my privilege to introduce the 31st edition of *Transforming Joint Air and Space Power – The Journal of the JAPCC*. Throughout my time here as the Chief of Staff, I have worked with a tremendous team from our 16 sponsoring nations as well as more than 100 contributing authors from around the world who have provided timely and thought-provoking contributions to inform the Air and Space Power Community of Interest on challenges facing the NATO Alliance and our partners.

Issue 31 addresses some hot topics in the Alliance today including 4th and 5th Generation systems integration, emerging hypersonic technologies, AI support to Battlespace Management, and the evolution of the Cyberspace and Space domains in NATO.

Our Assistant Director Brigadier General Giuseppe Sgamba opens this Journal reflecting on a challenging 2020 and the 'The Need for Speed' to remain the most advanced military in the world. 'Employment Considerations for 5th Generation Systems' and 'The Italian Air Force's International Flight Training School' address developments in the Air domain. 'Crossroads of Technologies and Authorities' and 'Future Battlespace Management' highlight different aspects of C2 challenges coming along with modernization and new technology which goes in hand with 'Cybersecurity Challenges with Emerging Technologies'.

The next two articles 'Hypersonic Threats' and 'Distance no Longer Equals Protection' take a critical look into emerging hypersonic technologies. A selection of different challenges regarding emerging technologies in Space and the Space domain itself are covered in 'NATO Space', 'Responsive Space for NATO Operations', 'Shortfalls in NATO Space Education' and 'Exploring Synergistic Potential of the Portuguese Space Strategy'. The Journal moves on to a View Point on 'Electromagnetic Operations in "Grey Zone" Conflicts' inspiring thoughts on a new undeclared form of warfare; and last but not least, 'Italian Bio-transport during COVID-19' examines a number of relevant considerations during this challenging time and the importance of such a critical capability.

The JAPCC has been at the forefront of Joint Air and Space transformation since its founding in 2005, which prompted us to develop a historical volume documenting the first 15 years of JAPCC work. Included with this issue of the Journal is an 8-page Gatefold flyer to provide a preview of the book, which will detail the substantial return on investment NATO has received from the JAPCC thus far.

Thank you for taking the time to read this edition of our Journal, I sincerely hope that it stimulates your thinking about important Air and Space Power issues facing our Alliance and our Nations. If it prompts you to share your own thoughts as either a comment on a particular article, or by submitting an article you yourself have developed as an Air and Space Power practitioner, I encourage you to reach out to us via our website: www.japcc.org, or via email: contact@japcc.org. If you do not already do so, you can also follow us on Facebook, LinkedIn or Twitter to keep abreast of the latest issues in our COI.

Brad A. Bredenkamp
Colonel, US AF
Chief of Staff, 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

Out of the Box

Inside the JAPCC

Book Reviews

Imprint:

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

Director
Joint Air Power Competence Centre
Gen Jeffrey L. Harrigian

Executive Director
Joint Air Power Competence Centre
Lt Gen 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 Henry Heren
Lt Col Paul MacKenzie
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.

Follow us on Social Media

The Need for Speed

More and Better Military Tools are Not Enough

By Brigadier General Giuseppe Sgamba, IT AF, Assistant Director JAPCC

Introduction

2020 was a challenging year, as we continued to provide deterrence and security for our Alliance in the face of the CoVID-19 Pandemic. I was impressed by the way all of us continually found innovative ways to work effectively together while remaining socially distanced. This is not the way we have traditionally functioned, neither within our militaries nor in the Alliance, but we were able to leverage emerging technologies and continue to advance NATO's Air and Space Power to remain the strongest combined force in the world.

With the continuing separation we face while our nations pursue the medical answers to this pandemic, it is difficult to coordinate and make decisions rapidly without the face-to-face coordination we are used to. However, technology does not feel the effects of a pandemic virus and continues to evolve at ever-increasing rates. To keep pace with more capable and faster technology, we have to be able to make decisions faster. When decision-making bodies are prevented from coming together, rapid decision-making becomes dependent on the rapid sharing of information across networks, and the effective use of virtual meeting capabilities that enable us to assess, decide and act with speed.

Speed of Relevance

Speed is perhaps the most cross-cutting political and military requirement for ensuring the security and defence of our Alliance. The contemporary global environment in which we live and work presents our nations and NATO with a rapidly evolving set of challenges and threats, enabled by innovative new technologies that can create effects quickly and in some cases with very little warning. In order to counter and defend against these threats or better yet deter the actors who pose them, we must be able to collectively leverage emerging technologies, network them together, make decisions and apply power across all domains at the 'Speed of Relevance'. Simply having more and better military tools is not enough, if those tools and forces can be disrupted, degraded, deceived or delayed and cannot be employed in time to deliver decisive effects.

Speed is a core tenet of Air Power. It allows us to cover great distances in a short period of time to mass forces at the most effective point, or to react to incoming threats quickly to deter or neutralize them. This also enables us to provide an umbrella of Air Superiority over an area of operations that enables freedom of manoeuvre for Land and Maritime forces as well as for Air Mobility operations such as Airdrop, Air Refuelling and logistics support. Air Superiority, or in many cases Air Supremacy, has been a security blanket over Allied forces for decades, with friendly forces able to conduct operations free from almost any threat of enemy interference from above. However, our great historical track record does not guarantee this will continue to be the case. Right now, we see our peer competitors investing heavily in and gaining ground on their ability to contest the Alliance's control of the Air domain, thus enhancing their own ability to threaten our forces from the air as well.

This evolution in our Air Power tools necessitates an adaptation of our warfare model and the way the Alliance approaches conflicts in the future. We are exploring the concept of Joint All Domain Operations (JADO) to help us better harmonize our efforts to optimize the effects generated by our forces across all domains by integrating their planning, and synchronizing their

© JAPCC

execution at a tempo and level of flexibility sufficient to effectively accomplish the mission. This level of complex execution will drive the requirement to be able to provide robust, resilient Command and Control (C2) across all domains in the form of Joint All Domain Command and Control (JADC2).

Networking and Data Sharing

As the ongoing introduction of advanced generation capabilities like the F-35 into NATO's national inventories shows, we are not resting on our laurels, but are continuing to evolve and integrate faster systems


© Aeronautica Militare

of our own. However, having faster shooters only gives us an advantage when we are able to coordinate data from multiple sensors into usable targeting information and transmit it to the shooters in time to be relevant. These advanced Air capabilities are highly dependent on Space-based data, products and services that provide situational awareness, indications and warnings, communications, navigation capability, and more with great precision and at high rates of speed. Overhead sensors allow us to see and sense at far greater ranges than the terrestrial horizon allows for surface-based or even airborne platforms. This also contributes to better informed, faster, or at least earlier decision-making.

I want to point out that this is not just an Air and Space problem; it involves threats across not only the operational domains of Air, Land, Maritime, Space and Cyberspace, but also within the human, political, economic and information environments. So as we look at training and equipping our existing force structure to be interoperable and ready to employ rapidly; at integrating emerging technologies into that force structure in ways that multiply the capabilities of all generations of systems; and being able to detect and defend against a fast-moving military adversary, we must be cognizant that there are non-military elements that have roles to play and these elements must operate at the speed of relevance as well in order for our Alliance to succeed in its three core tasks.

Space Support

These non-military elements are just as dependent on the Space-based communications, navigation, timing, weather data and other products and services as our militaries. Increasing civil use of and access to Space highlights the need to not only deconflict activities through shared awareness for safety reasons, but also to secure the Space-based assets that provide all of the services already noted and secure the networks over which they transmit information. The recognition of the growing presence in Space and the dependence on its capabilities resulted in the Alliance recognizing Space as a fifth operational domain just over a year ago in December 2019. Several of our nations have already begun to stand up separate Space Forces, and in order to ensure the coordination of needed support to NATO, an Initial Implementation Plan was approved in 2020 that included direction for the creation of a NATO

Space Centre, which NATO Defence Ministers agreed will be co-located with Allied Air Command at Ramstein Air Base[1]. This Space Centre will be the focal point in the European Theatre for coordinating Space support from nations to the Alliance and for developing advice and options on Space matters for the Supreme Allied Commander Europe and for the North Atlantic Council.

Information Protection and Sharing

In order to take full advantage of the impressive Space capabilities of our spacefaring NATO nations, we have to be able to protect the platforms and secure Cyberspace and the Electromagnetic Spectrum (EMS) through which they collect and disseminate information. Securing Cyberspace and competing effectively in the information environment through assured access to the EMS are both substantial issues in their own rights, and are areas where we need to get stronger or in some cases even catch up to our near-peer competitors. How we do this is already the subject of other ongoing studies and efforts, but for now we need to recognize that these two new domains and the EMS are of paramount importance for the Command and Control (C2) of military operations across all domains, and also key to the sharing of information that supports trust, cooperation and rapid decision-making in the political sphere to approve those operations when necessary.

Conclusion

NATO will continue to have the most advanced military tools in the world and the best-trained and educated people to employ them so that we can maintain Air and Space Superiority over any Battlespace. This nice military toolkit will not be enough unless we ensure we have the doctrine, standardization agreements, and political policies in place to support the rapid employment of Air and Space Power when needed, and to guarantee our communication and C2 networks are hardened and resilient enough to enable data analysis, information-sharing, decision-making and the distribution of orders at the 'Speed of Relevance'.

1. 'NATO's Approach to Space', https://www.nato.int/cps/en/natohq/topics_175419.htm, 23 Oct. 20.

Brigadier General Giuseppe Sgamba

born on 22 July 1963 in Rome, Italy. He attended the Italian Air Force Academy from 1982 to 1986.

In his operational tours he has served as Weapon System Operator in 36th Fighter Wing at Gioia del Colle – Italy, in the Royal Air Force in Cottesmore, UK, as flying instructor for operational tactics (Conventional all-weather fighter-bombers), and at the 6th Wing at Ghedi Air Base as 406 operational technical service Squadron Commander.

As Colonel he was Commander of the EW Operational Wing from 2009 to July 2012.

He has participated, with different roles, in the following operations: Gulf War 1990, NATO Kosovo Operation 1999, and NATO Unified Protector Libya 2011.

He served in Washington-DC (USA) as national representative of the C4I Interoperability Team, within the F-35 Joint Strike Fighter program and in Italy, within the 4th Innovation and Logistics Department of the Italian Air Force General Staff, in charge of the EF2000 aircraft development and in country in-servicing.

As Brigadier General he was Commander of the Air Force 4th Brigade Telecommunications, Air Defence Systems and Air Navigation Services from 2014 to 2016 and Deputy Chief of the Information and Security Department of the Italian Defence General Staff responsible for INTEL Policy, EW, Asymmetric Threat and Satellite Earth Observation.

Currently he is serving as Assistant Director of the Joint Air Power Competence Centre in Kalkar, Germany.

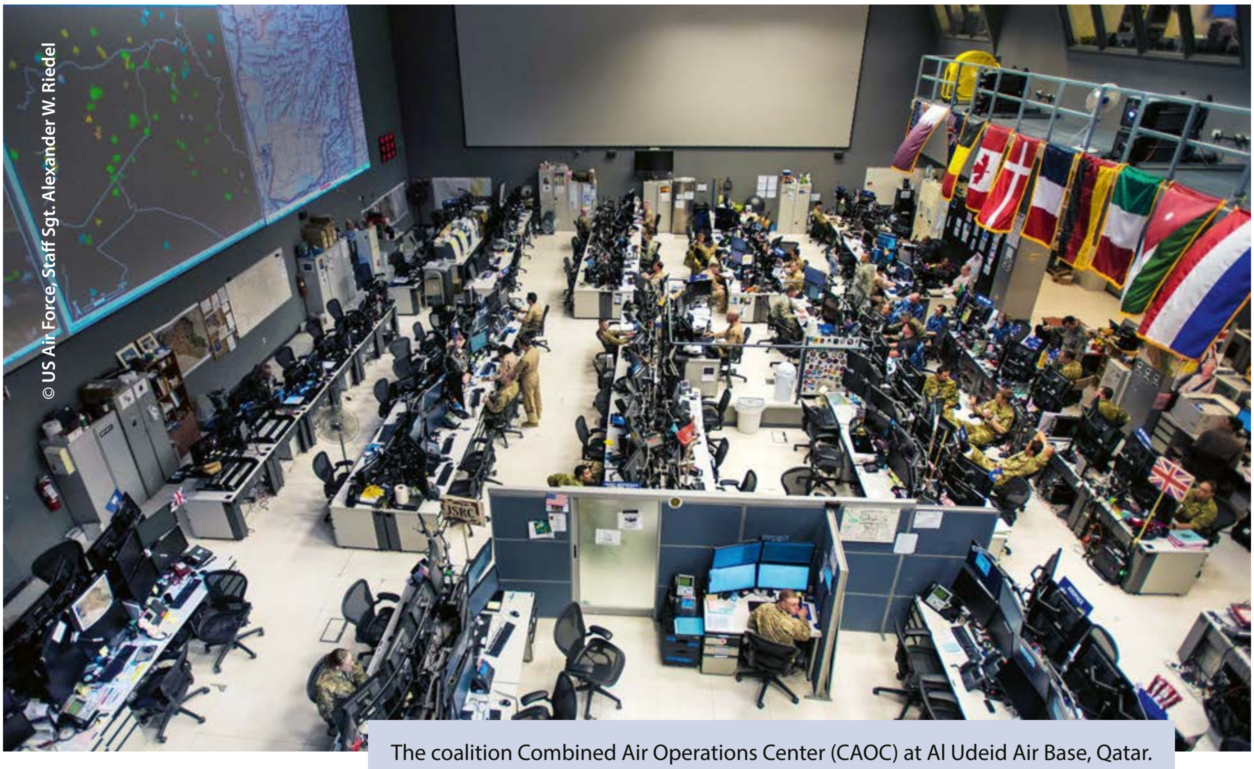
Employment Considerations for 5th Generation Systems

Incorporating F-35 Capabilities into NATO-led Operations

By Captain Daniel Cochran, US N, JAPCC

Introduction

When considering the complexities of modern warfare, including the targeting of military objectives in contested, congested, and rapidly shifting environments, the ability to quickly and precisely identify and counter adversarial strategies has never been more challenging. Swiftly and accurately discerning the type and affiliation of an object of interest is paramount to choosing the most advantageous tactical action. When considering the use of force, war-fighters must first ensure that the basic Law of Armed Conflict (LOAC) rule of distinction is met, in that there must be a reasonable belief the object being attacked is a military target based on all information at their disposal at the time.[1] In addition to this legal requirement, for policy reasons nations may specify heightened identification requirements through Rules of Engagement (ROE) necessitating Positive Identification (PID) prior to attack. While the definition of the term PID has evolved over time and among nations, in 2003 it was defined during *Operation Iraqi Freedom* by the coalition nations as 'a reasonable certainty that the proposed target is a legitimate military target'.[2] PID can be derived from observation and analysis of target characteristics including visual recognition, electronic signatures, non-cooperative target recognition techniques, identification friend or foe systems, or other identification techniques.[3]


© US Air Force, Staff Sgt. Alexander W. Riedel

The coalition Combined Air Operations Center (CAOC) at Al Udeid Air Base, Qatar.

As military technologies continue to advance at disparate levels throughout the Alliance, the potential to determine PID at tactically significant ranges and with precise geospatial coordinates has dramatically increased. So that it is possible to take full advantage of new weapons systems across the coalition force, state-of-the-art capabilities and derived intelligence must be shared throughout the fighting force. Information barriers that result from both policy and differing infrastructure between nations are certainly not a new issue within the Alliance. In fact, nothing fundamentally changes with the addition of the F-35 except that the negative effects of these information barriers are likely to be more substantial than they have been during previous generational upgrades.

This article describes how 5th generation systems have the potential to enable substantial improvements in providing more timely and accurate information, such as PID, leading to target engagement possibilities at longer ranges and with a higher operational tempo. However, since only a portion of NATO nations are employing the F-35, combined with the observation that it is highly likely the majority of NATO aircraft employing effects will not be 5th generation for the foreseeable future, the United States (US) and allied F-35 nations must make it a priority to reduce information-sharing barriers so as to field the most effective force possible.

PID Inside of ROE

In order to solve for the PID requirements detailed within the ROE, a 'PID matrix' is often given to tactical forces listing the combination of specific information required to meet an acceptable threshold. Since ROE are frequently local, addressing a given set of circumstances, the 'PID matrix' is also often unique, tailored for geopolitical issues along with assessments of adversary and friendly equipment as well as a nation's Tactics, Techniques, and Procedures (TTPs). The minimum requirements to solve for PID are provided for the purpose of abating unintended consequences (non-combatant, neutral, and friendly casualties), while enabling friendly forces to act effectively and decisively.

A typical 'PID matrix' includes heightened identification requirements beyond the LOAC 'reasonable belief' threshold to attack a target. Before electronic identification systems, distinction was often solved for visually.

A lawful combatant could see the enemy wore a different uniform, wielded foreign weapons, employed enemy tactics, and potentially possessed different physical features than their own forces. In air combat, a pilot could rendezvous in a position that was obscured from an opposing aircraft's sensors (including the pilot's field of view) and determine the nationality of the aircraft prior to engaging. In some situations, Point of Origin (POO) was also used. Based on the commander's understanding of the battlespace, orders were given directing lethal force be used on all forces meeting specific criteria, such as originating from a particular direction or located in a specific area (with other caveats, as required).

Using electronic systems to identify an object of interest began in the early stages of World War II with the development of the radar. National initiatives such as

Project Cadillac, conducted at the Massachusetts Institute of Technology, created the first airborne radar and subsequent Airborne Early Warning (AEW) aircraft.[4] Electronic capabilities continued to progress during the Cold War and the modern concept of Electronic Identification (EID), as it contributes to meeting the requirements of distinction, was employed during the Vietnam war by US aircraft with radar warning receivers able to identify ground-based targeting radars and provide some situational awareness regarding the location and type of air defences being employed.[5] With each new generation of weapons systems, the ability to electronically identify and provide the location of an object of interest has improved.

Using EID to Solve for PID

EID can be determined autonomously or manually, depending on approved ROE. When made autonomously, a computer system determines a target's identity-based on algorithms resident in the software, programmed by the manufacturer, or in some cases, by the tactical system operator. EID can also be accomplished manually by the tactical operator deciphering system-generated identification information from single or multiple sources and comparing this information with the 'PID matrix' to determine the identification of the object of interest. In other words, manual EID occurs by a human processing pieces of computer-generated *data* to determine *intelligence*. During autonomous EID, the computer system analyses the data and provides the intelligence directly to the operator.

As with any method used to determine the identification of an object, an EID will have a related level of confidence that the identification is correct, based on the technical details of the systems used to obtain the EID. The confidence level of an EID obtained from a single source, or through combinations of multiple sources, is considered to determine when the threshold for PID is met. Although the PID matrix will list many other considerations that aren't associated with EID to determine PID, there are situations where the confidence level of an EID is so high that it can be the sole source used to establish PID.

With each generational upgrade, the ability of military aircraft to provide EID has become more robust in terms of effectiveness, reliability, and automation. 5th generation systems are able to *fuse* multispectral signatures of objects of interest, greatly increasing the confidence level of an EID and also providing autonomous EID, minimizing operator workload. This higher quality EID has the potential to assign 'hostile' declarations to objects that friendly forces previously were unable to PID. This capability has the potential to dramatically improve coalition effectiveness and considerably increase the speed of the kill chain. However, there are obstacles that could limit these improvements.

For most state-of-the-art weapons, the details of the capabilities and actual confidence levels of EIDs are held nationally to safeguard them from competitors and potential adversaries. Since the F-35 has been an international programme from the start, the ability to share aircraft capabilities are similarly held,[6] whereby during future coalition operations comprised of both partner and non-partner F-35 nations, many tactically-important details such as EID capabilities of the F-35 may be restricted from being shared.

Intelligence Exchange Enables Effectiveness

During the execution phase of an operational plan, it is paramount that tactical units remain flexible so that they can be reassigned as the scenario develops. The operational-level joint targeting process links strategic-level direction with tactical-level execution. During the targeting process, air assets available to the operational commander for tasking are assigned missions based on their capabilities conducive to creating synchronized effects. Time-Sensitive Targets (TSTs) and targets developed through the Deliberate Dynamic Targeting (DDT) process, including TSTs, High Value Targets (HVT), and High Payoff Targets (HPOT) can be fleeting and require a flexible approach where resources may need to be reassigned and missions reprioritized.[7] Responsibility for the result of delivered effects lies at all levels in the chain-of-command, from the staff on the operations floor to the airman employing the effects. Each level must ensure the engagement is valid as defined by ROE and LOAC, based on the facts available to them and those facts that they should have reasonably obtained.[8]

In 2011, during NATO-led *Operation Unified Protector* (OUP), senior national liaison officers in the Combined Forces Air Component Command (CFACC) performed the role of national 'red-card holders', an element of NATO doctrine used to resolve areas in which consensus does not exist for issues on a specific mission. 'Red-card holders' ensure the missions their national assets undertake meet their internal policies, and possess the authority to veto the use of their national assets if they are not convinced the operation complies with these policies.[9] During OUP, DDT was adopted as a means of responding to urgent tactical targets. Shown to be highly effective, one United Kingdom representative reported that by the end of the campaign, over 80% of the targets were DDT's.[10] However, the problem of intelligence sharing among coalition partners remained throughout the conflict. For instance, US-produced target folders and intelligence products were initially not releasable to NATO due to national classifications. Air Tasking Orders (ATOs) had to be tailored in an effort to assign coalition assets missions based on national policies combined with the ability to share intelligence within the coalition.[11] These restraints undoubtedly put limitations on the use of certain national assets which led to an overall reduction in coalition effectiveness and reduction in flexibility.

In addition to causing complications for target engagement (as shown in OUP), the sharing of intelligence is also required during the assessment phase of

© US Navy

the joint targeting cycle. Especially when considering TST and/or HVT/HPOT, information from all sources must be quickly collected and analysed to determine if re-engagement is required and the target is still accessible.[12] Intelligence generated from all sources, including 5^{th} generation systems, will be needed by 'red-card holders' from nations that have committed assets. Requests such as, 'show me how you know the system is still operating' or, 'how are you coming up with this updated location' are likely to occur and without information-sharing, 'red-card holders' will be forced to restrict the use of their assets and opportunities for tactical or strategic successes may be lost.

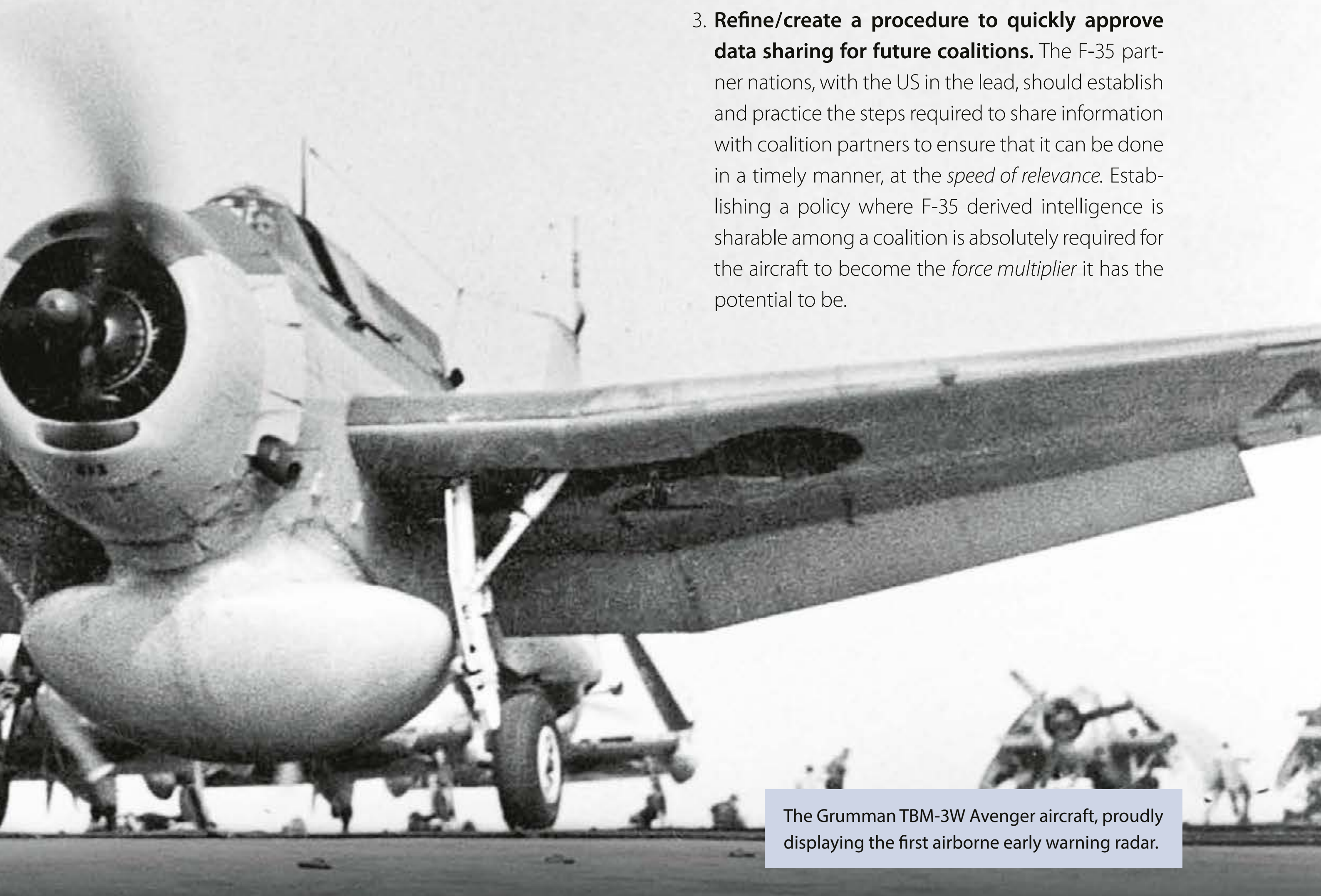
Recommendations

To address the intelligence and information barriers related to the employment of 5^{th} generation aircraft, the following steps should be considered:

1. **National leaders advocate for information and data sharing between and among all NATO nations,** with the appropriate level of detail to facilitate force packaging and common desired effects. The goal is to be able to share mission-specific and relevant information that enables interoperability and military cooperation. As early as possible in the acquisition process for future and current European F-35 programmes, holistic intelligence policies and requirements enabling this type of critical information-sharing should be established and refined, as necessary.

2. **Enhance the understanding of 5^{th} generation fighter capabilities with NATO planners.** NATO should ensure 5^{th} generation operators actively participate in operational planning and exercises, facilitating discussions at the appropriate security classification level to mitigate risk of erroneous conclusions being made by the training audience based on incomplete or incorrect information.

3. **Refine/create a procedure to quickly approve data sharing for future coalitions.** The F-35 partner nations, with the US in the lead, should establish and practice the steps required to share information with coalition partners to ensure that it can be done in a timely manner, at the *speed of relevance*. Establishing a policy where F-35 derived intelligence is sharable among a coalition is absolutely required for the aircraft to become the *force multiplier* it has the potential to be.



The Grumman TBM-3W Avenger aircraft, proudly displaying the first airborne early warning radar.

© US Air Force, Staff Sgt. Natasha Stannard

As an added benefit, effort given to more inclusive intelligence policies may provide nations an opportunity to proactively reduce national caveats. Although these political and legal variances will remain to some degree, they add complexity to operational plans and limit flexibility during execution. Especially when considering the case of a peer adversary, clear and consistent ROE throughout the coalition will go a long way to achieving the full potential of the declared forces. With renewed emphasis being given to joint, effects-based operations through emerging concepts such as Close Joint Support (CJS)[13] and Joint All Domain Operations (JADO)[14], solving information-sharing and classification issues will continue to be paramount in order to fully synchronize the combined capabilities and efforts of NATO militaries.

1. Protocols Additional to the Geneva Conventions of 12 Aug. 1949, Part IV Civilian Population. Available online: https://www.icrc.org/en/doc/assets/files/other/icrc_002_0321.pdf.
2. Operational Law Handbook, 2015, Chapter 5: RULES OF ENGAGEMENT, Armed Conflict: OPERATION IRAQI FREEDOM: CLFCC ROE Card, pp. 109. Available online: https://www.loc.gov/rr/frd/Military_Law/pdf/OLH_2015_Ch5.pdf. Accessed 28 Jul. 2020.
3. Department of Defense Dictionary of Military and Associated Terms, Joint Publication 1-02, Nov. 2010, Amended Feb. 2016, p. 187.
4. See http://steeljawscribe.com/2010/10/06/project-cadillac-the-beginning-of-aew-in-the-us-navy for more information.
5. See https://www.airspacemag.com/military-aviation/missile-men-north-vietnam-180953375/?page=2 for more information.
6. F-35 Joint Strike Fighter (JSF) Program, Congressional Research Service, 27 May 2020.
7. AJP-3.9, Allied Joint Doctrine for Joint Targeting, Edition A, Version 1, Apr. 2016: para. 0103, 0104, 0108, 0109, 0110, 0208.
8. AJP-3.9, Allied Joint Doctrine for Joint Targeting, Edition A, Version 1, Apr. 2016: para. 0121b.
9. Mueller, K., et al., 'Precision and Purpose: Airpower in the Libyan Civil War', RAND Corporation, 2015, p. 143.
10. Ibid., p. 176.
11. Ibid., p. 143–151.
12. AJP-3.9, Allied Joint Doctrine for Joint Targeting, Edition A, Version 1, Apr. 2016: para. 0208g.
13. Cochran, D., et al., 'Reshaping Close Support, Transitioning from Close Air Support to Close Joint Support', JAPCC, Jun. 2020.
14. Air Force Role in Joint All-Domain Operations, Curtis E. Lemay Center for Doctrine Development and Education, 1 Jun. 2020.

Captain Daniel D. Cochran

graduated in 1998 from Rensselaer Polytechnic Institute with a Bachelor's Degree in Materials Science and Engineering. He was designated a United States Naval Aviator in 2001. He is a distinguished graduate from the Air Force Institute of Technology earning a Master's of Science in Aeronautical Engineering. A graduate of the United States Naval Test Pilot School, he has completed tours as a test pilot and instructor. In the fleet, CAPT Cochran has completed 14 aircraft carrier deployments while assigned to F/A-18E and F/A-18C squadrons. During his most recent tour, he commanded the 'Royal Maces' of VFA-27, attached to CVW-5, homeported in Atsugi, Japan. He has accumulated over 3,200 flight hours in 32 aircraft, including 760 carrier-arrested landings. He is currently serving as the Maritime Air Section Head at the Joint Air Power Competence Centre.

© IFTS/Leonardo

The Italian Air Force's International Flight Training School

The Next Level of Training – Excellence for Military Pilots

By Colonel Gianfranco Liccardo, IT AF

Setting the Stage

The Italian Air Force's (ITAF) world-renowned excellence for flight training and the Leonardo Company's leadership in integrated-training solutions come together to create the brand new International Flight Training School (IFTS) in Italy. The announcement of this joint venture between the Italian Air Force and Leonardo was made on 17 July 2018 at the Farnborough International Airshow.

The IFTS's objective is to consolidate the growth and the internationalization process already in place in the ITAF by increasing capacity and the range of courses available to foreign countries in order to satisfy a growing demand for advanced flight training from allied and partner air forces. The IFTS delivers advanced Phase IV (lead-in Fighter Training) courses using the ITAF training syllabus, to adequately prepare the student pilot to operate the 4th and 5th generation fighter aircraft.

The IFTS offers customized training modules, in line with the modern Air Force's requirements, to best help the student pilot achieve the desired level of competence, further decreasing the amount of costly flight hours from Operational Conversion Units (OCU), saving time and valuable resources.

The IFTS is characterized by an international pool of military and former military instructor pilots, selected and trained following the 'Train As You Fight' principle.

The school has a brand and vast experience the ITAF acquired over decades of training both national and international combat pilots.

The Hardware

Leonardo contributes to the new IFTS with four M-346 advanced-trainer aircraft that complement the existing 18 T-346 aircraft in the fleet. All aircraft are equipped with the Embedded Tactical Training System (ETTS), which is in service with some of the most demanding Air Forces, including Israel, Singapore, Poland and Italy. IFTS also operates a Ground Based Training System (GBTS) with full state-of-the-art training devices, including Full Mission Simulators and above all a fully operational and leading edge Live, Virtual, and Constructive (LVC) environment, for maximum cost-effectiveness. A key element of LVC is the option to interconnect multiple simulators to one or more T-346s in real-time flight. The ETTS technology on board the aircraft enables the simulation and utilization of various sensors, electronic countermeasures and armament. These modern tactical simulation techniques generate highly realistic virtual operational environments, which are fundamental to the advanced and pre-operational training process.

More precisely, the collaboration between the ITAF and Leonardo further exploits the training capabilities of the 61st Wing at Lecce-Galatina Air Base (Apulia Region) and has facilitated the establishment of a new IFTS at Decimomannu Air Base (Sardinia) to support the increasing number of international requests for advanced pilot training.

The Advanced Training

To understand what IFTS is about, it is important to discover what happens in Galatina where the Italian Air Force 61st Wing is located and where the essence of the international Phase IV training is already in place. Each day, the constant presence of foreign pilots, students and instructors, encourages the exchange of experience and enhances the courses, as does the modularity and flexibility of the training syllabus.

Sitting in one of the briefing rooms of the 212th Squadron, 61st Wing, we listen to the expert ITAF instructor provide students with a detailed explanation of today's mission. 'Dragon 74' will face 'Dragon 75' and conduct a series of Basic Fighter Manoeuvres to gain an advantage during a simulated combat exercise. Once completed, the exercise will be repeated reversing the roles.

After receiving the latest updates about the mission in the operations room, the pilots go to the flight equipment room to gear up. A few minutes later they are conducting pre-flight checks on their assigned aircraft, which bear the patch logo of the IFTS on the tail fin.

Air-to-Air Refuelling (AAR), use of Night Vision Goggles (NVG), Beyond Visual Range (BVR) engagements, Air-to-Ground range events and use of Helmet Mounted Display (HMD) are just some of the advanced operational skills that students can be provided with, through the use of M-346 jets and the sophisticated simulation devices. The number of flying jets used in multiple-aircraft scenarios and real-time events are fewer because of the possibility to connect, in real-time, the students flying the actual aircraft with students sitting in a Full Mission Simulator (FMS) inside the GBTS.

The Infrastructures

The 61st Wing is where the ITAF performs basic and advanced flying training for the Italian and international student pilots. By the end of 2020, with the arrival of the new M-345 used for Phase II and III basic training, Galatina will reach capacity. Activities related only to advanced Phase IV of the syllabus will then move gradually to Decimomannu Air Base in Sardinia (Italy).


© ITAF/Leonardo

Multiple factors make Decimomannu the optimal location for the IFTS. It has excellent infrastructure, including two runways suitable to accommodate a high volume of training flights. Near to the Air Base, multiple well-suited training areas are present for advanced training to cover any simulated scenario. Modern ranges to conduct air-to-air and air-to-ground live firing are within a few nautical miles, such as an Autonomous Air Combat Manoeuvering Instrumentation (AACMI) range and the Poligono Interforze del Salto di Quirra (PISQ), a high technology instrumented Air-to-Ground/Air-to-Air/Electronic Warfare (A/G-A/A-EW) range.

A logistics and maintenance centre is being constructed that will include a new maintenance hangar and a flight line intended for T-346 ground handling, a new GBTS that will comprise of classrooms, offices and space to accommodate two Partial Task Trainers and two Full Motion Simulators. A new residential area is being built for both students and instructors to include 100 apartments, a restaurant, officer's club, sports facilities and a swimming pool. Construction work commenced in 2020 and the first advanced IFTS course for student pilots making use of the new structure at Decimomannu Air Base is planned for the beginning of 2022.

IFTS Mission

The IFTS, thanks to the ITAF's extensive and consolidated flight training expertise and to Leonardo's leadership in advanced integrated training systems, guarantees advanced, top level training for the modern air forces at reduced costs. In other words, the next level of training excellence for military pilots. In an era of expensive flying hours and reduced defence budgets, this military-industry partnership provides both an effective and affordable solution to keep aircrews at the peak of capability.

Colonel Gianfranco Liccardo

joined the Air Force Academy in 1995. In 1999 he received a Political Science degree and in 2001 completed pilot training at Sheppard AFB (USA). From 2002 to 2016 he was assigned to the 156th Sqn, flying the TORNADO and operating in Afghanistan (Operation ISAF), Lybia (Operation Unified Protection) and Iraq (Operation Inherent Resolve).

In 2017 he received a master's degree in Strategic Studies and was responsible for 'pilot training policy' at the Aerospace Planning Department of the ITAF Air Staff. From 2018 he is also working at the IFTS Project Team as Deputy Chief.

He is a command pilot with more than 2,500 flying hours.

Crossroads of Technologies and Authorities

By Lieutenant Colonel Henry Heren, US Space Force, JAPCC

'… with great power there must also come – great responsibility!'[1]

Introduction

The United States (US) Military, particularly its Air Force and Army, are pursuing technical capabilities to facilitate Command and Control (C2) in multiple domains and/or across all domains … a tremendous capability (great power) indeed. While these efforts are not being pursued exclusively in the US, the US is currently spearheading the discussion and research into these types of capabilities and in the process attempting to gain a clearer understanding of what this means for future military operations. This is particularly relevant for NATO, as other member nations and NATO-aligned organizations have begun exploring concepts associated with Multi-Domain Operations (MDO) and Joint All-Domain Operations (JADO). One aspect of specific importance to the Alliance as it forges ahead with developing technologies associated with improved C2 capability will be to avoid over fixation on emerging technologies to the extent that they overlook the legal authorities associated with C2 … the responsibility half of the coin.

This article explores some of the perceived seams between the emerging technologies associated with Joint All-Domain Command and Control (JADC2), and related concepts, and the current command structure within NATO (specifically Allied Command Operations [ACO] and Allied Air Command) regarding the differences between capabilities and authorities. This article will rely on NATO ACO published definitions and descriptions of the command structure to serve as a basis for the discussion.

The Current Structure

'ACO is a three-tier command with headquarters and supporting elements at the strategic, operational and tactical levels. It exercises C2 of static and deployable headquarters, as well as joint and combined forces across the full range of the Alliance's military operations, missions, operations and tasks.'[2]

At the top of the ACO structure is Supreme Headquarters Allied Powers Europe (SHAPE) which serves as ACO's strategic headquarters. 'Its role is to prepare, plan, conduct and execute NATO military operations, missions and tasks in order to achieve the strategic objectives of the Alliance.'[3]

The next level below SHAPE is considered the operational level and consists of three standing Joint Force Commands (JFC); one each in Brunssum (Netherlands), in Naples (Italy), and in Norfolk (US). 'All stand ready to plan, conduct and sustain NATO operations of different size and scope. Effectively, they need to be able to manage a major joint operation either from their static location, or from a deployed headquarters when operating directly in a theatre of operation.'[4]

In theory, any of the JFCs would be supported by the third tier, or the tactical level. This level is comprised of Single Service Commands (SSC), one each for Air, Land, and Sea. 'These service-specific commands provide expertise and support to the Joint Force Commands.'[5]

However, 'they report directly to SHAPE and come under the command of SACEUR.'[6] As will be discussed later, this arrangement can create interesting, possibly convoluted, interactions when the JFC Commander strives to align forces for a specific mission.

As mentioned, there is an SSC for Air which is located at Ramstein Air Base in Germany in the form of Headquarters Allied Air Command (HQ AIRCOM). The role of AIRCOM is to 'plan and direct the air component of Alliance operations and missions, and the execution of Alliance air and missile defence operations and missions.'[7] Far from just a headquarters, AIRCOM 'with adequate support from within and outside the NATO Command Structure can provide command and control for a small joint air operation from its static location, i.e., from Ramstein or can act as Air Component Command to support an operation which is as big or bigger than a major joint operation.'[8] Additionally, HQ AIRCOM has three subordinate air C2 elements: 'two Combined Air Operations Centres (CAOC) and a Deployable Air Command and Control Centre (DACCC). The air elements are also structured in a more flexible way to take account of the experience gained in NATO-led operations.'[9]

© Olivier Le Moal/Shutterstock.com

The Structure in a Crisis

When it comes to executing specific operations, the JFC has, at least in theory, some flexibility in how it organizes its assigned and/or attached forces:

> **'The JFC's mission and operational approach, as well as the principle of unity of command and a mission command philosophy, are guiding principles to organize the joint force for operations. Joint forces can be established on a geographic or functional basis. JFCs may centralize selected functions within the joint force but should not reduce the versatility, responsiveness, and initiative of subordinate forces. JFCs should allow Service and special operations tactical and operational forces, organizations, and capabilities to function generally as they were designed.'[10]**

Additionally,

> **'When JFCs organize their forces, they should also consider the degree of interoperability among Service components, with multinational forces and other potential participants. Complex or unclear command relationships are counterproductive to synergy among multinational forces. Simplicity and clarity of expression are essential.'[11]**

This seems to synchronize with HQ AIRCOM's approach:

> **'For crisis response operations, NATO's Air Command and Control structures are based on standing up a Joint Force Air Component – a command and control centre that plans and executes the delivery of NATO Air Power across the entire spectrum of joint operations. Allied Air Command is responsible for the standing up of the NATO Command Structure's Joint Force Air Component that will be specifically tailored in size for any NATO operation.'[12]**

As long as the JFC and SSC leadership agree upon an organizational structure, there are no issues.

'Key to reducing duplication within NATO will be examining ways the organization can reduce bureaucratic infrastructure, while maintaining only those organizations with the ability and authority to conduct operations utilizing emerging technologies.'

However, since the SSCs report to SACEUR, the JFCs can find themselves in situations where their desired command structure might not be implemented. In the relatively permissive environments and operations NATO has encountered in recent decades, any differences have had little to no operational impact. However, in a major operation against a peer or near-peer adversary (or adversaries), any differences could carry heavy consequences.

Inclusion of JADC2 Capability

In June 2020, the US Air Force published a doctrine that clearly defined JADO and JADC2:

JADO

'Comprised of air, land, maritime, cyberspace, and space domains, plus the EMS [electromagnetic spectrum]. Actions by the joint force in multiple domains integrated in planning and synchronized in execution, at speed and scale needed to gain advantage and accomplish the mission.'[13]

and

JADC2

'The art and science of decision-making to rapidly translate decisions into action, leverage capabilities across all domains with mission partners to achieve operational and informational advantage in both competition and conflict.'[14]

The doctrine also provides a vision, which 'calls for connecting distributed sensors, shooters, and data from all domains to joint forces, enabling coordinated exercise of authority to integrate planning and synchronize convergence in time, space, and purpose.'[15]

This vision requires an advanced modern communications infrastructure. To that end, the CSAF [Chief of Staff of the Air Force] singled out a FY2021 [fiscal year 2021] budget proposal request for USD 435 million for a digital architecture and cloud architecture 'to be able to not only connect the Air Force, but to connect the joint force.'[16]

However, it is important to recall that 'command is the authority a commander in the armed forces lawfully exercises over subordinates by virtue of rank or assignment. Accompanying this authority is the responsibility to effectively organize, direct, coordinate, and control military forces to accomplish assigned missions.'[17] Hence, while the US Air Force is pursuing technologies to C2 across all operational domains, it does not possess the authority to C2 across all domains. Therefore, and from a NATO perspective, neither does HQ AIRCOM.

The authorities of command for an operation are delegated from SACEUR to the assigned JFC. With the JFC possessing the technical capability to command across all domains, the question arises as to what role the SSCs (including AIRCOM) would provide, other than expertise; expertise which could be re-assigned to the standing JFCs.

One could argue whether SACEUR needs to maintain three standing JFCs, particularly if that capability resides at SHAPE? While there is some merit to this perspective, it must be remembered that the SSCs do not possess the authority across domains; these authorities reside with SACEUR, other than when delegated to the JFCs.

Of course, the elephant in the room during this discussion is politics. SHAPE, the JFCs, and the SSCs reside in seven different NATO nations. So, even if there is agreement that NATO has too many permanent organizations, given that the ability to C2 across domains resides similarly at each, the host nations would most likely consider 'the other' organizations as redundant rather than those they themselves host.

Conclusion

JADC2 creates the possibility for operational and even financial streamlining, yet faces hurdles from the services and, in NATO's case, national political parochialism. The US Air Force's idea for JADC2 is 'greater decentralized execution, a higher degree of delegated authority, and less dependence on central planning and mission direction than recent, low-intensity conflict operations.' [18] For NATO, with a top-heavy command structure, the challenge to not only delegate authorities but also reduce bureaucracy may present a higher hurdle than the integration of the technologies which enable JADC2.

Still, NATO possesses an interoperability policy, which aims to ensure the ability of the Alliance to operate together effectively to achieve mission goals and objectives. Indeed, 'Interoperability reduces duplication, enables pooling of resources, and produces synergies among all Allies, and whenever possible with partner countries.'[19] Key to reducing duplication within NATO will be examining ways the organization can reduce bureaucratic infrastructure, while maintaining only those organizations with the ability and authority to conduct operations utilizing emerging technologies. NATO may soon have at its disposal capabilities which will greatly enhance its ability to ensure the collective defence of its member nations, but more importantly will it also possess the ability to act efficiently in light of these advancements?

1. Lee, Stan and Steve Ditko. Amazing Adult Fantasy #15: Spider-Man, Marvel Comics, Aug. 1962. Page 13.
2. NATO Allied Command Operations (ACO), 28 Nov. 2019. Available from https://www.nato.int/cps/en/natolive/topics_52091.htm [accessed on 30 July 2020].
3. Ibid.
4. Ibid.
5. Ibid.
6. Ibid.
7. Ibid.
8. Ibid.
9. Ibid.
10. US Joint Publication 3-0, Joint Operations, Change 1, 22 Oct. 2018. p. IV-4.
11. Ibid, p. IV-5.
12. The Joint Force Air Component: We Respond to Crisis. Available from https://ac.nato.int/missions/jfac [accessed on 30 Jul. 2020].
13. Air Force Doctrine Annex 3-1, Department of the Air Force's Role in Joint All-Domain Operations (JADO), 1 Jun. 2020, p. 5.
14. Ibid.
15. Ibid, p. 6.
16. Congressional Research Service Report, Defense Capabilities: Joint All Domain Command and Control, 6 Apr. 2020, p. 2. Available from https://fas.org/sgp/crs/natsec/IF11493.pdf [accessed 30 Jul. 2020]
17. U.S. Joint Publication 3-0, Joint Operations, Change 1, 22 Oct. 2018, p. II-1.
18. Air Force Doctrine Annex 3-1, Department of the Air Force's Role in Joint All-Domain Operations (JADO), 1 Jun. 2020, p. 7.
19. North Atlantic Treaty Organization (24 Mar. 2020) Interoperability: Connecting NATO Forces. Available from https://www.nato.int/cps/en/natolive/topics_84112.htm [accessed 30 Jul. 2020].

Lieutenant Colonel Henry Heren

is a NATO Space & Cyberspace Strategist assigned to the JAPCC. He is a Master Space Operator and a Fully Qualified Joint Staff Officer with operational and planning experience in the Pacific, Europe, Africa, and the Middle East. After more than 28 years' service in the US Air Force, he transitioned to the US Space Force in 2020. He is a graduate of the US Air Force Weapons School, with experience in assignments focusing on Space, Cyberspace, and Electronic Warfare Operations.

Future Battlespace Management

Fighting and Winning in the Increasingly Complex Air Operations Environment of the Future

By Lieutenant Colonel Livio Rossetti, IT A, JAPCC

Introduction

Robust Anti-Access and Area-Denial (A2/AD) structures, coupled with the proliferation of advanced technologies across multiple domains, will dominate the third dimension in the coming decades. Potential adversaries will blend conventional, asymmetric, and hybrid capabilities across each of the traditional physical domains (Air, Land and Maritime) plus Cyber and Space, and will adjust their strategies by utilizing these advancements in an attempt to overwhelm NATO's strengths. This could compromise NATO's freedom of manoeuvre, reduce its effectiveness in deterring potential aggressors and undermine stability along the Alliance's borders. A more comprehensive approach is needed for correctly dealing with these security threats, and effectively operating in this type of 'multi-domain environment'. It will be fundamental for NATO to develop new strategies that allow a more integrated and synchronized use of forces which can outmanoeuvre adversaries across multiple domains at speed. Recently, there have been numerous papers, studies, and articles proposing a new way of viewing the future battlespace. The previous United States (US) Air Force Chief of Staff (CSAF) General David L. Goldfein, recently summarized his vision in a simple comprehensive concept 'Victory in future combat will depend less on individual capabilities and more on the integrated strengths of a connected network available for coalition leaders to employ'.[1] It is time to embrace a transformation process that leads NATO forces to effectively conduct joint operations across all domains. This will drive the need for advanced Command & Control (C2) systems able to properly

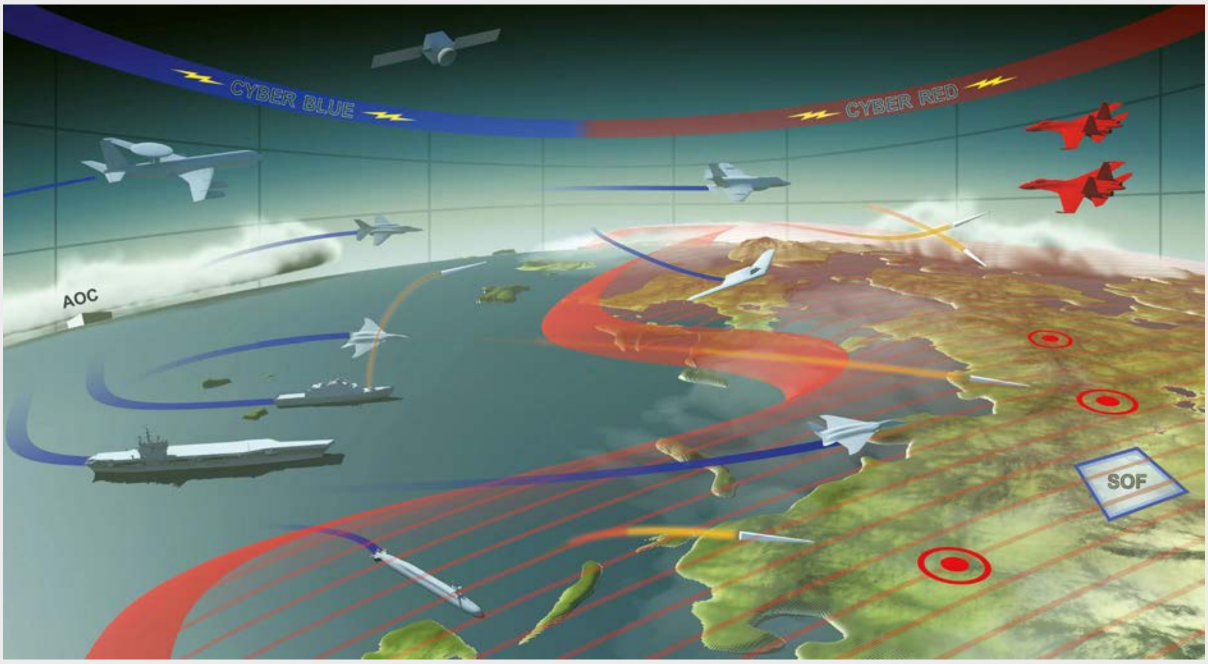
M Zumwalt: © US Navy; Tanks on the Mountain: © 2018 NATO JFCBS; X-47B: © US Navy, Erik Hildebrandt; A-10C Thunderbolt: © US Air Force, Tech. Sgt Katie Justen; Joint Terminal Attack Controller: © US Army, Maj Kurt Rauschenberg; Typhoon: © Crown Copyright; PzH 2000: © NATO; Network Structure: © TheDigitalArtist/Pixabay.com; Landscape: © Pexels/Pixabay.com connect, integrate, and synchronize forces, regardless of their service or domain affiliation. Systems that can guarantee future commanders the possibility to 'consider all domains from the beginning of the planning process and be empowered to coordinate dynamic all-domain retasking throughout execution'.[2] The future will be characterized by an exponential growth in airspace operations, both in number and complexity; this will pose new challenges to the battlespace management of the Air domain. The purpose of this article is to highlight the importance, for NATO, of developing modern battlespace and airspace management strategies, as the 'condition sine qua non' for fighting and winning in the increasingly complex air operations environment of the future.

Seeking Advanced C2 Systems

In a recent report, JAPCC depicts a possible scenario for explaining a future vision of Close Joint Support. In this scenario, a Multi-Domain Command and Control System (MDC2S) will be able to share data with all connected systems across all domains and will process multiple 'calls for fire' in real-time. After receiving a digital urgent troops-in-contact message, while considering time-on-target and weapons effect radii, the MDC2S presents a computer prioritized list of available attack options together with the respective Collateral Damage Estimation (CDE) to the Joint Fires Support Coordinator (JFSC). The attack options will include everything from long-range, network-enabled missiles fired from a ship in blue water to artillery and Multiple Launch Rocket Systems (MLRSs), to fixed- and rotary-wing manned aircraft, to overhead, long-endurance Unmanned Aerial Vehicles (UAVs) with on-board payloads able to be directly controlled by ground units.[3] JAPCC's study anticipates the search for a new approach to combat operations; an approach that can enable forces to plan and execute operations rapidly, but above all, using the capabilities offered by all domains in a synchronized, cooperative, and efficient manner. Indeed, more than the speed of the war platforms, in future fights, the rapidity and the way the commanders at all levels will understand and visualize the battlespace, will be a determining factor for victory.

© i3d/Shutterstock.com

To win future battles, the speed and availability of information sharing will be crucial to accelerating the decision-making process, exploiting the initiative, and creating a position of relative advantage. Current decision-making, planning, and execution processes seem to be slow and predictable. Competing with future peer adversaries will require advanced battle-space management concepts to facilitate rapid synchronization of efforts to create dilemmas for adversaries. This will require 'continuous and iterative near-term tactical planning, longer-term operational-level planning, and refinement as conditions change'.[4] Focused on this need, the US CSAF presented the necessity for an enhanced C2 system. A system that is capable of improving situational awareness, speeding up the decision-making process, and providing a refined capability to direct forces across multiple domains. Following this senior officer's request, the US Department of Defense (DoD) started a new initiative called Joint All Domain Command and Control (JADC2). JADC2 could be defined as a new battle management vision. A vision in which future forces will be characterized by the capability 'to support operations in a highly contested fight, ensuring not just cars, but aircraft, munitions, satellites, ships, submarines, tanks, and people are at the right place at the right time prosecuting the right target with the right effects, in seconds'.[5] With this initiative, the DoD is stating that it is no longer the time for developing domain-specific solutions. It is time to think about, develop and adopt a network-centric approach to connect each sensor from every domain with any shooter. In line with this, the 'Mosaic Warfare' concept is being developed by the Defence Advanced Research Projects Agency (DARPA). 'Mosaic Warfare' can be described as a revolutionary new warfighting platform built upon an interconnected and interoperable force package, able to leverage the best characteristics of different platforms.[6] A kind of 'system of systems' characterized by dedicated new interfaces, communication links, and precision navigation and timing software that will allow platforms to work together. It is based on the concept, that 'everything that has a sensor could be connected to everything that can make a decision, and then to anything that can take an action'.[7] NATO should leverage the possibilities offered by new technologies and develop advanced battle concepts



Artificial rendering of a future multi-domain battlefield scenario.

that will enable future commanders, at all echelons, to understand the battle rapidly, direct forces faster than the enemy, and deliver synchronized combat effects across multiple domains. As recently postulated by General Goldfein, 'The goal [is to] produce multiple dilemmas for our adversaries in a way that will overwhelm them … an even better outcome … is to refine Multi-Domain Operations [MDO] to the point where it produces so many dilemmas for our adversaries that they choose not to take us on in the first place.'[8]

New Challenges for Future Airspace Management

The above mentioned innovative conceptual battlespace-management models have one thing in common: the use of the third dimension. These concepts will work only if an adequate airspace management system guarantees the commanders rapid and flexible tactical execution through a fast re-tasking of assets, and the dynamic apportionment of airspace. This will require revised airspace management focused on an innovative approach that can guarantee dynamic, real-time airspace coordination while ensuring an adequate level of traffic de-confliction. The situation gets more complicated when considering that the usage of the airspace by all actors will increase significantly in the future, resulting in exponential growth of airspace operations. During the forecast period 2019 to 2026, for example, the usage of UAVs in military operations as well as civil and commercial applications, is expected to grow at a Compound Annual Growth Rate (CAGR) of 15.8 %.[9]

Moreover, all services are developing long-range, precision-guided 'multi-domain' weapons, which will drive the need for tighter joint management of the airspace. To highlight a few of these new systems, the US Navy is fielding a new Electromagnetic Railgun, which would be able to zero in on targets from 100 nautical miles away and fire a solid metal slug that could travel at speeds of 4,500 miles per hour.[10] The US Army is developing the long-range hypersonic weapon, a rocket-powered boost-glide missile whose expected range is classified but could easily be

Real-time Airspace Awareness and De-confliction for Future Battles.

thousands of miles. The US Army is also pursuing a strategic long-range cannon, a supergun using gunpowder to launch guided projectiles over one thousand miles.[11] Futuristic hypersonic weapons, which promise to cross more territory in a shorter time, will break the traditional norms of long-range weapons, including the maximum altitudes reached. Furthermore, it has to be considered that changes in the A2/AD environment coupled with adversary advancements in Cyberspace and the electromagnetic spectrum, will limit the use of conventional aircraft tracking systems and will drive the growth of demand for stealth platforms. Managing airspace in the near future will become more complex than it is today. Anticipating the future vision of airspace management which is able to face such a complicated scenario, DARPA launched a new initiative for a programme named Air Space Total Awareness for Rapid Tactical Execution (ASTARTE). 'The goal of the ASTARTE Program is to provide real-time, low-risk de-confliction between airspace users and joint fires to enable support to tactical units and build a resilient air picture under an A2/AD bubble while conducting JADC2 operations … It will interoperate and coordinate with existing C2 systems to ensure airspace users and operators have the most current and relevant information available.'[12] Even if only focused on the airspace above an Army Division, (a block of airspace approximately 100 km by 100 km, from the ground up to 18,000 feet) DARPA leads the way for a project that, if fielded, could radically change the current concept of airspace management and make a difference in planning, and conducting future battle strategies.

Interoperability: A Long-Standing Problem

The operating principle of these new battle and airspace management initiatives is mainly based on the possibility offered by leveraging technologies to connect all the available sensors and to process the related data by using artificial intelligence. The Director of the JAPCC and Commander, Allied Air Command, (Ramstein Air Base, Germany), General Jeffrey L. Harrigian, warns, that 'sensors exist across every domain, but connecting those sensors remains challenging.'[13] The current situation, in NATO, contains a plethora of different systems, and sensors, that do not guarantee an adequate level of interoperability. ASTARTE promises to solve this issue by adopting new algorithmic solutions designed with an Application Programming Interface (API) that enables easy integration and interoperability with the full range of currently existing US military C2 Systems.[14] Perhaps, the moment has arrived for the Alliance, to make wide-ranging holistic political-military changes that can address and solve the long-standing problem of interoperability, keeping in mind that 'interoperability does not necessarily require common military equipment. What is important is that the equipment can share common facilities, and is able to interact, connect, and communicate, exchange data and services with other equipment.'[15] DARPA's initiative with the ASTARTE project aimed at obtaining an API that integrates and makes the different C2 systems currently in use interoperable is undoubtedly something that deserves to be sponsored and supported.

Conclusions

The motto 'divide et impera' meaning divide and rule, although of uncertain origin, highlighted a policy dear to the ancient Roman emperors. The strategy aimed at maintaining their territories or conquering new ones, dividing and fragmenting the power of the opposition, so that they could not unify toward a common goal. In reality, this strategy helped to prevent a series of small entities, each with a precise amount of power, from uniting and forming a more relevant and stronger entity. NATO is an intergovernmental military alliance between 30 different countries and could encounter difficulty competing with an enemy who shows himself strongly united by the use of the same language, tactics, techniques, procedures, and technologies. Using the motto mentioned above as a warning, NATO will have to be capable of promoting new strategies to ensure that the Alliance's entities are joined to form a centre of power, ready to provide the military forces needed to deter war 'et impera' for a long time to come. To achieve this, NATO must seek innovative C2 systems, able to properly connect, integrate, and synchronize forces from all domains. This will require revised airspace management, too. A new one focused on an innovative approach, able to guarantee dynamic, real-time airspace coordination while ensuring an adequate level of traffic deconfliction. Initiatives such as JADC2, 'Mosaic Warfare' and the ASTARTE programme will make the difference if developed and adopted collectively by all 30 NATO Nations. As stated by General Harrigian, 'as we think about existing and developing sensors, we must connect them to form a cohesive, resilient, and self-healing collective network. Therefore, it is crucial that we build in multi-domain interoperability from early design with any future capabilities.'[16] It is time to focus on a common framework by which it will be possible to build the future battlespace management as a comprehensive and integrated solution, creating the conditions to position NATO to fight and win in the increasingly complex air operations environment of the future.

1. Pope C., Secretary of the Air Force Public Affairs (Sep. 2019), Goldfein, details Air Forces' move towards a 'fully networked', multi-domain future. Available from https://www.af.mil/News/Article-Display/Article/1963310/goldfein-details-air-forces-move-toward-a-fully-networked-multi-domain-future/ [accessed 17 Jul. 2020].
2. US Air Force Doctrine Note 1-2 (Mar. 2020), USAF Role in Joint All-Domain Operations.
3. Cdr Cochran D., Lt Col Haider A. and Lt Col Stathopoulos P. (Jun. 2020), Reshaping Close Support – Transition from Close Air Support to Close Joint Support. Joint Air Power Competence Centre (JAPCC), Kalkar, Germany. Available from https://www.japcc.org/portfolio/reshaping-close-support/.
4. Curtis E. Lemay Center for Doctrine Development and Education (Jun. 2020), Annex 3-1, Department of the Air Force Role in Joint All-Domain Operations (JADO). Available from https://www.doctrine.af.mil/Operational-Level-Doctrine/Annex-3-1-DAF-Role-in-Jt-All-Domain-Ops-JADO/ [accessed 24 Jul. 2020].
5. Nishawn S. Smagh (Apr. 2020), Defence Capabilities: Joint All Domain Command and Control. Congressional Research Service. Available from https://fas.org/sgp/crs/natsec/IF11493.pdf [accessed 1 Jul. 2020].
6. DARPA (Undated), DARPA Tiles Together a Vision of Mosaic Warfare [advertisement]. Available from https://www.darpa.mil/work-with-us/darpa-tiles-together-a-vision-of-mosiac-warfare [accessed 1 Jul. 2020].
7. Ibid.
8. Ibid. 1.
9. CISION PR Newswire (Jan. 2020), Unmanned Aerial Vehicle (UAV) Market Size Worth Arounds US$ 48.8 Bn by 2026. Available from https://www.prnewswire.com/news-releases/unmanned-aerial-vehicle-uav-market-size-worth-around-us-48-8-bn-by-2026ñ300995216.html [accessed 29 Jun. 2020].
10. Suciu P. (Jul. 2020), Dead or Alive: What is the Fate of US Navy's Big Railgun Project? The National Interest. Available from https://nationalinterest.org/blog/reboot/dead-or-alive-what-fate-us-navys-big-railgun-project-163949 [accessed 21 Jul. 2020].
11. Sydney J. Freedberg Jr (May 2020), Army Tests New A2/AD Tools: Howitzers, Missiles & 1,000-Mile Supergun. Breaking Defence. Available from https://breakingdefense.com/2020/05/army-tests-new-a2-ad-tools-howitzers-missiles-1000-mile-supergun/ [accessed 21 Jul. 2020].
12. DARPA Broad Agency Announcement Air Space Total Awareness for Rapid Tactical Execution (ASTARTE) – Strategic Technology Office (7 Apr. 2020). Available from https://beta.sam.gov/opp/897bf13ef9a044b298d0de164781412c/view [accessed 7 Jul. 2020].
13. Gen Harrigian, Jeffrey L. (2019), Shaping the Future Multi-Domain C2. Transforming Joint Air and Space Power, The Journal of the JAPCC, Ed. 29, p. 6–8. Available from https://www.japcc.org/wp-content/uploads/JAPCC_J29_screen.pdf
14. Ibid. 12.
15. North Atlantic Treaty Organization (24 Mar. 2020), Interoperability: Connecting NATO Forces. Available from https://www.nato.int/cps/en/natolive/topics_84112.htm [accessed 13 Jul. 2020].
16. Ibid. 13.

Lieutenant Colonel Livio Rossetti

was commissioned in the Italian Army in 1993, as an infantry officer. After three years he transited to the Army Aviation schools and graduated as a rotary-wing pilot in 1998. Lieutenant Colonel Rossetti has served as Platoon Commander, Squadron Commander, and S3-cell Chief. He has flown utility helicopters AB-206, AB-205, AB-212, AB-412, as well as the AW-129, Mangusta, combat helicopter. As an aircrew and staff officer, he has deployments to the Balkans Peninsula (Albania, Kosovo), Middle East (Lebanon, Iraq) and Central Asia (Afghanistan). Lieutenant Colonel Rossetti is a qualified CBRN (Chemical, Biological, Radiological and Nuclear) specialist, an airmobile instructor, and he is currently stationed at the JAPCC – Kalkar, as Air-Land Operations expert in the Combat Air Branch.

Cybersecurity Challenges with Emerging Technologies

How to Leverage New Technologies in Modern Battlefields

By Major Fotios Kanellos, GR AF, JAPCC

Introduction

It was the end of April 2020 when the first 5G base station was installed by Huawei, together with China Mobile, on the 'roof of the world', Mount Everest, at an altitude of 6,500 m, near the Qianjin camp, providing invaluable wireless communication to climbers and researchers. At the summit on the Northside of Mount Qomolangma (the Tibetan name for Mount Everest) the highest 5G tower provides high definition live broadcast and monitors environmental and scientific activities.

Huawei has been one of the leading providers globally of Information and Communications Technology (ICT) and is pursuing the commercialization of 5G technology all over the world, including in extreme environments such as the highest mountain peaks along the Chinese-Nepalese border, the hot deserts of Kuwait, the subarctic areas of Russia and the wet tropical savannas of South America. This giant among IT companies, the world's second-largest manufacturer with 18 % of the global smartphone market and more than 180,000 employees, was founded in 1987.

Initially, Huawei produced communications equipment for mobile phone networks in Shenzhen, southern China, and was founded by a former People's Liberation Army officer who was also a member of China's Communist Party. Because of the military background of Huawei's founder and its dominant role as a supplier of 5G cellular network equipment, an increasing number of countries have raised concern and have serious reservations about trusting its products and services.[1] The security risks and threats that 5G networks and smart devices pose due to design and manufacturing vulnerabilities (even intentional) are incredibly high and difficult to mitigate. Because of these risks, United Kingdom's National Cyber Security Centre (NCSC) published a review (14th July 2020) that changed their initial security assessment of Huawei's presence in the national 5G network, recommending the government to completely ban the Chinese technology company and remove its 5G kit from UK's mobile providers' networks by 2027.[2] That decision will have a significant impact on the roll-out of 5G technology in Britain. However, the possibility of controlling the 'sensitive parts' of such a promising and advanced mobile network, with a decade-long impact, would risk not only the communications but also some of the most cutting-edge technologies of the 21st century which are based on 5G infrastructure.

M Soldiers: © Getmilitaryphotos/Shutterstock.com;
Technological Background: © Timofeev Vladimir/Shutterstock.com;
Data Protection Artwork: © Rawpixel Ltd./stock.adobe.com


© Pasko Maksim/Shutterstock.com

Emerging Technologies

Self-driving cars, Artificial Intelligence (AI), Machine Learning (ML), Automation, Virtualization, Smart Cities, Blockchain Networks, Big Data, Internet of Things (IoT), Internet of Senses, Cloud and Quantum Computing are but some of the most transformative innovations that are currently under development, and that are substantially altering the social, financial, business, and military environments. Over the next five to ten years, these emerging digital technologies, together with the sophisticated applications they produce, will generate new opportunities and create new challenges in almost all of the daily activities, especially the conduct of military operations.[3]

Thanks to 5G's unique technical characteristics, including data rates ten times faster than present, the capacity to support a huge number of connected devices, almost no delay, continuous mobility, energy efficiency and service reliability, new tools and services are continually being developed. Connecting billions of smart devices, like 'everything to everything' (X2X), collecting and analysing Big Data from multiple networks (Cloud Computing) and establishing peer-to-peer networks (Blockchain) are only possible because of the components and functions that 5G technology offers into the new and ever-evolving Information Era.[4]

Virtualization, for example, is an immersive technology that can provide an effective cyber hygiene ecosystem. It makes computing environments more independent of physical infrastructure and creates virtual scenarios. Together with artificial neural networks and other systems, virtualization may determine, in advance, the vulnerabilities of the networks and the effect of these individual technologies providing the added benefit of building resilience. Virtualization aims at enabling a better understanding of cyber capabilities and vulnerabilities. This knowledge will support Cyber Threat Intelligence (CTI) tracking of malicious attacks and maintaining the required security standards.[5]

Cloud computing, 5G technology and real-time virtual environments can take military training and exercises to a new level of innovation and agility. Accessibility and flexibility will become key features of new, advanced mobile simulations where trainees will learn at their own pace and in their own space.[6] Moreover, Extended Reality (XR) – encompassing Augmented Reality (AR), Mixed Reality (MR) and Virtual Reality (VR) – has been highly developed and empowered by miniaturization and increased processing power. Especially during the Covid-19 pandemic, XR has played an even more significant role by becoming the next ubiquitous computing platform, not only for gaming but also for distance training, retail shopping, working and socializing.

Since 2019, the British Army has been working on a project to switch from individual training to collective XR-based training. Using advanced XR Head-Mounted Displays (HMDs), several dozen trainees may operate together in the same virtual world and a variety of training scenarios based on agile operational demands. Such high-tech collective XR-based systems can also be deployed as mobile training services.[7]

This leads to the application to the Air environment, where this technology has proven to be especially important for air-to-air combat operations by improving human-machine teaming and communication. To automate such complex air operations, certain levels of trust, scalability and autonomy must be reached and matured. Human-machine interactions are built on three levels of autonomy: semi-autonomous (human-in-the-loop); human supervised autonomy (human-on-the-loop); total autonomy (human-out-of-the-loop).[8] Autonomy and intelligence are the key factors in determining the range of 'reality-virtuality continuum', transforming a human experience, increasing situational awareness and refining the decision-making process. The new communication patterns and unlimited connectivity in the Joint Air domain may also transform the level of Command and Control (C2) across NATO and enhance even more the interoperability of such a networked operating environment.[9]

On 20 August 2020, the Defence Advanced Research Projects Agency (DARPA) completed its AlphaDogfight Trials (ADT) project which can be considered the epitome of the collaboration of multiple advanced technologies such as AI, Virtualization, Automation, ML, and Cloud Computing. During a three-day simulated aerial combat 'tournament' between an AI-driven 'pilot' and an experienced US Air Force F-16 pilot, the former went undefeated in all five rounds of mock air combat.[10] Through advanced algorithms, the Heron Systems' F-16 AI agent quickly and effectively learned how to execute aggressive and precise manoeuvres that the human pilot could not match.[11] The within-visual-range air combat manoeuvres (dogfights) clearly represent the rising interest in AI and autonomous capabilities within the military aerospace environment.

Cyberspace Challenges

However clear it is that those technologies will radically change how people work, communicate, think, and even fight in the near future, they simultaneously generate great concern that state-sponsored actors could interfere and disrupt their features and services, posing a massive threat to strategically vital networks. 5G technology has the potential to drastically increase the attack surface and the number of entry points for hackers because of the large number of connected devices (from baby monitors to refrigerators and fire alarms) with weaker security features. However, not only do low-cost interconnected devices introduce vulnerabilities, the communication between these devices can be the weakest link in 5G's security. Under this rationale, the UK government decided to mitigate the risk (if not eliminate it) by restricting Huawei's 5G kit despite the consequences of a two to three years delay on the roll-out of the technology and the additional costs of up to GBP 2 billion.[12]

Similarly, cloud computing technology consists of computer storage, front-end technology (laptops, Personal Computers), networking infrastructure and cloud-based applications which may also be disrupted and exploited. Most of this risk applies both to the extended commercial clouds (Google Cloud Services, Microsoft Azure, Amazon Web Services) and to the smaller-scale cloud services used for classified operations and secured sensitive data. Speed and security level are defining the different types of clouds and depend upon 'off-premises' and 'on-premises' equipment. However, meeting the essential security demands, especially from a military perspective, while leveraging the multi-cloud capabilities and benefits, may be challenging. Aerospace and defence supply chains can take great advantage of the multi-cloud services involving different defence contractors of varying sizes by pulling data from multiple sources and delivering them to a single location and single application.[13] Autonomic Logistics Information System (ALIS), a complex, web-enabled, interconnected and distributed military logistics service, supporting the world's fifth-generation fighter, F-35 Lightning II, exemplifies the integration of advanced technologies in military operations.

© markusspiske/Pixabay.com

The increased speed of the connections and the wide range of services and applications will introduce a plethora of new security challenges. Malware, Phishing, Man-in-the-middle (MitM), Distributed Denial-of-Service (DDoS) and Social Engineering attacks have been growing daily, creating many challenges and infecting the digital ecosystem. After all, the great power competitions of the future will probably not take place on battlefields or in boardrooms but on smartphones, computers and on the digital infrastructure that supports them. In countries like China and Russia, the government and the private sector are working closely together, developing and deploying new technologies and applications that will have a global reach, which they consider vital for their cyberspace sovereignty.[14] On 1 June 2017, exactly three years after China's Cybersecurity (Internet Security) Law was implemented, another document was published, entitled 'Cybersecurity Review Measures', setting the rules of security and supply chain standards that 'Critical Information Infrastructure (CII)' products and services should apply.[15]

Cyber Threat Intelligence

In spite of introducing more vulnerabilities, emerging technologies can also provide essential help tackling cybersecurity challenges by offering useful tools to clean the cyber threat landscape. AI, for example, can automatically gather, analyse and disseminate intelligence and valuable information across various global networks providing capabilities to indicate cyberattacks and mitigate anomalies based on optimum prevention strategies. This CTI is an important factor for all armed forces in combating cyber threats from both a defensive and offensive perspective. According to the Allied Joint Doctrine for Cyberspace Operations (CO), published in January 2020, '… freedom of action in cyberspace may be as important as control over land, air and space, or sea.'[16] In an increasingly interconnected environment, 'it is more difficult to distinguish between the strategic, operational and tactical levels'.[17] Since cyberspace is a domain of operations 'an operational shift to a focus on mission assurance is needed'.[18] Managing a real-time, dynamic, and complex framework that can predict and prevent cyberattacks can be a real game-changer to 'ensure the continued function and resilience of capabilities and assets … critical to the execution of NATO mission-essential functions in any operating environment or condition'.[19]

Effective CTI primarily deals with exploiting ML and advanced AI technology, enabled by a dynamic, specific knowledge base to understand potential threats and what might motivate an adversary to launch an attack.[20] Delicate ML tools, together with sophisticated AI algorithms, can maximize accuracy in attack attribution. These two technologies combined can 'find correlations between events that may appear random and unrelated to the human eye. Only AI can analyse such a vast amount of information in real-time …'[21] Therefore, training AI and feeding ML processes necessitates increasing data from diverse sources. Monitoring user information and analysing user behaviours, device usage, network activities, location and application data can, hence, be a source of both protection and threats.

Many hacker groups, surprisingly, do not vary their procedures when attacking either military targets or civilian facilities, making attribution a straightforward task. Most of the time, those actors simply pause their behaviour for a specific period before they deploy a new automated tool (i.e. bots[22]). Based on this pattern, it is possible to use automation to track and analyse raw threat-intelligence feeds and provide quick and reliable information that could reveal whether something has changed over time against specific criteria.

ML and AI algorithms can also enhance Incident Management by reducing the number of the security events and queries that need to be addressed and solved by human operators to 10 %, shifting the status from man-in-the-loop to man-on-the-loop level. Moreover, cloud services and infrastructure not only have the inherent ability to store vast amounts of data from diverse sources, like the hundreds of sensors of a military aerial platform [daily data generated from IoT devices are estimated to exceed 5 quintillion bytes (1 Billion Gigabytes)][23], but also can establish sets of rules and practices that can be replicated across all different data sets providing high-security standards. Incredibly, for aerospace and defence supply chains, the use of Blockchain technology in a cloud environment can even further secure and simplify processes. In particular, this would create 'digital identities' for all components and parts in the supply chain and enable the tracking of movement around the chain in a safe manner working as a secure ledger.[24]

Conclusion

The extraordinary capabilities of these emerging technologies have extended and endowed cyberspace with capabilities beyond the hyper-connectivity of the Internet itself. These breakthroughs, however, have not only been enormously advantageous. The expanded network infrastructure and increased number of connected devices (even those that appear not to be connected) introduce more vulnerabilities to intrusions. Furthermore, the enormous volumes of data processed and shared among the vast numbers of Internet-connected nodes become increasingly likely targets of exploitation and distortion.

State and non-state actors who seek to develop sophisticated methods of manipulation and surveillance, particularly by exploiting emerging technologies, will shape the conflict in the geopolitical arena for years to come. The information ecosystem

'becomes more polluted, segmented, and rigidly controlled',[25] making it even harder for democratic countries to build resilience and respond to external threats. Therefore, it 'is essential to the Alliance's successful functioning in peace, crisis and conflict'[26] to coordinate, synchronize and execute cyberspace and information activities that will deliberately create comparable counter effects, leveraging the tools and capabilities the emerging technologies may offer. ●

1. Bowler, Tim, 'Huawei: Why is it being banned from the UK's 5G network?', BBC, 14 Jul. 2020 (accessed 11 Sep. 2020).
2. National Cyber Security Centre (NCSC), 'Huawei advice: what you need to know', 14 Jul. 2020, available at https://www.ncsc.gov.uk/information/huawei-advice-what-you-need-to-know (accessed 11 Sep. 2020).
3. Heren, H., 'Future Developments Panel Introduction', JAPCC Read Ahead 2020, available at https://www.japcc.org/future-developments-panel-introduction/ (accessed 11 Sep. 2020).
4. Ibid.
5. Cowan, G., 'Cyber Threat Intelligence: Industry solutions begin to lean on AI and ML advances', Jane's, 24 Oct. 2019 (accessed 11 Sep. 2020).
6. MS&T Magazine, 'Industry Vectors in AI, XR, 5G & More', Volume 37, Issue 1.2020.
7. Ibid.
8. Pappalardo, D., 'The Role of the Human in Systems of Systems: Example of the French Future Combat Air System', OTH Journal, 27 Jan. 2020 (accessed 7 Sep. 2020).
9. Presa, C. and Perkins W., 'Air Warfare Communication in a Networked Environment: An Interdisciplinary Analysis', JAPCC, Jul. 2017, available at https://www.japcc.org/portfolio/air-warfare-communication-in-a-networked-environment/ (accessed 26 Oct. 2020).
10. Trevithick, J., 'AI Claims "Flawless Victory" Going Undefeated In Digital Dogfight With Human Fighter Pilot', TheDrive, 20 Aug. 2020 (accessed 11 Sep. 2020).
11. DARPA, 'AlphaDogfight Trials Foreshadow Future of Human-Machine Symbiosis', available at https://www.darpa.mil/news-events/2020-08-26 (accessed 11 Sep. 2020).
12. Ibid. 1.
13. Cowan, G., 'Cloud computing: Armed forces aim for the sky', Jane's, 24 Oct. 2019 (accessed 11 Sep. 2019).
14. Rosenberger, L., 'Making Cyberspace Safe for Democracy', Foreign Affairs, May/Jun. 2020, p. 146–159.
15. Dudley, L. et al., 'China's Cybersecurity Reviews Eye "Supply Chain Security" in "Critical" Industries', 27 Apr. 2020, available at https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cybersecurity-reviews-eye-supply-chain-security-critical-industries-translation/?fbclid=IwAR33yv-q06LZ6cT5p94_yzUjXL8zdQQ-QjqB1umqgW0lt-9GFTjYNK7gB_o (accessed 10 Sep. 2020).
16. AJP-3.20, 'Allied Joint Doctrine For Cyberspace Operations', Jan. 2020.
17. Ibid.
18. Ibid.
19. Ibid.
20. Ibid. 5.
21. Ibid.
22. Bots are software programs that perform simple repetitive tasks (scripts) over the Internet, much faster than a person could.
23. Ghosh, I., 'AIoT: When Artificial Intelligence Meets the Internet of Things', 12 Aug. 2020, available at https://www.visualcapitalist.com/aiot-when-ai-meets-iot-technology/?fbclid=IwAR3fV3p76bi_o4e6h3HXWy-ktzNi_u1Lpf-BMNmflLhe3Nv5acDIA9nTTTs (accessed 10 Sep. 2020).
24. Ibid. 12.
25. Ibid. 13.
26. Ibid. 15.

Major Fotios Kanellos

graduated from the Hellenic Air Force (HAF) Academy in 2003 as an Electrical Engineer with specialization in Telecommunication and Computer Science. He holds two Master degrees, one in Technical-Economic Systems from the National Technical University of Athens (NTUA) and another in Environmental Sciences from University of Patras.

Major Kanellos served as an inspection engineer for T-2 C/E aircraft and system engineer for the T-6A Flight Simulator at the Hellenic Air Training Command (HATC) in Kalamata. His previous appointment was at the HAF Support Command (HAFSC) managing IT and Cybersecurity projects. His current appointment is as a Cyberspace SME at the Joint Air Power Competence Centre.

© Dianov Boris/Shutterstock.com

Hypersonic Threats

Hype or Game Changer for NATO's Deterrence?

By Lieutenant Colonel Andreas Schmidt, GE AF, JAPCC

Introduction

It is almost impossible to read current literature about NATO's threat spectrum without having Hypersonic Operational Threats (HOT) mentioned as an emerging 'game-changer.' The following article is based on a Specialist Team Report of NATO's Science and Technology Organization about Hypersonic Threats[1] and will analyse the impact hypersonic threats may have on NATO's defensive posture, what kind of gaps might be created, and what NATO might have to do to mitigate these vulnerabilities.

Threats like Hypersonic Glide Vehicles (HGV) or Hypersonic Cruise Missiles (HCM) are not a completely new threat category, since they bear certain similarities to ballistic missiles or 'old fashioned' sub-hypersonic cruise missiles. Hence, it seems reasonable to base the analysis on available capabilities against these existing threats.

However, HOT are a significant challenge for NATO's current defensive capabilities. Extensive studies are necessary to gain a sufficient understanding of the severity of the situation and the resulting necessary steps to maintain a stable security environment for NATO.

NATO's Current Deterrence Framework

NATO's capability to successfully deter potential adversaries is based on a credible combination of offensive (including both nuclear and conventional) and defensive options. Therefore, these options cannot be looked at in isolation, but rather must be evaluated in a comprehensive manner. Collective Defence is one key element of NATO's overall deterrence strategy. In order to gain a military advantage, it can be expected that potential adversaries will develop capabilities to undermine NATO's current capability set (e.g. NATO Integrated Air and Missile Defence System (NATINAMDS)), which will automatically weaken the credibility of NATO's deterrence. This necessitates an adaptive posture and likely new capabilities on the Alliance's side, such as NATO Ballistic Missile Defence (BMD) or the NATO Very High Readiness Joint Task Force (VJTF) in the past. From this perspective, the emergence of HOT is a logical reaction from potential adversaries towards the current defensive and offensive capabilities of NATO.

Hypersonic Capabilities as a Threat

A military threat, being the combination of capability and intent, is generally anticipated to create a particular effect, geared towards generating a tactical, operational or strategic advantage over an opponent. In contrast, every defensive measure is conceptualized to cover a specific threat or threat spectrum. In the framework of air threats, key parameters like speed, reach, and height[2] have significant importance, as can be seen in Figure 1 below.

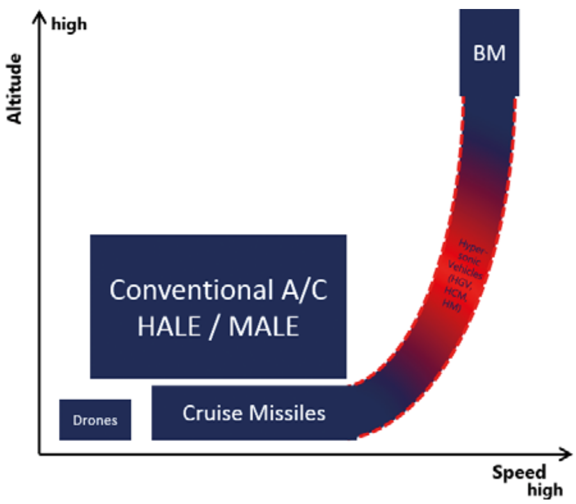


Figure 1: Threat Model.

Historically, the most common air threats were regular aircraft. Over recent decades, this threat portfolio broadened with the addition of ballistic and cruise missiles and unmanned aerial vehicles, to which NATO always found an answer for maintaining a deterrent balance, for instance NATO BMD for ballistic missiles. HOT represent an area not covered, or only marginally so, by NATO's current defensive capabilities; this should energize NATO to take its next adaptive step to mitigate this challenge.

Definition of Hypersonic Operational Threats

Despite the lack of an unambiguous definition for hypersonic speeds, for this paper and in most military contexts, a speed greater than Mach 5.0 will be assumed. This causes a severely reduced timeframe for implementing a potential kill chain. Furthermore, the altitude bands used by HOT, combined with significant manoeuvrability at these high speeds, create further complications for available sensors and interceptors. In comparison to a ballistic missile threat, HOT flight paths and impact points are very unpredictable. Generally, two classes of HOT can be identified: HGVs or HCMs. For both systems, it has to be assumed that they have precision strike capabilities which are supported by on-board sensors.

Hypersonic Glide Vehicles

HGVs are non-powered manoeuvrable vehicles that are boosted by and later separated from, a carrier system, for the attack of land or sea targets. The carrier system, normally rocket boosters, must be capable of creating the initial speed for the HGV to perform hypersonic gliding manoeuvres. After re-entry, they can cover additional large distances by flying glide or phugoid trajectories. After an initial, rather depressed ballistic trajectory, HGVs have an average gliding altitude between 30 and 80 km. During the final phase, which can be gradual or very steep, their speeds should be reduced to high supersonic levels. These systems consist of a launch device and at least one glide vehicle. Options for ground, sea or air-launch are conceivable.

	Ballistic Missile	Cruise Missile (CM)	Hypersonic Glider	Hypersonic CM
Range	More than 5,500 km	Up to 3,500 km	More than 5,500 km	Up to 1,000 km
360 Deg Threat	No	Yes	Yes	Yes
Manoeuvrability	Limited	Yes	Yes	Yes
Impact Point Calc	Yes	No	No	No
Speed	Hypersonic	Sub Hypersonic	Hypersonic	Hypersonic
Altitude	up to 1,000 km+	0–10 km	30–80 km	20–40 km

Figure 2: Parallels to Existing Threats.

Hypersonic Cruise Missiles

HCMs are powered air-breathing vehicles characterized by sustained hypersonic flight for the majority of their trajectory. They rely upon aerodynamic forces for lift and are used to attack land or sea targets. Generally, they travel at altitudes of between 20 and 40 km to maintain their hypersonic cruise speeds ranging between Mach 5 and Mach 7 (higher speeds are possible.) For the attack phase, they might either perform a steep dive manoeuvre or enter a traditional low flight profile phase; in both cases slowing down to speeds of approximately Mach 3.

Bridging Capabilities

Other threats with hypersonic speeds, like the Russian Kinzhal or other ballistic missiles with very depressed flight paths, might have attributes of an HGV, but are not considered as a HOT. However, this shows that the modernization of existing threats (e.g. SS-26 Iskander) can bridge the gap between classical threats and HOT. Therefore, HOT should not be looked at in isolation.

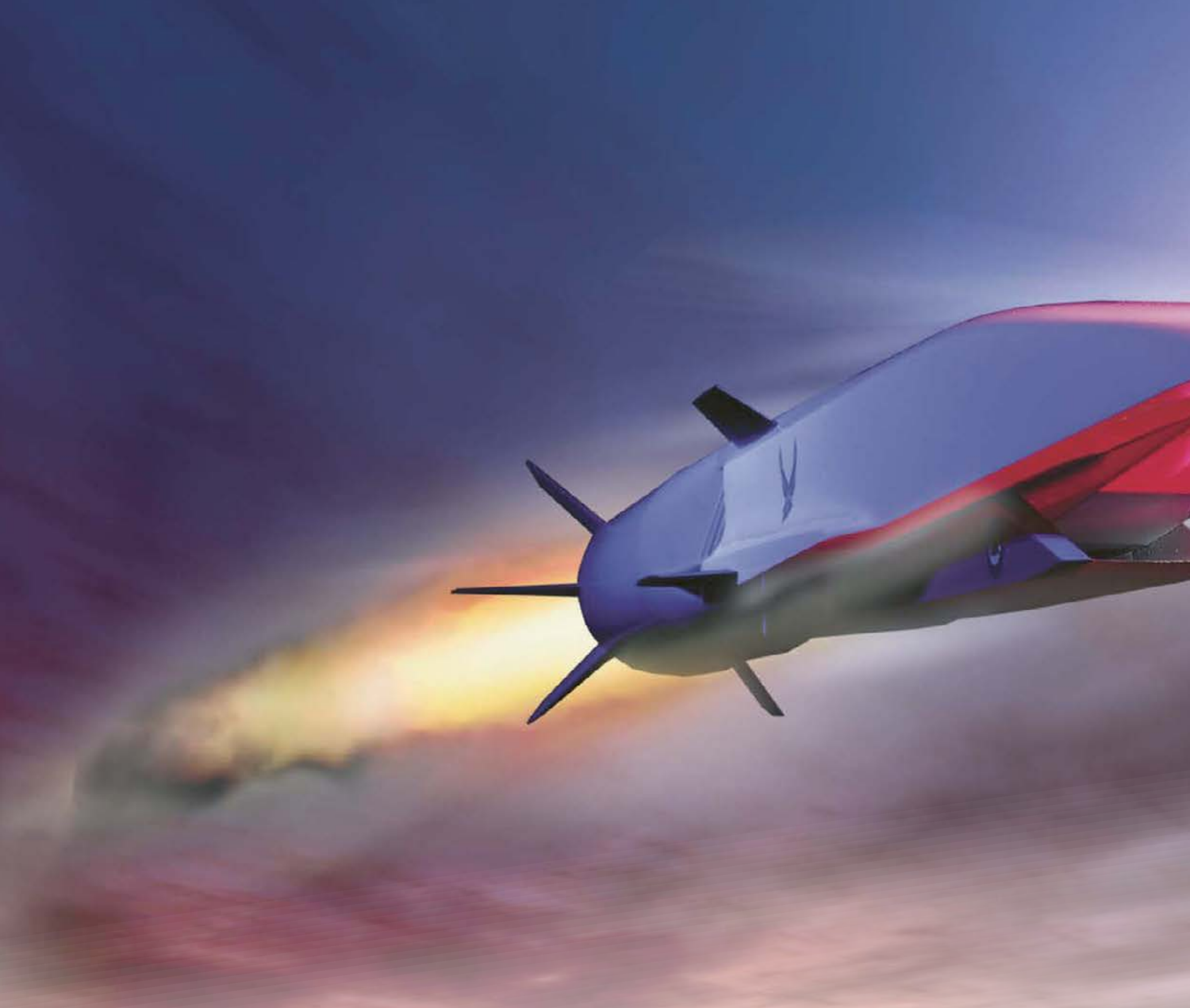
Parallels to Existing Threats

From a defensive perspective, and based on the manoeuvrability and range, there are parallels between HOT and conventional cruise missiles. In both cases, it is nearly impossible to get an early impact point prediction, and it poses a 360° threat for critical assets. Should NATO possess an operational HOT defence system, the defence design would most likely have to follow the principles used for cruise missile defence. However, NATO does not have such a system nor enough resources to employ a comprehensive cruise missile defence for all NATO territory today. Currently, only specially identified objects and limited areas can be defended against cruise missile threats.

Potential Limitations of Current NATO Air Defence Systems

The effectiveness of Air and Missile Defence (AMD) systems is determined by the capabilities of their sensors and interceptors. NATO's current portfolio spans numerous systems that cover various threat categories, but do not include any systems (due to technical feasibility or monetary reasons) that can cover all threat categories in all altitude bands.

This does not mean that NATO nations do not already possess very potent space-based, airborne or surface-based sensors. Still, they need to evaluate which sensors qualify for the detection and tracking of HOT, and which sensors can provide fire solutions. It can be surmised that modern, often software-steered sensors can be adapted, but how this affects overall functionality



and performance still needs to be evaluated. Also, adequate data fusion of all available sensors needs to be in place or enabled to cope with these future threats.

The area in which AMD interceptors can deliver their effect is called 'battlespace,' which is mainly limited by the interceptor's propulsion and manoeuvrability. The significantly elevated threat requirements of HOT increase the likelihood of them taking flight paths outside of the current interceptors´ battlespaces.

With the currently available interceptors, it is likely that an intercept has to occur in the final phase of the flight path. This limits tremendously the distance by which an interceptor can be separated from a protected asset and reduces the opportunity for a second shot at the threat.

Although current Command and Control (C2) structures and data link capabilities are potent and agile enough to handle the present threat set, how they may need to be adapted to also cover HOT has yet to be evaluated.

Use-Case Options for HOT

Currently, three adversary use-cases seem plausible for HOT:

1. Due to the increased likelihood of delivering the intended effect, HOT are likely to be used as a tool for strategic or immediate tactical/operational effects. Currently, peer opponents do not gain many additional benefits by employing HOT against NATO


© US Air Force graphic

European territory, since the same effect can be achieved by existing and less expensive means. Against the United States of America (USA), however, HOT create options for avoiding missile defence systems like the Ground-Based Midcourse Defence system or to threaten high-value assets like aircraft carriers or critical infrastructure. Nevertheless, due to the very high chance of effect delivery by HOT, independent of employed defensive means, the opponent's calculation of necessary offensive means becomes more predictable, the strategic communications messaging more straightforward, and places additional stressors on NATO's defence design decisions. For near-peer or non-peer opponents, HOT represent a real gain in capabilities, since they have no other means to overcome NATO's AMD systems. Therefore, HOT, in this case, may be a credible means of coercion, to promote political interests, and for steering escalation/de-escalation of a conflict.

2. For an 'escalate-to-deescalate' strategy by peer opponents, HOT seem to be an effective tool, since even a single weapon can reliably produce a strategic effect. Also, HOT could support a credible second-strike capability for peer opponents.

3. HOT can be employed as a force enabler and multiplier, by aiming at critical elements of NATO IAMD or other critical military components to allow more numerous offensive weapons to be employed effectively. For peer opponents, this is currently only a quantitative benefit, since the same effect could be reached by saturation. Still, for near- or non-peer opponents this is a significant qualitative benefit.

How Can a Capability Gap be Mitigated?

As with the adversary use-cases, there is a distinction between peer and non-peer opponents as well as peacetime and conflict scenarios. Since HOT influence both of NATO's pillars of deterrence (nuclear deterrence and collective defence), compensatory measures should ensure that the sum of both pillars still provides credible deterrence.

For peer opponents in peacetime against NATO Europe, HOT will not be able to deliver extra effects and therefore do not drive a need to react. Existing credible means of deterrence should continue to be employed. However, the compressed decision timelines, especially in the transition to conflict window, need to be reflected in NATO's C2 structure and processes. Should deterrence fail, and conflict becomes likely, a qualitative and quantitative overmatch for available AMD systems can be assumed. In such a scenario, NATO should concentrate on the defence of critical and high-value assets.

Since no potential non-peer opponents possess HOT, NATO should concentrate on the non-proliferation of HOT systems, materials and knowledge. Should these measures fail, NATO should raise the severity of consequences for opponents to employ HOT, to maintain credible deterrence. The development of counter-HOT systems will take several years, and NATO-wide protection is not only technically, but economically complex. Therefore, the capability gap must first be offset by harsher consequences through credible offensive measures to reduce the perceived benefits to a potential adversary of using HOT. Should deterrence still fail, NATO must evolve its collective defence capabilities so that they can be effectively employed in a conflict including HOT. A combination of defensive, offensive and passive defence measures, supported by a suitable Battle Management, Command, Control, Communications and Intelligence (BMC3I) system, needs to be identified, to significantly reduce the added value of employing HOT by the opponent.

What is Needed to Close the Capability Delta?

As a first step, NATO needs to assess HOT realistically, including our current capabilities to counter HOT, and ensure that the policy/doctrine basis is fit for their optimal employment and that these are suitable for new capabilities to be seamlessly integrated. NATO must strategically state that initial weaknesses in collective defence are compensated (in short- to mid-term) by other measures of credible deterrence. It seems plausible that this will necessitate a multi-domain approach, which needs to be reflected in an adequate C2 structure, appropriate rules of engagement, and is represented in NATO and national education and training processes at all military and political levels.

System Requirements for HOT Defence

A comprehensive answer covering system requirements for an effective solution to HOT requires an assessment of all four pillars of NATO Integrated Air and Missile Defence (Active Air Defence, Passive Air Defence, Surveillance and BMC3I) and all steps of the kill chain. Point and area defence plans or schemes of assets must both be assessed.

It would be beneficial to have sufficient sensor capabilities to gain and maintain a continuous track of a HOT from launch to intercept or impact. Due to the relatively low altitude compared to ballistic missiles (HGVs 30-80 km, HCMs 20-40 km), this is hard to achieve. Because of the earth's curvature and anticipated flight levels, detection ranges are limited.

Antenna Height/ Flight Level	80 km	40 km	30 km
1 m	1,110 km	790 km	680 km
10,000 m	1,500 km	1,170 km	1,070 km

Therefore, the initial focus should be on the necessary sensor network for early warning (both military and civilian) and engagement; hence the boost phase and the phase before intercept, currently most likely the final phase. These ranges lead, in combination with the target speed, to corresponding early warning times.

Range/Mach	5	10	20	27
700 km	410 s	205 s	103 s	76 s
1,000 km	590 s	295 s	148 s	108 s
1,500 km	880 s	440 s	220 s	163 s

For more accurate and better early warning and cueing of other sensors, space-based sensors in various orbits (e.g. geostationary, low earth orbit) may be beneficial. Detailed requirements for coverage and robustness, especially against peer opponents, must be identified.

Outside of simulation environments, HOT are not available for testing against current AMD weapons systems. This makes solid intelligence data necessary, not only for future defence planning, but also for defining general system requirements. It cannot be stated with high confidence that sensors currently available (e.g. PATRIOT, SAMP/T, SMART-L) are capable of detecting and tracking manoeuvring HOT. Although these systems may be adapted using software fixes, the consequences for the remaining task load

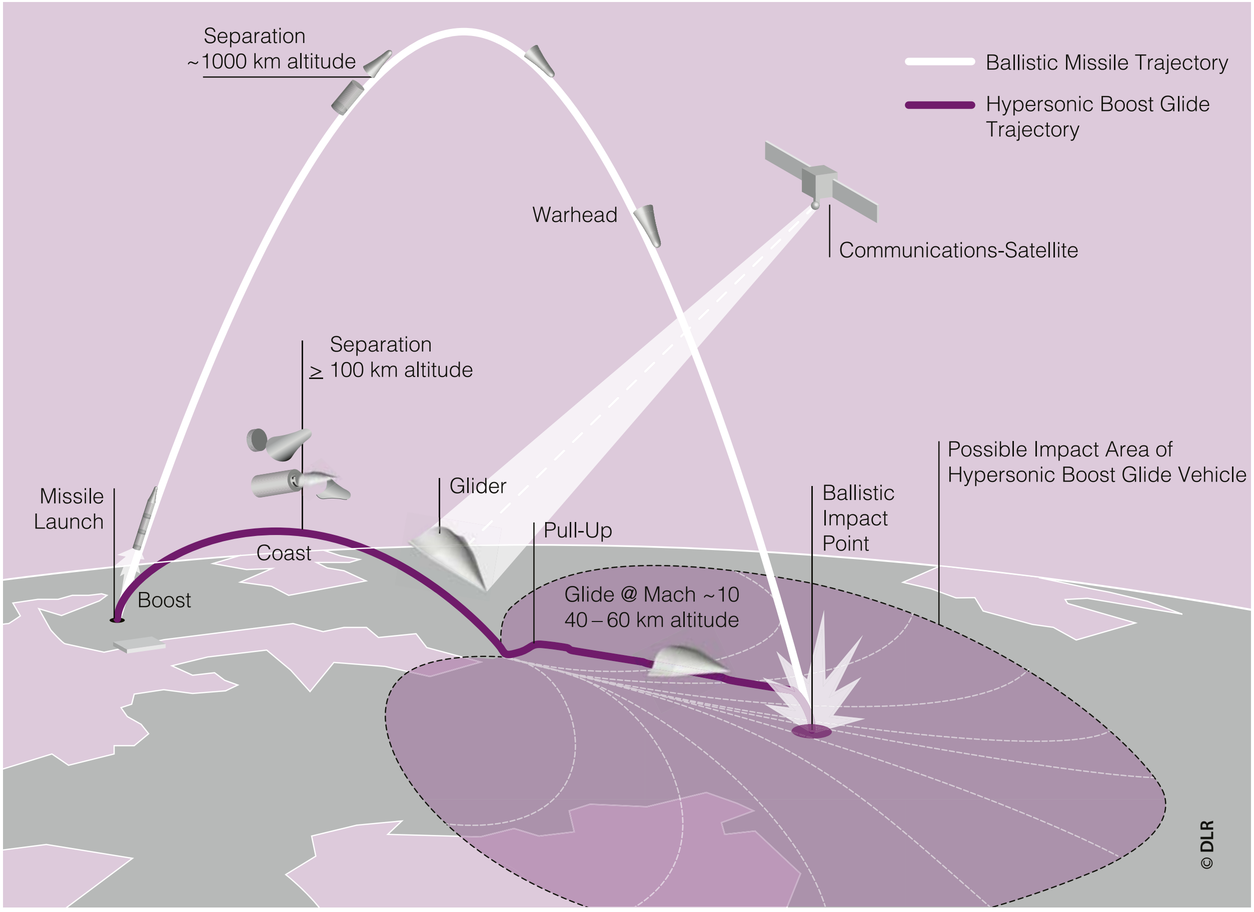


Figure 3: Hypersonic Vehicles and Ballistic Missiles in Comparison.

(e.g. tracking aircraft or ballistic missiles) must also be identified. Existing early warning systems like the US Shared Early Warning (SEW) system, which uses infrared sensors to detect missiles in their boost phase, should be capable of detecting HGVs and likely HCMs since their boosters have a significant boost phase. The need for further land-, sea-, air- or space-based sensors must be analysed to guarantee successful defensive engagement options against HOT.

PATRIOT: Phased Array Tracking Radar, Intercept of Target

SMAP/T: Sol-Air Moyenne Portée Terrestre

SMART-L: Signal Multibeam Acquisition Radar for Tracking, L-Band

Radar sensors seem suitable to produce fire-control solutions for HOT, and point defence should be possible, assuming the availability of suitable sensors and effectors. For a comprehensive area defence, a very large number of sensors is required, especially when considering the need for a robust array of sensors and the required communications architecture. This also necessitates a very robust network and seamless integration into NATINAMDS. Given these networked capabilities, the remote engagement options[3] should be made available to support optimized sensor-effector usage.

In general, an interceptor needs to be capable of reaching an intercept point with its intended target, and it needs to have an appropriate warhead to deliver a sufficient effect on the target. For HOT, this means that interceptors need to reach altitude bands between 20 and 80 km. Also, the interceptor needs to have extended range at high speed, and very high agility to be useful against manoeuvring HOT. Specific parameters for different HOT must be analysed and identified. Options for other than ground-based interceptors should be assessed as well.

Furthermore, the effects on target need to be sufficient to deny the primary mission of the HOT and to minimize collateral damage, such as debris or remaining Weapons of Mass Destruction (WMD). Based on BMD experience, hit-to-kill technology can achieve such effects. Alternatively, interceptors with fragmentation warheads could be effective due to the high speeds, high temperatures and importance of structural integrity of a HOT. Even minor amounts of damage caused by small fragments might be sufficient to cause fatal structural damage. Overall, it has to be analysed, which kind of interceptor is preferable for engaging HOT targets. Directed energy solutions appear to be less promising since HOT are designed to withstand high temperatures by nature. Electronic Warfare such as jamming and spoofing of HOT seems to be very difficult due to the high speed and non-predictability of offensive systems.

On the assumption that a HOT interceptor is available, appropriate fire doctrines need to be determined. This could be supported by ideas from swarm technology or artificial intelligence. Also, a higher level of interceptor autonomy might be useful, but a legal framework to employ such systems must be developed and agreed upon before use.

Conclusion

In the light of Russia's claim that their HGVs have been operationally available since December 2019 and western scientists' assessments that the development of HOT is progressing well, it is reasonable to assume that HOT will be appearing on the battlefield within the next 5–10 years; hence the imminence of the threat is very credible. Considering procurement timelines for advanced weapon systems such as HOT defence systems or the time it might take to adapt existing AMD systems, NATO will have a capability gap against HOT for some time. A decision must be made as soon as possible on how to mitigate this gap. The potential deficit in credible deterrence must be offset by a balanced mix of defensive measures and credible measures of 'deterrence by punishment'. Considering that NATO has no comprehensive area defence against regular cruise missiles for various reasons, it will be even more challenging to achieve this for HOT.

Hence, the initial focus for HOT defence should be point defence of identified critical military or civilian assets. As a second step, the necessity and feasibility of area defence needs to be looked at and possibly implemented. Overall, NATO must ensure that the required framework for credible deterrence of adversaries with HOT remains intact.

1. NATO Science and Technology Organization Technical Report: 'Assessment of the Status and Challenges Posed by Hypersonic Operational Threats', 28 Aug. 2020.
2. NATO's Allied Joint Publication 3.3 Edition B, 2016.
3. Young, Bonnie W. 'Future of Integrated Fire Control', Northrop Grumman, 2005. Available at https://apps.dtic.mil/dtic/tr/fulltext/u2/a464249.pdf.

Lieutenant Colonel Andreas Schmidt

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

Distance No Longer Equals Protection

Development and Testing of Authorities and Planning Concepts for Hypersonic Strike Weapons

By Mr F. Patrick 'Spam' Filbert, US, Joint Hypersonic Strike, Planning, Execution, Command and Control Joint Test

'The military services are ramping up spending on hypersonic weapons and defense capabilities, from rocket-based glide systems to air-breathing weapons to low-altitude cruise missiles and more.'[1]

Where to Start

Advances in technology continue to outpace the techniques, procedures, and doctrinal aspects of how a new weapon integrates into the Joint Force, specifically Hypersonic Strike Weapons (HSW). The 'traditional model' has been 'develop what we want, we will figure things out later', which can thicken the fog of war due to unintended second- and third-order effects that were not originally considered. Figuring out the use aspect, prior to full weapon development instead of after, can rapidly improve Joint Force integration. At the same time, technology's rapid advancement can and does outpace doctrinal development which also challenges training.

© Photo provided by Purdue Research Foundation

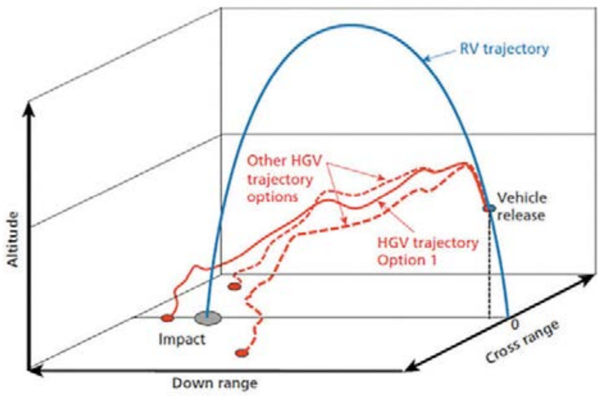
M1A1 Abrams Main Battle Tank.[2]

What is the Rationale?

Manoeuvrable HSWs are not new. Research began during the Cold War in the US and Soviet Union, but various technological hurdles resulted in a 'start/stop' approach that continued through the end of the Cold War and follow on period of perceived peace.[3] Such hurdles encompass the areas of propulsion, navigation, and heat resistance due to the high speeds involved. However, recent 21st Century technological developments have led to progress in a number of areas. These advancements have enabled China, Russia, and the US to develop and test HSWs with China and Russia fielding HSWs.[4]

Recent demonstrations, claims, and military parades by China and Russia appear to show both countries are ahead of the US in HSW development. China unveiled new HSWs at a military parade in 2019 and Russia claims to have tested HSWs in 2018, fielding an aircraft-launched HSW called Kinzhal and a land-based HSW identified as Avangard in 2020. How these countries and the US, view HSW use and Joint Force integration differs – to include perceptions of the actual advantage of the weapon.

During the Cold War, the nuclear triad of Intercontinental Ballistic Missiles (ICBM), Air-Launched Cruise Missiles (ALCM), and Submarine Launched Ballistic Missiles (SLBM) provided the superpowers with a strategic measure of deterrence and power. However, ICBMs, ALCMs, and SLBMs can be tracked by sensors due to their stable ballistic trajectory allowing target assessment based on their flight path. HSWs introduce a measure of unpredictability after launch. This is due to lack of sensor optimization to accurately predict, target, and intercept HSWs as they fly towards their targets which remain unknown until the final seconds due to the speed and manoeuvrability of HSWs.



Ballistic Reentry Vehicle (RV) versus Hypersonic Glide Vehicle Trajectories.

© Courtesy of RAND, document RR-2137-CC[5]

ICBMs required significant resources and were developed in secret. This meant that only countries with the resources for development and fielding could afford these weapons. Further, actual use of ICBMs beyond their deterrence attributes is less likely than

© US Navy, Oscar Sosa

Common HSW warhead launch, Pacific Missile Range Facility, Kauai, HI, 19 March 2020.[11]

use of HSWs; especially as US HSWs are planned to only carry conventional payloads. From a cost perspective, HSWs will be less expensive than a SLBM (USD 31 million for a D5/TRIDENT II) compared to an estimated USD 6.9 million per HSW.[6,7]

'Hypersonic missiles are a key military capability because we can reach out and launch these things from thousands of kilometres and hit their targets within a few feet. Their high speed also makes them extraordinarily survivable because it is so hard to shoot down, and that's why the United States as well as Australia are aggressively pursuing this technology.'

Dr George Ka'iliwi III,
US Indo-Pacific Command J8[8]

Increasing capability as a cost reduction attribute is not just something the US, China, and Russia are working towards. The development of HSWs has spread to international partner nations (e.g., Australia and India) who are benefiting from teaming with the US, China, and Russia. This teaming could provide for further cost reduction due to sharing HSW technology development. Additionally, Japan, France, and Germany are in development of their own HSWs and benefit from available research.[9]

Who is Doing Something About It?

In the US, HSW development and testing continues at a more measured pace specific to the fielding of conventional armed systems. This approach requires developing a high degree of accuracy that Russian and Chinese weapons do not require with their intention to maintain nuclear-capable HSWs. Recent US testing of HSWs in 2017 and 2020 resulted in successful flight test events towards the development of a common HSW warhead.[10]

An additional HSW aspect to consider is the potential response that may occur from an adversary after a 'first use', especially if the adversary has their own HSWs and is a nuclear power. Critical to HSW use is ensuring an adversary nation does not confuse a HSW launch with the launch of an ICBM or SLBM, particularly through proper messaging of the new capability. The impact of adversary propaganda, disinformation, and wide-scale efforts to misinform or create a media panic must be managed related to a potential war between nuclear-armed nations. To date, there are only two examples of such wars. Yet the aspect of vertical escalation towards nuclear weapons use was identified and managed by the nations involved – 1969 Sino-Soviet war and 1999 Kargil war between India and Pakistan. Neither conflict had the aspect of instant news and social media that will have a definite impact on information operations and strategic messaging to keep escalation from occurring in a future conflict.[12]

How to Start HSW Incorporation?

Most reports on HSWs have been specific to the development of the weapon, problems of control at hypersonic speeds (in excess of Mach 5 or 3,800 miles per hour), and missile/rocket body design to boost the warheads to high speed. Yet the ability of HSWs to hold a target at risk because of the speed and unpredictability attributes, coupled with the difficulty in identifying the specific target, should be driving discussions on concept of operations (CONOPS) development before, not after, HSWs are fielded. Producing HSWs is not as easy as simply opening or retooling a production line. HSWs require a long lead production time, resulting in low availability until production efficiency is achieved. How to incorporate HSWs into planning and, ultimately, senior leader understanding of use effects must be resolved before HSWs are fielded.

Developing factors specific to Command and Control (C2) authorities and planning for HSWs at the operational and strategic levels of war requires early consideration development. The Joint-Hypersonic Strike Planning, Execution, Command and Control (J-HyperSPEC2) Joint Test (JT) was chartered in August 2018 under the authority of the Office of the Secretary of Defense (OSD), Director, Operational Test and Evaluation. J-HyperSPEC2 JT's charter is to develop, test, and evaluate a C2 CONOPS to manage authorities, support employment, planning, and execution for HSWs. With the continual push for rapid development and fielding, the J-HyperSPEC2 JT is at the forefront of planning for the deployment and use of these new weapons.

The J-HyperSPEC2 JT is sponsored by US Strategic Command (USSTRATCOM) with the team operating in two locations: Offutt Air Force Base (AFB), Nebraska, and Nellis AFB, Nevada. The J-HyperSPEC2 JT team worked closely with several Combatant Commands (CCMD), Services, and OSD to develop an initial CONOPS through two writing groups. The J-HyperSPEC2 JT team conducted a multi-part field test to collect data on the CONOPS for revision and validation.

The A2/AD Challenge

The Joint Force remains over-reliant on stand-off weapons and fourth-/fifth-generation strike platforms to address the Anti-Access/Area Denial (A2/AD) challenge. As the adversary countries continue to push their 'A2/AD bubble' outwards, developing weapons to overcome this expansion enables a way to get within the adversary's decision-making process.

To address the A2/AD expansion aspect to better integrate HSWs, the J-HyperSPEC2 JT conducted development and refinement efforts using warfighter inputs from events such as CONOPS writing groups and CCMD exercises as test events to test and refine the CONOPS. The team interacted with US European Command (USEUCOM); Commander, Submarine Force, US Pacific Fleet; USSTRATCOM; and the 805th Combat Training Squadron. The resulting C2 CONOPS was field-tested at US Indo-Pacific Command's (USINDOPACOM) Exercise Pacific Sentry (PS) in January 2020 in Hawaii.

The J-HyperSPEC2 JT trained exercise participants on the CONOPS and notional HSW capabilities and then observed deliberate planning and dynamic targeting processes. The test's data collectors observed HSW discussions and planning efforts at lower echelon components, gathered multiple data points to inform CONOPS revisions and, concurrent with the PS exercise, the team supported the integration of HSW into the Chairman of the Joint Chief of Staff's Global Integration Exercise 20. This integration enabled discussions of US conventional HSW 'first use'. Post-exercise, a series of General Officer/Flag Officer interviews and roundtables occurred to gain insight on how senior leaders identify HSW integration, authorities of use, escalation, and strategic messaging.

Representative examples of air-, sea-, and land-HSW launchers.

Looking Forward

Exploring the 'how to use and when' aspects are part of the CONOPS development. Specific to the use aspect, the team identified early in CONOPS development a lack of planning tools to support planner's efforts to incorporate HSWs into operations. While several entities were developing such tools, they were not ready for use during the PS exercise. To enable CONOPS testing the team developed a Mission Planning Handbook (MPH) as a surrogate planning tool. The MPH provided PS mission planners with HSW attributes enabling current process planning.

The J-HyperSPEC2 JT has already benefited the Department of Defense (DoD) in getting ahead of the 'buy, field, develop concept of use' approach. As the Services field HSWs, enabling them the capability to hold distant, defended, fleeting, and high-value targets at risk, the warfighter will be better equipped to meet national objectives and impose costs on potential adversaries by having a way to do this via the C2 CONOPS.

Depiction of the US Falcon hypersonic test vehicle prior to re-entering the atmosphere.[16]

The J-HyperSPEC2 JT is currently slated to end in Fall 2020. This does not mean future HSW-related efforts will cease. The C2 CONOPS will provide an effective operational and strategic context to inform HSW use and, eventually, inform development of Tactics, Techniques, and Procedures (TTP). Such TTPs will further reinforce the use of HSW by empowering the commander to develop standards in the areas of manning, equipping, training, and planning in the Joint Force. In the interim, the J-HyperSPEC2 JT developed CONOPS will provide planners with a starting point for HSW use while also serving to focus future DoD and industry investment.

1. Cynthia Sequin, 'NDIA, Purdue launching inaugural hypersonics capabilities conference to advance transformational military capabilities', Purdue University, 29 Jul. 2019 [cited on 30 Nov. 2019]. Available from https://www.purdue.edu/newsroom/releases/2019/Q3/ndia,-purdue-launch-inaugural-hypersonics-capabilities-conference-to-advance-transformational-military-capabilities.html; Internet.
2. Army Tanks, 'M1 Abrams Main Battle Tank', 17 Feb. 2019 [cited 14 Mar. 2020]. Available from https://www.tanks.net/; Internet.
3. Stone, Richard, '"National Pride at Stake." Russia, China, United States race to build hypersonic weapons', Science Magazine, 8 Jan. 2020 [cited 26 Mar. 2020]. Available from https://www.sciencemag.org/news/2020/01/national-pride-stake-russia-china-united-states-race-build-hypersonic-weapons#; Internet.
4. Chan, Millie, 'China and Russia's push to develop hypersonic weapons raises fears of arms race with US', South China Morning Post, 19 Jan. 2020 [cited 20 Apr. 2020]. Available from https://www.scmp.com/news/china/military/article/3046667/china-and-russias-push-develop-hypersonic-weapons-raises-fears; Internet.
5. Speier, Richard; Nacouzi, George; Lee, Carrie; and Moore, Richard; 'Hypersonic Missile Proliferation: Hindering the Spread of a New Class of Weapons', RAND Corporation Report 2137 [cited 10 Sep. 2020]. Available from https://www.rand.org/pubs/research_reports/RR2137.html; Internet.
6. Department of the Navy, 'Fact File: Trident II (D5) Missile', [cited on 22 Apr. 2020]. Available from https://www.navy.mil/navydata/fact_display.asp?cid=2200&tid=1400&ct=2; Internet.
7. Axe, David, 'Should America Buy 2000 Hypersonic Missiles Instead of Another Carrier?', National Interest, 12 Nov. 2019 [cited 22 Apr. 2020]. Available from https://nationalinterest.org/blog/buzz/should-america-buy-2000-hypersonic-missiles-instead-another-carrier-95161; Internet. Cost calculation derived from comment 'Which do you think the Chinese leadership would fear more: 2,000 conventional strike missiles . . . or one new carrier? Because those two things cost about the same amount of money.' $13 billion divided by 2,000 = $6.9 million.
8. Harper, Jon, 'Hypersonics, AI Top Indo-Pacific Command's Tech Wishlist', National Defense Magazine, 3 Mar. 2020 [cited 6 May 2020]. Available from https://www.nationaldefensemagazine.org/articles/2020/3/11/indo-pacific-command-lays-out-top-st-priorities; Internet.
9. Sayler, Kelley, 'Hypersonic Weapons: Background and Issues for Congress', Congressional Research Service Report R45811, 11 Jul. 2019, p. 15.
10. Press Release, 'Department of Defense Tests Hypersonic Glide Body', Office of the Secretary of Defense, 20 Mar. 2020 [cited 22 Apr. 2020]. Available from https://www.defense.gov/Newsroom/Releases/Release/Article/2119458/department-of-defense-tests-hypersonic-glide-body/; Internet.
11. Ibid.
12. Morris, Zachary, Maj US Army, 'Risking Nuclear Escalation The Characteristics of War from the Sino-Soviet and Kargil Wars', The Institute of Land Warfare at the Association of the US Army, Oct. 2019 [cited 22 Apr. 2020]. Available from https://www.ausa.org/sites/default/files/publications/LWP-129-Risking-Nuclear-Escalation-The-Characteristics-of-War-from-the-Sino-Soviet-and-Kargil-Wars.pdf; Internet.
13. The Engineer, 'US Airforce Tests Its New Hypersonic Missile On A B-52 Bomber', Wonderful Engineering, 17 Jun. 2019 [cited 10 Jun. 2020]. Available from https://wonderfulengineering.com/us-airforce-tests-its-new-hypersonic-missile-on-a-b-52-bomber/; Internet.
14. Wang, Brian, 'US Navy Will Develop Hypersonic Submarine Launched Weapons', nextBIG Future, 24 Nov. 2018 [cited 10 Jun. 2020]. Available from https://www.nextbigfuture.com/2018/11/us-navy-will-develop-hypersonic-submarine-launched-weapons.html; Internet.
15. Malyasov, Dylan, 'U.S. Army discloses ground-launched hypersonic weapon development', Defence Blog, 11 Aug. 2019 [cited 10 Jun. 2020]. Available from https://defence-blog.com/news/army/u-s-army-discloses-ground-launched-hypersonic-weapon-development.html; Internet.
16. Andrew Reddie, 'Hypersonic missiles: Why the new "arms race" is going nowhere fast', Bulletin of the Atomic Scientists, 13 Jan. 2020 [cited 21 May 2020]. Available from https://thebulletin.org/2020/01/hypersonic-missiles-new-arms-race-going-nowhere-fast/; Internet.

Mr F. Patrick 'Spam' Filbert

is a Test Planner for the J-HyperSPEC2 JT at Nellis AFB, NV. He has supported three previous Office of the Secretary of Defense Joint Test (Distributed Air Operations Center planning, swarming UAS, counter-UAS) efforts. He holds a History degree from the University of Hawaii and a Master's of Strategic Intelligence with Honors from American Military University. In 2019 he received his Intelligence Fundamentals Professional Certification. Commissioned an Armor Officer and transitioned to Military Intelligence he served 24 years retiring as a Major. Post-military career includes Senior Intelligence Analyst (547 & 526 Intelligence Squadrons), Intelligence Contract Team Lead (432 Wing Operations Center), and Project Manager, USINDOPACOM J2 Socio-Cultural Intelligence Dynamic Analysis effort.

NATO Space

Recognition versus Current Reality

By Lieutenant Colonel Henry Heren, US Space Force, JAPCC

'People see what they want to see and what people want to see never has anything to do with the truth.'[1]

Introduction

On 4 December 2019, the North Atlantic Council announced in London: 'We have declared space an operational domain for NATO, recognising its importance in keeping us safe and tackling security challenges, while upholding international law'.[2] In the months since that declaration, NATO developed an Initial Implementation Plan for Space, while outside NATO there have been numerous opinion pieces published recommending how NATO should proceed from both policy and strategy perspectives. The goal of each of these efforts has been to normalise Space within NATO, to recognise NATO's reliance on Space-based capabilities and to promote greater understanding and appreciation for safeguarding the use of those capabilities. Questions abound concerning how NATO should integrate Space-based capabilities into existing policy, doctrine, strategy, operations, and exercises.

Germany concluded in its 2010 released Space Strategy that 'a paradigm shift has occurred within space: once a symbol of the technology race and a contest between opposing systems, it is now, in every sense, a part of our everyday lives and an essential instrument for the achievement of economic, scientific, political and social goals'.[3] In 2019, France released its Space

Defence Strategy which 'outlines the future of our space defence in accordance with a roadmap that looks to 2030 and beyond'.[4] This document 'marks a turning point for the future of our armed forces and for France's capacity to act in all domains and maintain its strategic autonomy of assessment and decision'.[5] Most recently, in June 2020, the United States (US) released its Department of Defense (DoD) Space Strategy which states: 'This strategy identifies how DoD will advance spacepower to enable the Department to compete, deter, and win in a complex security environment characterized by great power competition.'[6] Collectively, these nations and others are experiencing a renewed interest, excitement, and focus on Space-related activities. It is both natural and understandable that this enthusiasm will cross over into NATO organizations and discussions.

Several Alliance Nations have increased promotion of Space within their own militaries. France, Germany, Italy, the United Kingdom, and the US have moved to establish Space Commands to varying degrees, and the US took the additional step of establishing an independent military service, the US Space Force. The combined national activities, accompanied by growth in the commercial Space sector, have created an excitement surrounding Space endeavours not seen in several decades.

However, the various advancements in the commercial sector, national militaries, and NATO with regards to Space are far from equal. The enthusiasm felt across communities of interest does not mean all nations are at the same stage of development and capacity with regards to Space-based capabilities. This article will discuss the unique challenges facing NATO with regards to Space strategy, exercises, and personnel as compared to other national entities which in some cases possess more mature capabilities. The goal being to allow for discussion on a way ahead for Space in NATO based upon NATO requirements.

Strategy

Even as NATO recognised Space as an operational domain, NATO Secretary General Jens Stoltenberg emphasized: 'NATO has no intention to put weapons in space. We are a defensive Alliance.'[7] He further clarified, 'NATO will continue to by and large draw on national space capabilities in support of its missions and operations'.[8] Currently NATO receives Space-related Data, Products, and Services (DPS) from several member nations, and does not own or operate any Space-based capabilities. This means, currently, when it comes to the legal authority to operate Space-based Capabilities, including command and control, the NATO Command Structure (NCS) does not play an active role.[9]

However, this does not mean the NCS has no role to play with regards to Space. The NCS recently approved a concept for a NATO Space Centre, which will serve as a hub for Space-related information, expertise, and activities and directly liaise with the several nations providing Space DPS. Once operational and fully staffed, it will provide greater ability for NATO to coordinate requests for Space DPS.

In the meantime, with regards to Space Strategy, the focus must be on how NATO ensures the flow of Space DPS within the NCS. Calls for additional NATO Space Strategies[10] 'in parallel to its maritime and airpower plans'[11] to 'help NATO align members states on key tactics, tools, and procedures'[12] are premature at best as this role is currently fully the purview of the member nations. In the future, if NATO reconsiders its position and seeks to acquire NATO-operated Space-based capabilities, then a strategy on how to utilise those capabilities will not only be prudent but necessary. NATO is currently better served focusing on how it will work with the nations to ensure interoperability and access to Space DPS across the Alliance, and not pursuing strategies that require both capabilities and authorities that it does not currently possess, and is unlikely to in the near future.

Exercises

It has been suggested that NATO develop large-scale Space-focused exercises, akin to the several Air, Land, and Maritime focused exercises. As previously noted, NATO does not own nor operate any Space-based capabilities, and calls for NATO to host large-scale Space exercises ignore the lack of capabilities present to necessitate such an exercise. NATO could benefit from sending personnel in an observer role to Space-focused exercises conducted by the nations, but that is significantly different from what is being suggested.

Recommendations for these exercises cite the ability 'to systematically develop and refine space contingencies against red cell adversaries'[13] to 'signal allied resolve'.[14] While laudable, these ideals overlook not only the lack of authorities within NATO regarding Space-based capabilities, but also the fact that NATO forces are reliant on Space DPS … which should be the focus of increased Space-participation in exercises.

With only 19 Space Billets spread across the NCS, and some of those filled by other than Space educated, trained, and focused professionals, for the time being NATO would be better served in ensuring its leaders understand the role Space plays in their operations beyond the mere acknowledgement of Space's role as an operational domain. The Space Professionals who have served in the NCS have done an admirable job conveying that Space is important, to the extent that exercise controllers are not permitted to fully exercise degradation of Space DPS as it affects the exercise too significantly.

Space Professionals participating in exercises need to be given the latitude to meaningfully impact Space DPS so the entire exercise team can not only gain increased appreciation for how reliant they are upon Space-based capabilities, but also so Tactics, Techniques, and Procedures (TTP) can be developed from valuable lessons learned. Those TTPs will be critical if NATO finds itself in a conflict with not only peer-competitors, but also those competitors who are able to exploit asymmetric seams to reduce NATO Combat Capabilities.

Personnel

The creation of any new policies, strategies, doctrines, and expanded exercises will rely on educated and trained personnel to create and maintain them. Within the NCS, as previously noted, there are currently 19 Space Billets. The validity of that number drops precipitously when considering some of these positions are not filled, while still others are filled with people who are not educated, trained, nor experienced in Space Operations (as conducted by NATO nations). Add in the fact many personnel assigned to those positions are double-billeted, which means they work primarily on other activities and responsibilities, and focus only occasionally on Space-related issues, and the effectiveness of that already limited number of personnel is further reduced. The result is NATO has only a handful of Space-proficient personnel dedicated day-in and day-out to Space-related activities.

A concept calling for the establishment of the NATO Space Centre was recently approved by the Defence Ministers in October 2020. That concept includes an increase in Space personnel billets within the NCS, at the Space Centre and at the Joint Force Commands

and subordinate organizations. Space educated and trained professionals are desperately needed to fill these billets if NATO is to increase its interoperability regarding Space.

Several challenges stand in the way of a trained and ready NATO Space cadre. Aside from the obvious funding concerns, the primary nations to which NATO would look to provide these professionals are, as noted earlier, reorganising their Space communities internally to their respective nations. They are therefore currently ill-suited to provide additional personnel to the NCS. This could result in personnel being assigned to the Space Centre without the requisite Space education and experience, requiring an increase in training and additional funding. It also means NATO may have a Space Centre severely lacking in resident Space Operations Expertise.

Conclusion

As Space Professional and policy-makers seek to influence and guide NATO's approach to Space, they must be careful not to project ideas compatible within their national Space approaches onto NATO organizations, in other words to see what they want. This will include understanding that NATO's use of Space is almost completely as a utility to support operations in other domains, not operations in the Space Domain. The Alliance has not placed an emphasis on

Space significant enough to generate personnel and capabilities comparable to several of its member nations, and thus requires a different approach. National Space Professionals need to ensure they understand the capabilities and capacity within NATO, before promoting recommendations which NATO might not be prepared to incorporate or execute at this point in its integration of Space-related capabilities and expertise.

1. Bolaño, Roberto. 2666, Picador; Reprint edition (1 Sep. 2009).
2. NATO London Declaration, 4 Dec. 2019. Available at: https://www.nato.int/cps/en/natohq/official_texts_171584.htm. [accessed 20 Aug. 2020].
3. German Federal Ministry of Economics and Technology, Making Germany's Space Sector Fit for the Future: The Space Strategy of the German Federal Government, Nov. 2010, p. 3.
4. French Ministry for the Armed Forces, Space Defence Strategy, 2019, p. 8.
5. French Ministry for the Armed Forces, Space Defence Strategy, 2019, p. 12.
6. US Department of Defense, Defense Space Strategy, June 2020, p. 1.
7. Paulauskas, Kestutis, 'Space: NATO's Latest Frontier', NATO Review, 13 Mar. 2020. Available at: https://www.nato.int/docu/review/articles/2020/03/13/space-natos-latest-frontier/index.html. [accessed 30 July. 2020].
8. Paulauskas, Kestutis, 'Space: NATO's Latest Frontier', NATO Review, 13 Mar. 2020. Available at: https://www.nato.int/docu/review/articles/2020/03/13/space-natos-latest-frontier/index.html. [accessed 30 Jul. 2020].
9. The NATO Communications and Information Agency (NCIA), which exists outside of the NATO Command Structure, does operate the payload of some communications satellites. However, the satellites themselves are control by a consortium of nations (France, Italy, and the United Kingdom). Additional information available at: http://www.eu2015lu.eu/en/agenda/2015/11/25-seminaire-SatCom/3_Presentation-Tom-PLACHECKI.pdf. [accessed 26 Aug. 2020].
10. In addition to NATO's Overarching Space Policy approved on 27 Jun. 2019.
11. Silverstein, Benjamin, 'NATO's Return to Space', War on the Rocks, 3 Aug. 2020. Available at: https://warontherocks.com/2020/08/natos-return-to-space/. [accessed on 3 Aug. 2020].
12. Silverstein, Benjamin, 'NATO's Return to Space', War on the Rocks, 3 Aug. 2020. Available at: https://warontherocks.com/2020/08/natos-return-to-space/. [accessed on 3 Aug. 2020].
13. Bowman, Bradley and Andrew Gabel, 'NATO Declares Space 'Operational Domain,' but More Work Remains', Defense News, 16 Dec. 2019. Available at: https://www.defensenews.com/opinion/commentary/2019/12/16/nato-declares-space-operational-domain-but-more-work-remains/. [accessed on 3 Aug. 2020].
14. Silverstein, Benjamin, 'NATO's Return to Space', War on the Rocks, 3 Aug. 2020. Available at: https://warontherocks.com/2020/08/natos-return-to-space/. [accessed on 3 Aug. 2020].

Lieutenant Colonel Henry Heren

is a NATO Space & Cyberspace Strategist assigned to the JAPCC. He is a Master Space Operator and a Fully Qualified Joint Staff Officer with operational and planning experience in the Pacific, Europe, Africa, and the Middle East. After more than 28 years' service in the US Air Force, he transitioned to the US Space Force in 2020. He is a graduate of the US Air Force Weapons School, with experience in assignments focusing on Space, Cyberspace, and Electronic Warfare Operations.

Responsive Space for NATO Operations

By Wolfgang Jung, German Aerospace Center (DLR)
By Lieutenant Colonel Tim Vasen, GE AF, JAPCC

Introduction

Space Support plays a significant role in modern warfare. After the fall of the iron curtain, the threat to western Space assets and capabilities was significantly diminished. The current development of Space capabilities, especially on the commercial side, as well as the increased number of Space users, has changed this situation. Use of the Space domain is becoming more congested and contested. Additionally, counter-Space assets and methods are being proliferated worldwide. Space systems must be protected, redundancies must be increased or other means of security have to be pursued, all of which falls under the umbrella of resilience. Another option is to pursue alternative solutions, using also non Space capabilities, which are comparable to a Space-focused approach or refer to other technologies which still have to be developed and fielded. The combination of resilience methods and alternative solutions that together ensure persistent support to warfighters is referred to in the context of this article as ´Responsive Space´.

This article is the first in a series on the topic of Responsive Space and will focus on the definitions as well as potential worldwide concepts currently being discussed. Ongoing developments, an analysis for NATO and national options, and chances for contributions to NATO will also be discussed in follow-on articles.

Space Resilience versus Responsive Space

It is not simple to delineate between the two terms Space Resilience and Responsive Space, as these two terms overlap in several ways. Still, a path to understanding the differences can be found in the following documents provided by the USA.

The fact sheet on Space Resilience published in 2011 by the US Department of Defense included reconstitution, meaning the ability to plan and execute operations to replenish lost or diminished functions.[1] The overall goal for reconstitution was ensuring at least an acceptable level of functionality such that military operations can still be pursued.

In the white paper on Space Domain Mission Assurance published in 2015, the term reconstitution was extracted from resilience and introduced on the same level of relevance.[2] Reconstitution is further defined in that document as adding capability or capacity through additional assets or links, which makes it an element of Responsive Space. It is further stated that reconstitution and resilience complement each other.

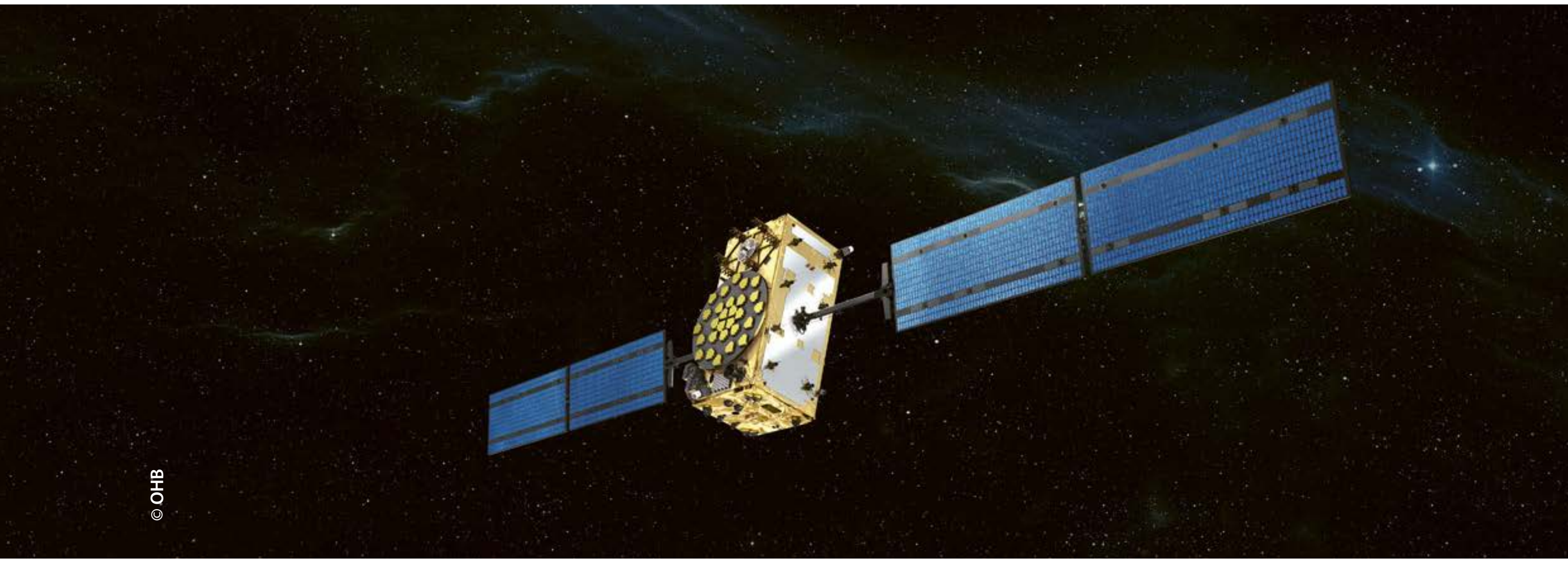
Both a robust and resilient Space architecture and the ability to react to hostile acts via Responsive Space means offers a wide field of deterrence. As an Alliance of 30 nations, NATO should use its multinational approach to gain the greatest advantage from nationally-provided Space data, products, and services by developing resilience as well as Responsive Space methods as needed.

Information regarding Space Resilience concepts for NATO are discussed and addressed in the NATO-Restricted JAPCC White Paper 'Resiliency in Space as a Combined Challenge for NATO' published in January 2021.[3]

Definitions and Concepts of Responsive Space of NATO Nations

United States

The need for a Responsive Space concept in the USA was initiated after vulnerabilities and shortfalls were discovered by the Rumsfeld Commission in January 2001.[4] The findings led to a programme called Operational Responsive Space (ORS). In 2007, the US definition of ORS was given as the ability to gain 'assured Space power focused on timely satisfaction of Joint Forces Commanders' needs'. ORS 'will provide an affordable capability to promptly, accurately and decisively position and operate national and military assets in and through Space and near Space'.[5] Most of the US techniques focus on responsive launch capabilities. The US Joint Publication on



Space Operations addresses the responsiveness of Space assets and services in general and the flexibility of their use.[6] The responsive access to Space and the ORS programme are also addressed, but they mainly feature under the responsive launch function. The Defence Space Strategy released in 2020 addresses the need for capabilities to counter hostile use of Space, which also includes responsive means.[7]

Canada

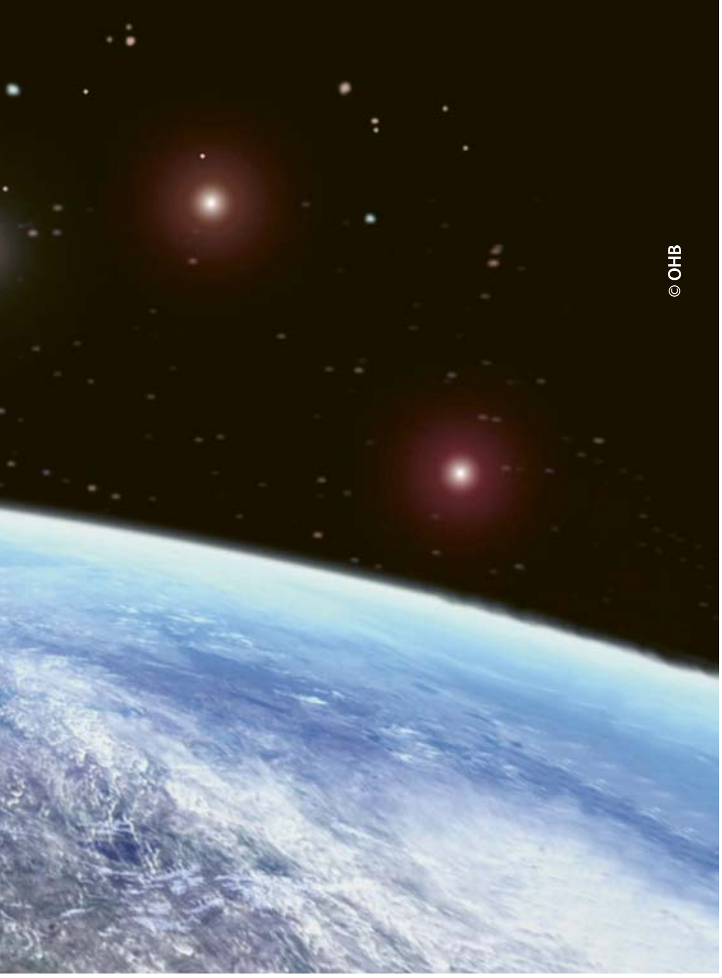
Canada does not directly address Responsive Space as a term.[8] While adapting US definitions, Canada focuses on cooperation and collaboration with allies and partners to increase resilience and counter opponents' threats. Without using the term directly, Canada addresses methods and actions that can be referred to Responsive Space.

France

In its Space Defence Strategy published in 2019, France introduces the term Space Service Support in its military Space operations.[9] One element is the reconstitution of capabilities. Apart from restoring capacities, compensating for or replacing a diminished or missing capability are identified as options. To arrange this, the potential use of complementary allied or commercial capabilities which are made available via a cooperative and collaborative approach are included in the Space Defence Strategy. Even though the term Responsive Space is not used, the French plan results in a similar capability.

Germany

The Space Strategy of the German Government (2010)[10] states that internal and external stability increasingly depends on the functioning of Space-based infrastructure. This makes Germany vulnerable to both unintentional and deliberate disruption (electronic interference, hostile takeover of satellites), or even targeted destructive interference. The German White Paper on Security Policy and the Future of the Bundeswehr (2016)[11] and the Conception of the Bundeswehr (2018)[12] have all declared Space as an operational domain. Satellites and associated ground segments are described as security-relevant critical infrastructure, which have to be resiliently designed and need to be protected.



The Federal Ministry of Defence tasked the German Aerospace Center (Deutsches Zentrum für Luft- und Raumfahrt [DLR]) to establish the technology base for a national Responsive Space Capability (RSC) and to demonstrate key elements in Space. On 1 September 2020 the Responsive Space Cluster Competence Center (RSC3) was inaugurated.[13] Responsive Space is understood to be the ability to launch small satellites (up to 500 kg) on demand and on call into Low Earth Orbit (LEO) and to start operating within days, in order to reconstitute lost capabilities, augment existing – capabilities, fill unanticipated gaps in capabilities, and enhance survivability and deterrence.

United Kingdom

In their National Space Security Policy, released in 2014, Responsive Space is not stated directly. However, as an element of Responsive Space, service assurance is stated which should be realized through the integration of commercial opportunities.[14] The UK Joint Doctrine dealing with Air and Space Power states that it generally follows the US definitions.[15] The term Responsive Space is not stated in this document, but with synergies inside the country and in collaboration with allies, specific elements are referred to and responsiveness is implied.

Definitions and Concepts of Responsive Space of European Organizations

International Space University

The International Space University, located in Strasbourg, France, conducted a study, with results published in 2010, on the requirement and capabilities for European Responsive Space.[16] An outcome of this study was highlighting the fact that definitions change over time, driven by threats and requirements. The study stated that most Responsive Space definitions and developments are focused on responsive launch capabilities. Responsive Space encompasses more than just the short notice launch of satellites to either close gaps in the Space architecture due to successful opponents' counter-Space activities, or to intensify the use of Space-based services in areas of interest via specifically designed orbits. The Space University study assessed responsive actions instead, such as reorientation of satellites or the use of on-orbit spare satellites.

European Space Policy Institute (ESPI)

Europe, via the ESPI, has been monitoring and assessing the potential need for Responsive Space capabilities for security since 2010.[17] Recent worldwide counter-Space actions have renewed the relevance and interest in the analysis. The study was primarily conducted to analyse the US ORS programme and to find synergies for Europe to contribute Responsive Space options to support security organizations, such as the European Defence Agency (EDA) and NATO.

Interoperability, capability sharing, cooperation, and integration are addressed as the building blocks for Responsive Space in the future. Synergies between the civil and military applications, not just from the nations but also from organizations such as the European Union (EU), are recommended. Space functional areas of Positioning, Navigation and Timing (PNT), Satellite Communication (SatCom) and Intelligence,

Surveillance and Reconnaissance (ISR) in particular are identified and assessed to be the focus. Technological requirements have to be formulated and new technology has to be embedded to ensure flexible and affordable solutions for operational capabilities, even when they are part of a long-term process. On the administrative side, data sharing via agreements as well as definitions and standards for data formats in secured networks that allow data throughput to whoever needs it must be ensured.

To achieve the best possible Responsive Space architecture and service for Europe, and for NATO as a prominent partner, the 'responsiveness via international collaboration' seems to be the objective for the future. Responsive Space techniques in a multinational European approach made available as a contribution to the Alliance gives NATO the chance to use a more resilient architecture that is based on interoperable or at least shareable national and commercial capabilities. To ensure this, NATO has to obtain an overview of the national capabilities and capacities that the member nations are willing to provide.

Definitions and Concepts of Responsive Space of other Nations

People's Republic of China

China did not directly address developments and needs for Responsive Space technology in its Space White Paper (2016).[18] However, the statements focused on developing technology with a comprehensive approach, combined with the ongoing research at military universities in particular, lead to the assessment that China is very active in this type of Space approach. The development of counter-Space technology underlines this. China is able to degrade an opponents' Space capability and to react to the degradation of its own Space architecture by an opponent, which provides a certain level of deterrence. The Defence White Paper released in 2019 points out one national defence aim that China's security interests in outer Space[19] have to be safeguarded.[20]

Russian Federation

Russia does not directly address the term Responsive Space. Their military doctrine released in December 2014, identified some technical means that have to be ensured with all available options.[21] For the internal security of the country, strategic communication links which also rely on SatCom services are specifically stated. Ensuring a persistent service can be seen as a Responsive Space action. Russia follows an inter-governmental approach in security which includes Space data, products and services. In the National Security Strategy released in 2015, the inter-governmental approach was confirmed.[22] Additionally, Russia will monitor the worldwide development of Space technology to ensure that it does not fall behind potential opponents. Even if it is not stated, it encompasses counter-Space as well as Responsive Space means.

Interim Assessment and Conclusion

Responsive Space is an element ensuring persistent Space Support for NATO. As addressed, some Responsive Space capabilities are already available in certain NATO member nations. With the further development of Space within the NATO Command Structure, it has to be assessed which role NATO will play in the future regarding Responsive Space. The nations of the Alliance offer a wide area for burden-sharing, especially for the European allies to support the USA as the dominant Space power. With its role agreed upon as a non-autonomous Space actor, NATO should primarily focus on arrangements and coordination, defining standards to make national Space data, products, and services available as much as possible. Having capable Responsive Space options that support a resilient Space architecture offers a high level of deterrence that NATO needs to ensure peace and stability for the next seventy years and beyond. ●

1. US Department of Defence, Fact sheet: Resilience of Space Capabilities, 2011, available from: https://archive.defense.gov/home/features/2011/0111_nsss/docs/DoD%20Fact%20Sheet%20-%20Resilience.pdf [accessed 1 Sep. 2020].
2. US Assistant Secretary of Defense, Space Mission Assurance: A Resiliency Taxonomy, Washington DC, Sep. 2015.
3. JAPCC, Resiliency in Space as a combined challenge for NATO (NATO Restricted), Kalkar, Jan. 2021. Available upon request to properly authorized persons. An unclassified version, releasable to the public, will be published later in 2021 and will be available from: www.japcc.org.
4. Space Daily: Rumsfeld Commission warns against "Space Pearl Harbor", 2001, available from: https://www.spacedaily.com/news/bmdo-01b.html [accessed 1 Sep. 2020].
5. European Space Policy Institute (ESPI), Responsive Space for Europe: Elements for a roadmap for Europe based on a comparative analysis with the US Operational Responsive Space Concept, Feb. 2010, available from: https://espi.or.at/publications/espi-public-reports/category/2-public-espi-reports?start=60 [accessed 2 Sep. 2020].
6. US Joint Chiefs of Staff, Joint Publication 3-14, Space Operations, Washington DC, Apr. 2018.
7. US Department of Defense, Defense Space Strategy Summary, Washington DC, June. 2020.
8. Royal Canadian Air Force; Air Space Power in formation: Concept of Operations for the CAF Joint Space Program, Ottawa, May 2020.
9. French Ministry for the Armed Forces; Space Defence Strategy: Report of the Space working group, Paris 2019.
10. Space Strategy of the German Government (2010, New Release 2012); https://www.bmwi.de/Redaktion/DE/Publikationen/Technologie/zukunftsfaehige-deutsche-raumfahrt.html.
11. White Paper on Security Policy and the Future of the Bundeswehr (2016); https://www.bmvg.de/de/themen/weissbuch.
12. Conception of the Bundeswehr (2018); https://www.bmvg.de/de/aktuelles/konzeption-der-bundeswehr-26384.
13. DLR RSC3; https://www.dlr.de/content/de/artikel/news/2020/03/20200902_startschuss-fuer-aerospacepark-am-dlr-trauen.html.
14. UK Government, National Space Security Policy, London, UKSA/13/1292, Apr. 2014.
15. UK Ministry of Defence, Joint Doctrine Publication 0-30: UK Air and space Power (2nd Edition), Shrivenham, Dec. 2017.
16. International Space University, 2009, available from: https://isulibrary.isunet.edu/doc_num.php?explnum_id=83 [accessed 27 Aug. 2020].
17. ESPI Report 22 "Responsive Space for Europe", Feb. 2010.
18. State Council of the People's Republic of China, White Paper on Space activities, 2016, available from: http://english.www.gov.cn/archive/white_paper/2016/12/28/content_281475527159496.htm [Accessed 24 Aug. 2020].
19. Outer Space in this context means the use of near-earth Space in orbits like LEO, MEO, GEO and HEO.
20. State Council Information Office of the People's Republic of China, China's National Defense in the New Era, 2019, translated version available from: https://www.andrewerickson.com/2019/07/full-text-of-defense-white-paper-chinas-national-defense-in-the-new-era-english-chinese-versions/ [accessed 2 Sep. 2020].
21. Russian Federation, approved by the President; Military Doctrine of the Russian Federation, Moscow, Dec. 2014.
22. President of the Russian Federation, Russian federation National Security Strategy", Moscow, Dec. 2015.

Wolfgang Jung

Wolfgang Jung started his career as a Reserve Officer for Tactical Ballistic Missiles (MGM-52 Lance) and holds two diplomas in Aerospace and Space Systems Engineering. In the last 25 years at DLR's Mobile Rocket Base (MORABA), he was responsible for Launch Services and designing new Hypersonic Flight Vehicles. In 2019 he was nominated as DLR's Coordinator for Responsive Space.

At the beginning of this year, he was appointed as the Head of Technology and Department Head for Technology Demonstration at the newly established DLR Responsive Space Cluster Competence Center (RSC3). Besides this, he supports the Air Force Command in Berlin in a Reserve Officer capacity.

Lieutenant Colonel, DipEng, MSc. Tim Vasen

served for several years in command and staff positions within the artillery branch, including a deployment to KFOR as company commander of the GE ISTAR-company before becoming a career intelligence officer. Serving in positions responsible for IMINT planning and technical assessments, including positions at the office of military studies as a senior analyst for Space systems and head of Space intelligence at the German Space Situational Awareness Centre (GSSAC). Since October 2017 he serves as Space Intelligence SME at the JAPCC, e.g. responsible as OPFOR Space planner in TRJN17, TRJE18, TRJU19 and STJUJA20.

Shortfalls in NATO's Space Education

JAPCC's View on Potential Mitigation Methods

By Lieutenant Colonel Tim Vasen, GE AF, JAPCC

Introduction

Space support plays a significant role in today's military operations and governmental decision-making processes. The current technical advantage in Space allows the NATO Alliance to act more precisely, make assessments earlier based on independent data, and maximize the benefits of modern command and control. However, technical developments are ongoing worldwide and it is challenging for Alliance members to maintain their current advantage.

NATO started to incorporate Space professionals into its organization at the beginning of the last decade when initial positions were established inside the NATO Command Structure (NCS). Based on requirements and operational needs, the number of positions has increased over time but the overall number of positions that ensure persistent Space Support in NATO Operations is still limited. In parallel, NATO established the Overarching Space Policy (OSP)[1], which then led to the declaration of Space as an operational domain for NATO.[2] The implementation of the Space

Earth: © Johan Swanepoel/Shutterstock.com; Business Setting: Matej Kastelic/Shutterstock.com domain will trigger follow-on developments that give further advice on how the Space Support structure of NATO has to evolve. This includes the author's opinion on how and where additional Space personnel have to be assigned not only in the NATO Space organization but also in other staff functions such as intelligence, planning, or operations.

All this will lead to a significant demand for Space personnel inside the NCS within the next few years. A similar assessment is likely for the NATO Force Structure (NFS). Even while the number of required personnel has yet to be requested or even agreed upon, there will clearly be an increased demand for Space Education and Training (E&T) within the Alliance. These efforts will be essential to ensure that properly trained and experienced personnel are available to staff the new positions.

Organization of Space Education and Training Today

NATO personnel have to be trained through national courses to ensure they have a comprehensive baseline of Space education before they can be sent to their NATO positions. Only a few Space-faring nations of the Alliance currently offer Space courses and education, and few of these national courses are offered to Allies, as stated in the Discipline Alignment Plan (DAP), which is updated annually.[3] Nevertheless, as a precondition, there usually must be bilateral agreements signed, allowing students of one nation to attend courses in another nation. The management of the Space education in NATO is organized by the Department Head (DH) in close coordination with the Requirement Authority (RA) and the Joint Force Trainer (JFT).[4]

Currently, NATO offers one course at the NATO School Oberammergau called 'Introduction to Space Support for NATO Operations' for entry-level Space professionals and personnel working on Space-related activities as the primary target audience.[5] The overall aim is to give non-Space personnel inside NCS, NFS as well as nations an overview of opportunities and limitations of Space Data, Products, and Services (DPS). Additionally, the NATO process for accessing Space DPS is taught relating to how and where the Space Support Coordinators, who are organizing the Space support coordination process, can be found. This basic course can be seen as a first minor step in individual Space education to train Space personnel to the standard required.

A second course is currently in development and planned to be established in 2021. This 'Space Support Coordinator Course' will focus on personnel filling Space positions, and teaches the specific DPS processes utilized inside the Alliance. In the future, this course may become a mandatory requirement for nationally educated and trained Space personnel to be certified for NATO Space positions.

It is important to understand that the mere completion of these two NATO School Oberammergau courses does not provide the knowledge needed to effectively fill a specific NATO Space position nor does it give the ability to complete all Space-related activities required and requested of the positions. These courses add additional NATO requirements to an already existing national E&T in unity with high skill.

Space Educational Demands for the Future

Analysis of the E&T requirements, the planned increase in the number of Space personnel in NATO, and the associated timeline for filling these positions is needed. This requires an update of all related documents: the Strategic Training Plan (STP), the Training Requirements Analysis (TRA), and the Training Needs Analysis (TNA), by the RA and the DH for Space Support to NATO Operations Discipline.

Additionally, an agreement concerning the required basic education standards is needed to ensure only sufficiently trained personnel are sent to NATO Space positions. Once these standards are agreed upon, they need to be fixed in the job descriptions of the Space-related positions. Establishing standards that incorporate NATO and national courses will provide personnel with the best possible opportunity to be prepared to serve in Space positions inside the Alliance. As the development of Space support also emerges inside the national structures, some non-Space faring nations are currently establishing various national structures and processes, with the eventual goal of being able to contribute to the NATO Space process as well. To avoid excluding any Alliance nation, NATO must find a solution that encompasses at least one national course or a series of courses that can be offered to any ally or groups of allies. To ensure this, bilateral and multilateral agreements have to be assessed and potentially established to give allies a chance to pursue the best educational opportunities. NATO should use this chance to ensure a more federated approach in staffing its Space positions. The inclusion of more willing and interested allies should be the goal, particularly in the long-term in order to enhance NATO's Space capabilities. Conversely, lowering the required educational requirements or allowing insufficiently trained personnel to staff a NATO Space position must be avoided.

With the establishment of Space as an operational domain, personnel dealing with Space-related capabilities must foster connections inside the headquarters. To ensure a broader understanding of the Space domain inside all NATO headquarter staffs, an initiative to apply Space lessons in more E&T opportunities should be started. Especially at the NATO School Oberammergau and potentially other Education and Training Facilities (ETF) such as Centres of Excellence (CoE) that offer courses for disciplines such as intelligence, operations, and planning. Space lessons should be implemented to foster increased understanding and it is imperative for the DH and RA for Space to begin talks with Department Heads of other E&T disciplines while striving to achieve a common understanding and exploit synergies.

Notwithstanding the previously mentioned NATO-owned, NATO-accredited, and national ETFs, it seems appropriate to also assess commercially available E&T opportunities. These can mitigate shortfalls within the major augmentation phase, which can be expected in the mid-term. However, it must be kept in mind that military requirements and needs for the use of Space may not completely align with commercial or civilian courses.

Requirements and Recommendations

Agree on a baseline level of Space E&T to be ensured prior to an individual being sent to a NATO position. Agree on the offered and selected courses (national, NATO ETF and commercial opportunities) that are valid to ensure this kind of education.

Openly discuss and encourage the Space faring nations to offer more courses or make more seats available for allies, to ensure continuity amongst nations and to support NATO's future staffing.

Identify action items the non-Space faring nations have to achieve (e.g. data sharing agreements) to prepare personnel to be sent to national courses and assist the nations to do so. This can be bi- or multilateral, as well as for the whole Alliance.

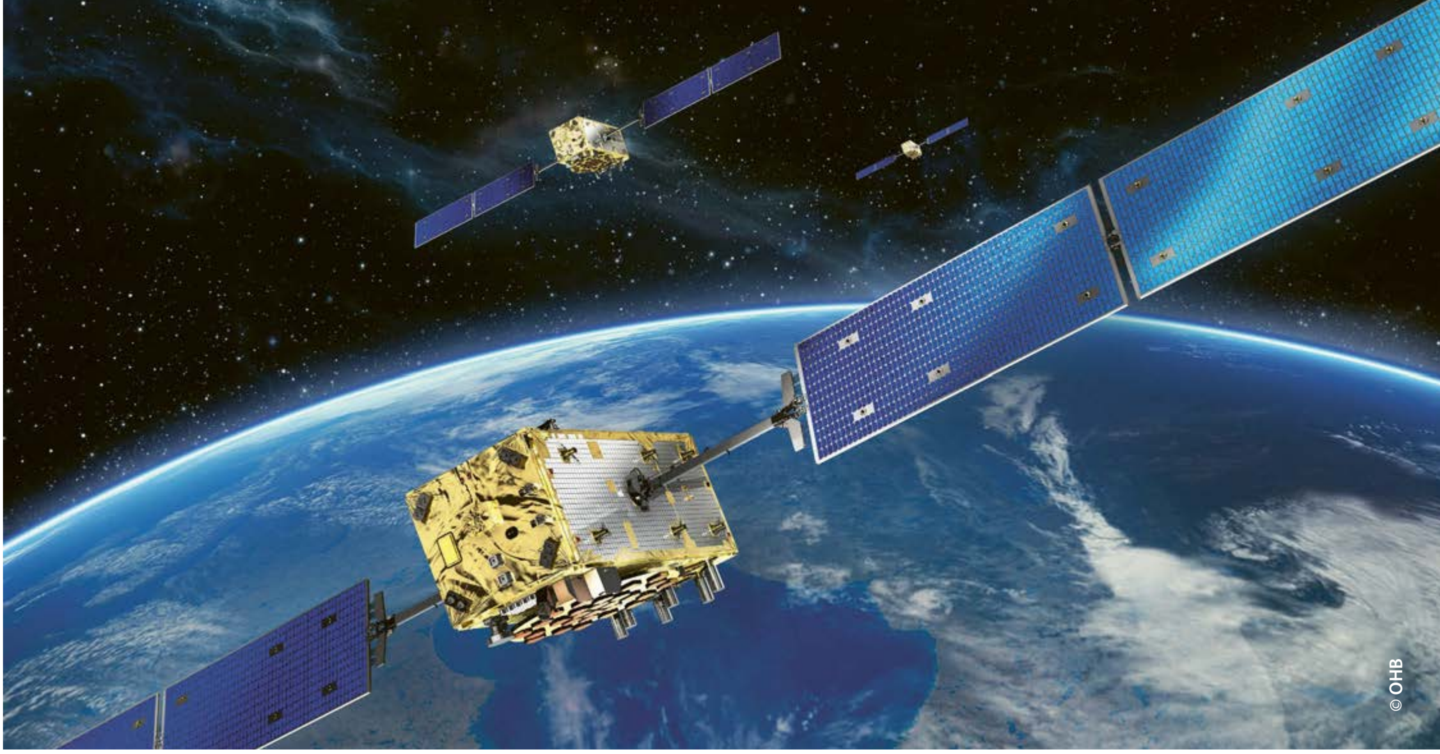
Identify non-Space faring allies who are willing to staff NATO Space positions. Based on this, assess an annual demand for required courses and/or education and training that Space faring nations are requested to provide to allies.

Assess the required number of iterations for the NSO courses (or those provided by other NATO ETFs), based on the personnel augmentation that should be decided within the short to mid-term. This also applies to the Space lessons that have to be integrated into other discipline's courses.

Pass all information on available national Space related E&T opportunities, open or potentially open to member nations and/or for NATO to the DH for Space to increase the number of offers in this domain.

Conclusions

E&T for Space Support in Operations needs to be transformed and adapted to the new status of Space as an operational domain. This requires a significant number of E&T opportunities, both in NATO and within the nations. Therefore, it is necessary to understand how many additional NATO Space personnel



are planned within the NCS and NFS. NATO, with all its ETF's, does not offer baseline E&T to ensure non-Space personnel can be trained while serving in a NATO assignment. The first key elements are national courses offered by Space-faring allies and making these available to the Alliance. ●

1. NATO, 'NATO Defence Ministers approve new space policy, discuss readiness and mission'. Brussels, 2019 [accessed 12 Nov. 2020]. Available from: https://www.nato.int/cps/en/natohq/news_167181.htm; Internet.
2. NATO, 'Foreign Ministers take decisions to adapt NATO, recognize space as an operational domain'. Brussels, 2019 [accessed 12 Nov. 2020]. Available from: https://www.nato.int/cps/en/natohq/news_171028.htm; Internet.
3. NATO ACT, 'Discipline Alignment Plan (DAP) for the Space Support in Operations discipline' (2019).
4. Console, A. and Grest, H., 'Managing Space Education and Training in NATO', JAPCC Journal Edition 23 (2016), p. 38–44.
5. NATO ACT, 'NATO Electronic Education and Training Opportunities Catalogue (ETOC)', (online) Norfolk: NATO Allied Command Transformation [accessed 14 Aug. 2020]. Available from: https://e-itep.act.nato.int/Guest/ETOCindex.aspx?sEncCrit=KTfmWLxPHci%2BxBaQEhKu2jFxxoJ67NQZ2FdWv%2FF3Y54W%2B9LqrZq9J2nt1PiLEYlsqXprdug2U2eNetZF%2FSWDQViaaH9Rsxd89XxanwjbZGNgZGEm%2BFk5BQJBBq7KIUXTbzcBLvJKzniEloCqYoFcGPYrkq3xCCiANiXvwORLsnjeKrzcVEpR%2BAm4TCz30Xk5KdESLzKYPE7rW9istSTbjg%2Bbe1C35u6UmAC%2FNn%2FCenk1Vb8bRKjIPP4trTespp%2BIg4YbMNOwhps8XVfYrPIGAPAUzxuEC%2BygiqMGMcOT15T5%2BU5PJh8DWs4o84E88iI0bSdoKQLs84Y8CHR6i%2BGIGw%3D%3D; Internet.

Requirement Authority (RA) (SHAPE)
is responsible for the identification of individual and collective E&T requirements.

Department Head (DH) (JAPCC)
identifies and coordinates effective, efficient and affordable E&T solutions.

SACT Joint Force Trainer (JFT)
is responsible for direction of the whole E&T spectrum and coordination between the disciplines within one discipline.

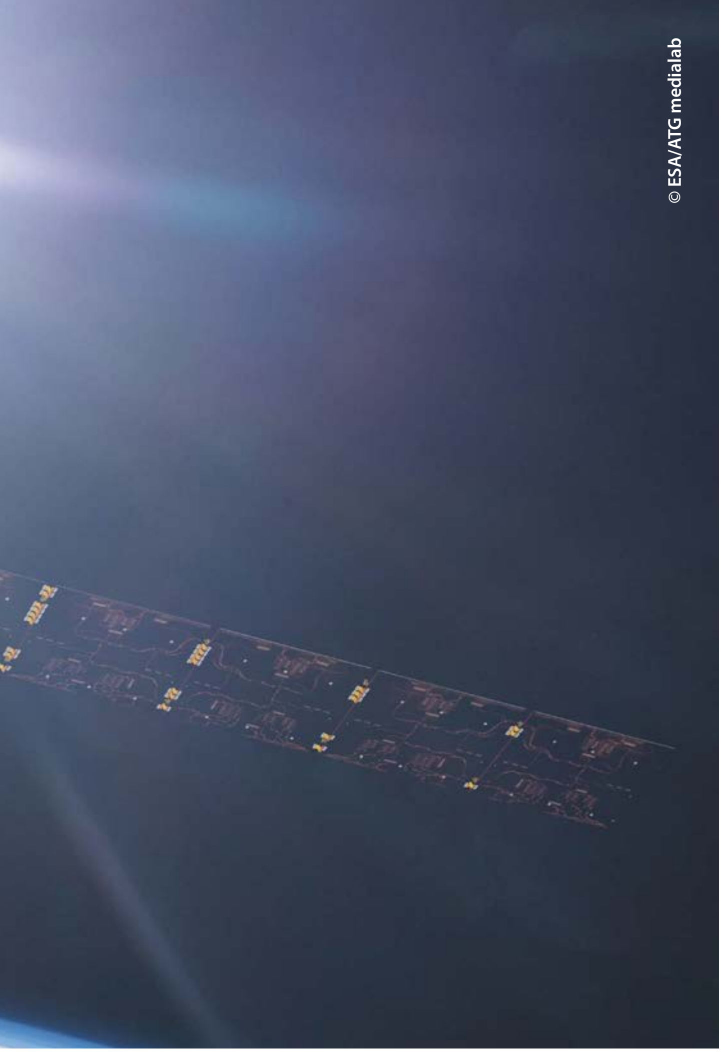
Lieutenant Colonel, DipEng, MSc. Tim Vasen
served for several years in command and staff positions within the artillery branch, including a deployment to KFOR as company commander of the GE ISTAR-company before becoming a career intelligence officer. Serving in positions responsible for IMINT planning and technical assessments, including positions at the office of military studies as a senior analyst for Space systems and head of Space intelligence at the German Space Situational Awareness Centre (GSSAC). Since October 2017 he serves as Space Intelligence SME at the JAPCC e.g. responsible as OPFOR Space planner in TRJN17, TRJE18, TRJU19 and STJUJA20.

Exploring Synergistic Potential of the Portuguese Space Strategy

By Major Augusto Figueiredo, PO AF, DACCC

Introduction

Space is critical for societal activities and military operations. Inferring from this axiom one can state that ceasing access to space and space data will severely disrupt normality. This highlights the importance of the subject and identifies the need for coherent, thoroughly reasoned and oriented action. Portugal has done just that by constructing a National Space Strategy (NSS), known as 'Portugal Space 2030', setting in the form of governmental resolution the ambition, vision and goals for the space sector for the next ten years, leading inter-ministerial efforts towards economic development, job growth and innovation in this area. At a time characterized by the advent of the New Space industry, the very own concepts of Security and Defence evolve when confronted with boundless threats and uncertain risks, with the potential to impact every sector of society, thus requiring a well synchronized whole-of-government approach to tackle this challenge. One of the required steps to achieve this desideratum is the establishment of a more security-oriented complement to the overarching NSS, more specifically in the form of a National Defence guidance. This article intends to provide insights on what the end-state should be and how to pursue it, following the vision of a well-integrated action from civil, commercial and security space participants, reminiscent of a truly symbiotic interaction.



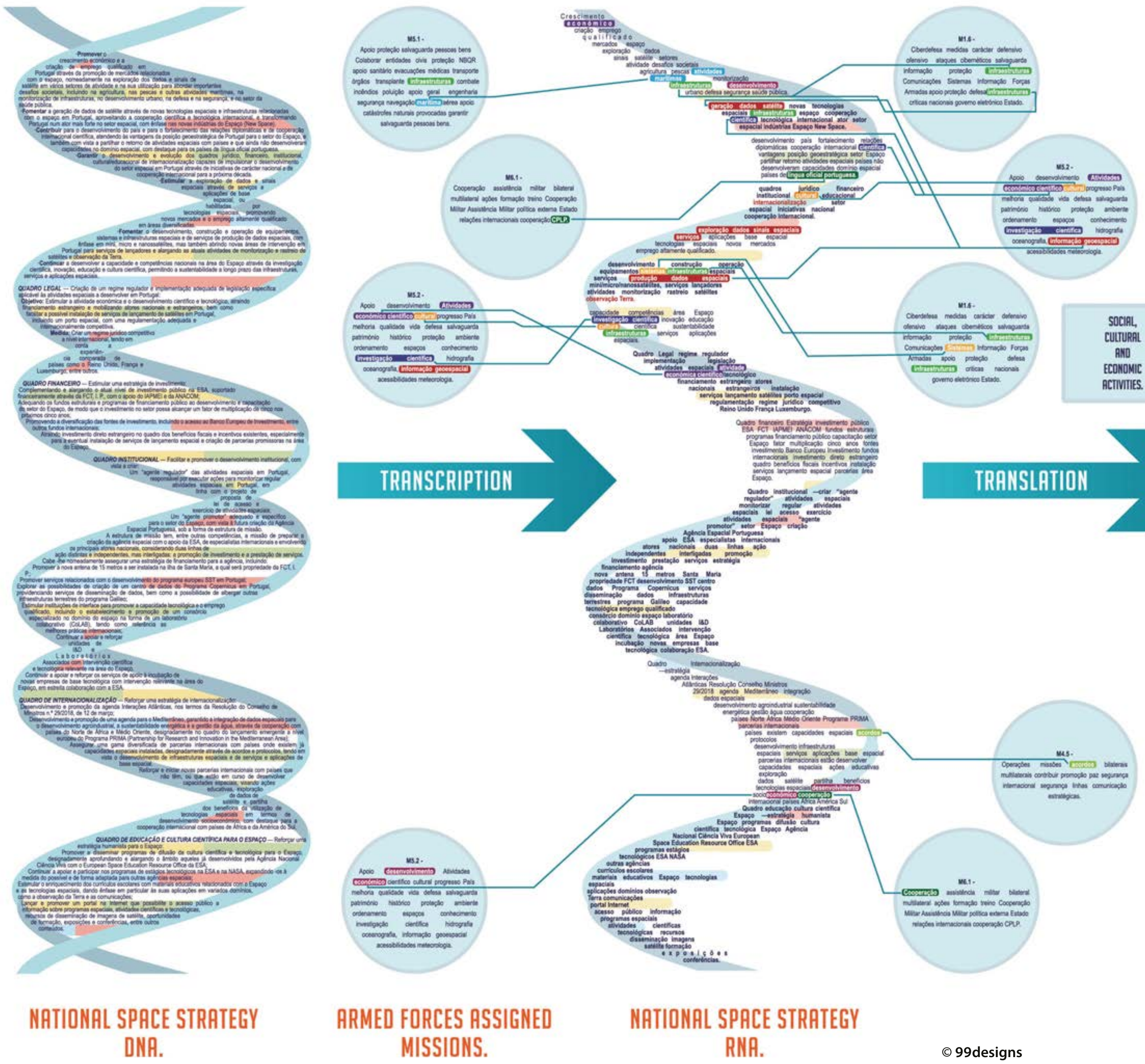
Proposed End-State

Building on the understanding that strategy 'provides direction for the state, seeking to maximize positive outcomes and minimize negative outcomes, as the state moves through a complex and rapidly changing environment into the future'[1] hints that the strategic space environment, seen as competitive, congested and contested, is leading the need to shape the future to meet National Interests. As the desired end-state clearly defined on the NSS is focused mainly on the economic development of the space sector, the reliance on space for military operations and emergency response structures, call for a security-oriented end-state. Beyond this vulnerable reliance, the official recognition of space as an operational domain represents an added responsibility for NATO members to contribute for the overall effort that intertwines the Alliance resolve. Surmounting this political-military commitment, the competition continuum multiplied by the fast-paced technological development has driven an aspiration to effectively harness a Joint All Domain concept of operations, where flawlessly synchronized effects are attained across domains regardless of traditional Service or Branch expertise. This duality of necessities, both in military diplomacy and operational requirements, emerge from a threat analysis where state and non-state actors reveal growing capability on the counter space continuum.[2] Deriving from this context, and to properly balance ways and means, a generic end-state, to be pursued by the National Defence Space effort, is proposed: ensure continuous access to space and space-generated data to permanently support combat operations, emergency situations and peacetime mission requirements, across the entire Area of National Strategic Interest, based on a resilient, redundant, regenerative and connectable space infrastructure.

Baseline Research

The research on NSS and the Portuguese Armed Forces[3] started by analysing the strategic space process of the United States of America and the United Kingdom (UK), to realize that, in both cases, it is composed by several documents that follow a hierarchical, well-defined and complementary logic between participants from the civil, commercial and security space sectors, harmonizing efforts around the National Interests in the space domain. Interestingly, the analysis of the UK process, where space has been designated a Critical National Infrastructure, pointed out the close link between space and cyberspace domains, in both the organizational steps followed to build new-domain capabilities and the technological interdependency.[4] After the analysis of the strategic framework in both case studies, the research proceeded to identify the existing connections to the armed forces by referring to the fundamental concepts military, armed forces and joint force found within the documents of reference on space-related context. This layer pointed out elements such as vulnerability, assets, reliance, human resources, cooperation, resiliency and degraded operational environment, fitting in the structural, operational and genetic aspects of strategy.

The next research step was to adopt the same approach to the incipient Portuguese space strategic process. Parsing through the NSS and the Portuguese Space Agency Business and Installation Plan, the only existing sources available for analysis, leads to the conclusion that none of the key concepts were present at all. Such findings warranted a different approach, one that could assess the compatibility between the NSS and the armed forces. To accomplish that, an analogy to the molecular biology processes of transcription[5] and translation[6] was sought and applied in practical terms to the text processing of the NSS and the Portuguese Armed Forces Mission Statement, constructing the ideation of, based on the interlinked concepts, the current definition of what the armed forces execute can potentially produce an outcome embedded in the NSS, labelled synergistic potential. This abstract conceptualization is captured in Figure 1.



Synergistic Potential

Picking up on the synergistic potential identified at the fundamental levels of both the NSS and the Armed Forces Mission Statement, the following discussion aims at turning the abstract exercise into tangible, realistic terms by highlighting some of the current initiatives and projects that could be leveraged by Defence, while bringing benefits in the form of capability. This is not meant to be an all-encompassing list but rather a starting point to build from and simultaneously address the technological challenges that will define future space developments.

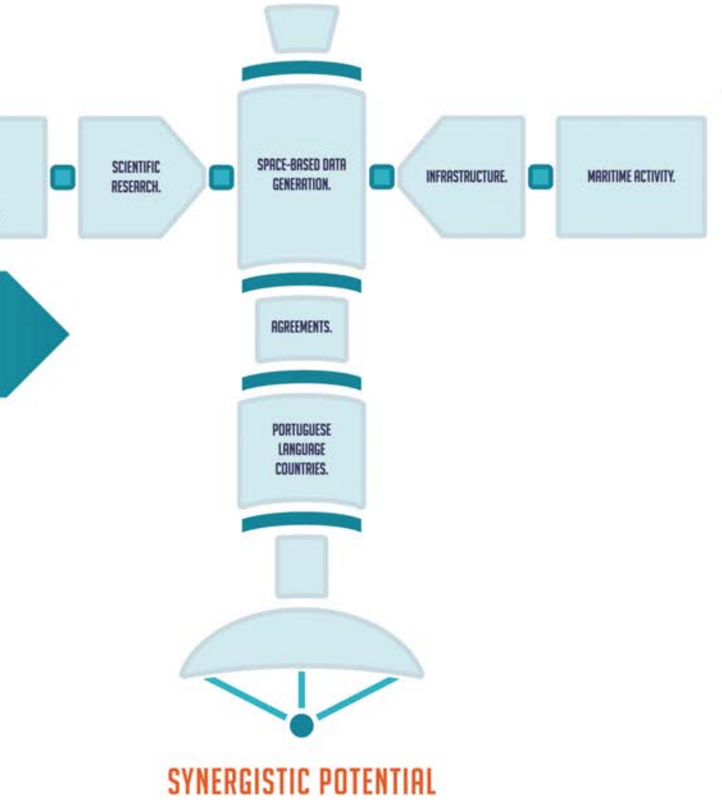


Figure 1: Synergistic Potential between the NSS and the Portuguese Armed Forces (Design by Alex Curiel)

Infrastructure

One of the flagship projects of the Portuguese Space endeavour is the Atlantic International Satellite Launch Programme, with the objective of designing, installing and operating a spaceport on the island of Santa Maria, in the Azores. The goal of this initiative is to start sustainable small-satellite launch services by 2021, taking advantage of the privileged location of the Azores to explore unobstructed, over the water, launch trajectories for Low Earth Orbits (LEO), specifically Polar Orbits and Sun-Synchronous Orbits (SSO). This type of facility can ensure continuous access to Space and incorporate the concept of Operational Response Launch[7], with high-readiness times focused mainly on Intelligence, Surveillance, and Reconnaissance satellites carrying tailored sensor payloads, contributing to the redundant and regenerative aspects of the integrated space infrastructure.

Agreements

The establishment of agreements on a space context has been conducted separately by Defence and civil entities, mainly through the Ministry of Defence and the Portuguese Space Agency. But why not merge and broaden the spectrum of activities, designed jointly from the start? This approach will allow a comprehensive understanding and creation of expertise in this field – a necessary condition to navigate the range of European mechanisms and programs[8] available, reinforcing the Portuguese Space contributions through internal cooperation.

Maritime Activity

With the long-awaited extension of the Continental Shelf[9], Portugal will have increased responsibility for a substantial part of the Atlantic. This challenge requires extended range and depth for current Defence activities, calling for new ways to monitor surface and subsurface persistently. This might be achieved by fusing data from Manned-Unmanned Teamed Systems, both aerial and maritime, connected by a space structure that enables a timely decision-making process.

This requisite demands higher bandwidth availability from communication satellites, a quest that might be revolutionized by photonic-aided receiver payload on phased array antennas, implementing optical beam-forming networks.[10]

Development of Social, Cultural and Economic Activities

Artificial Intelligence (AI) Moonshot is an ongoing open-challenge that invites everyone to create solutions to identify and track Ocean plastic through the use of AI. This approach to deal with an increasing Environmental issue, resembling the successful Defense Advanced Research Projects Agency Grand Challenge format, has the potential to bring together highly qualified participants with diversified backgrounds, voluntarily working on complex problems that often result in disruptive concepts. Beyond this creative ensemble, the format fosters a community that will stay connected in intensive social dynamic, with the potential to influence cultural evolution and opening new economic activities, as it happened with Autonomous Driving.[11] This might be the most intangible benefit, but potentially, the most impactful, not only at a technological level where AI will play a role in several levels, such as payload and orbit optimization but also at a moment when the armed forces struggle with recruitment and retention issues, appealing to a young space generation seems a valid option.

Scientific Research

The technological space evolution has been powered by scientific research and will continue to require scientific breakthroughs to progress. The armed forces, mainly through the Service Academies' research programs, have the necessary conditions to contribute actively in this field. For this purpose, two vectors must be aligned. First, setting guidance for research development focused on (1) payload technology that supports military activities, such as electro-optical, Synthetic Aperture Radar and Signals sensors; (2) satellite communication technology, looking at the integration with the 5G ecosystem and the required Software Defined Networking and Functions Virtualization architecture that will enable the use of space as a backhaul for 5G[12]; and (3) encryption, mainly through the development of Quantum Key Distribution protocols that will define secure communications standards in the near future.[13] Secondly, by educating Defence personnel in this subject, becoming familiar with concepts and language that allow cooperation with civil and commercial partners for quick and effective technology transfer, similarly to the approach established in the International Space University.[14]

Space-based Data Generation

Defence is leading the national participation on the European Union Space Surveillance and Tracking programme that will soon have sensors and an operations centre implemented at the islands of Madeira and the Azores. This capability will undoubtedly contribute to an increased Space Situational Awareness and also increment Space Safety. But it must not stop here. This initiative can be the ground segment starting point for a more ambitious commitment with the development of an orbital segment that allows the generation of data, essential for several other mission areas such as Space Weather, Space Traffic Management and Shared Early Warning. It is crucial that the initial infrastructure design accounts for connectivity with other partners and also future growth potential.

Portuguese Language Countries

Portugal holds a historical, cultural and emotional link with all the Portuguese language speaking countries, a heritage that has evolved along the centuries and manifests across society. One of the strongest bonds has been guarded by the military institutions from all the countries, formally represented in the Community of Portuguese Language Countries, and becomes visible through permanent staff, operational and academic exchanges, and technical military cooperation. Using this established and trustworthy framework might very well be the most effective way to increase the development of the space sector within a very relevant and broad community, whose member states span the entire Atlantic.

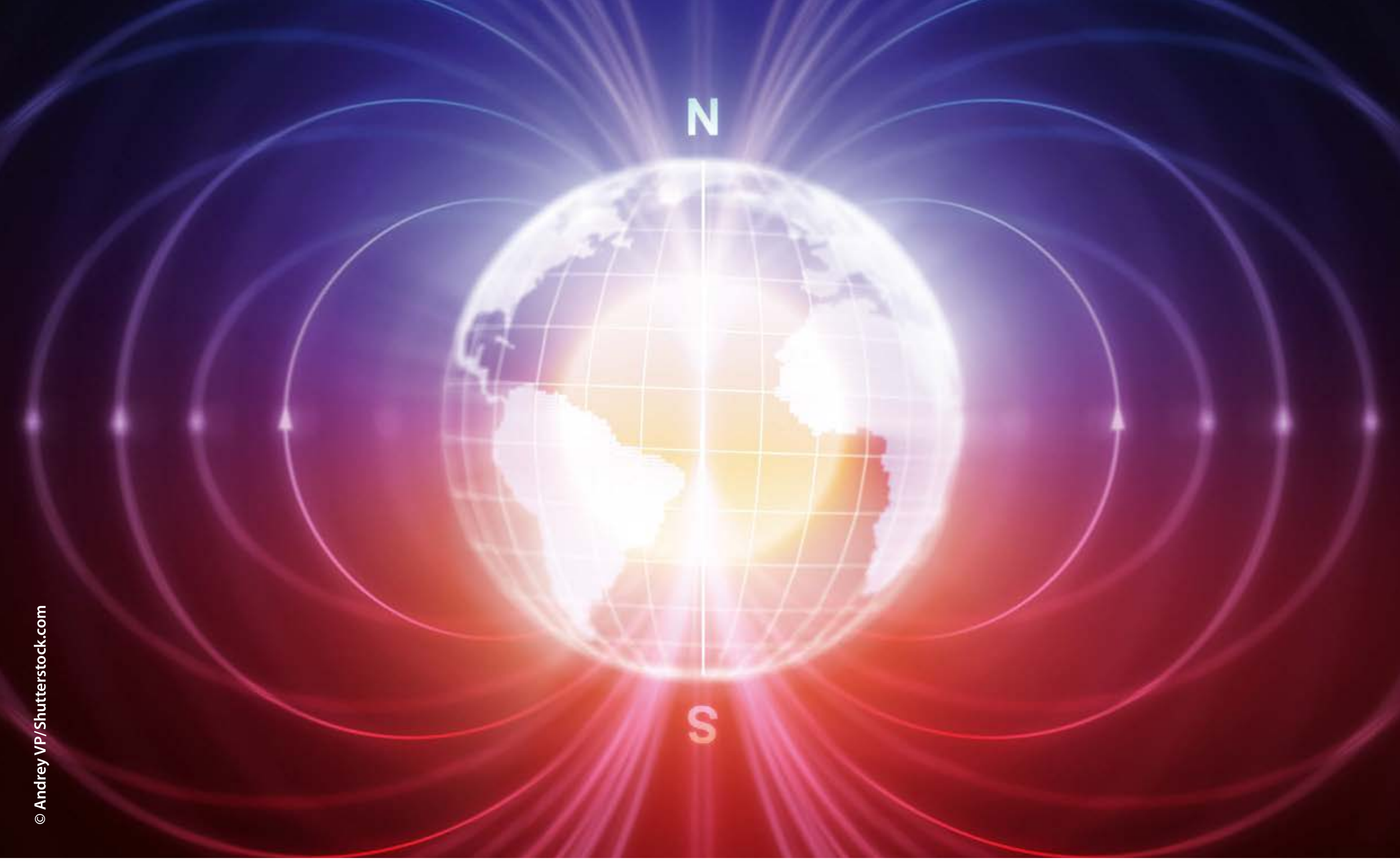
Conclusion

The necessity to benefit society from space, where Defence activities are paramount to provide Security, is uncontested. The vision discussed demonstrates the potential to align Defence efforts to the overarching NSS and avoid excessive branching or duplication of resources. From a wide range of opportunities, it ought to be in synchrony with the overall end-state implicit on the NSS that Defence must act as a catalyst agent. This posture observes the principle of complementarity, contributing actively towards the achievement of the National global objectives, by aligning the compatible/common categories and realizing synergies from that connection. It does not mean pursuing the same outcomes: it translates into coupling technological and organizational assets when required to establish Defence Space capability to support combat operations, emergency situations and peacetime mission requirements, but seeking alternatives means when dual-use is not feasible. A critical key to success in this regard, adding up to the required financial investments, is the need for skilled human resources able to bridge across all space sector participants, creating solutions for the non-linear problems presented on this uncharted system, supported by leadership with enough organizational backpedal to accept risk and learn from failure.[15]

1. Yarger, H. R. Strategic Theory for the 21^{st} Century: The little book on big strategy, US Army Strategic Studies Institute, 2006.
2. Defense Intelligence Agency, Challenges to Security in Space 2019, https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf.
3. Figueiredo, A. F. A Estratégia Nacional para o Espaço e as Forças Armadas Portuguesas. Instituto Universitário Militar: Lisboa: 2019. https://comum.rcaap.pt/bitstream/10400.26/30046/1/TII%20CAP%20AUGUSTO%20FIGUEIREDO.pdf.
4. Stickings. A. Is Space the New Cyber? UK Dependencies and Vulnerabilities. Royal United Services Institute Conference Report, https://rusi.org/sites/default/files/20190313_space_conference_2019_report_web.pdf.
5. The process by which an RNA copy of a gene is made (Allison, 2007, p. 707).
6. The process by which ribosomes decode an RNA message (mRNA) to synthesize a protein (Allison, 2007, p.707).
7. Vasen. T. 'Responsive Launch of ISR Satellites. A Key Element of Space Resilience?', JAPCC Journal, no. 27 (2018): p.17–21.
8. European Space Policy Institute. 'ESPI Report 72 – Europe, Space and Defence – Full Report', https://espi.or.at/news/new-espi-report-europe-space-and-defence.
9. https://en.emepc.pt/.
10. Duarte, V. C. et al. Modular coherent photonic-aided payload receiver for communications satellites, https://www.nature.com/articles/s41467-019-10077-4.
11. Defense Advanced Research Programs Agency, The Grand Challenge, https://www.darpa.mil/about-us/timeline/-grand-challenge-for-autonomous-vehicles.
12. Boero, L. et al. Satellite Networking Integration in the 5G Ecosystem: Research Trends and Open Challenges, https://ieeexplore.ieee.org/document/8473415.
13. Kerstel, E. et al. Nanobob: a CubeSat mission concept for quantum communication experiments in an uplink configuration, https://link.springer.com/article/10.1140/epjqt/s40507-018-0070-7.
14. International Space University, https://www.isunet.edu/.
15. Bryant, S. F. & Harrison, A. Finding Ender: Exploring the Intersections of Creativity, Innovation, and Talent Management in the U.S. Armed Forces. Institute for National Strategic Studies, https://inss.ndu.edu/Portals/82/Documents/Strategic%20Perspectives/SP%2031%20Bryant-Harrison%20FINAL%20for%20Web.pdf?ver=2019-05-21-111752-910.

Major Augusto 'PRIME' Figueiredo

Joined the Portuguese Air Force Academy in 2003 and completed his pilot training in Columbus Air Force Base, USA, in 2009. Shortly after was assigned to Monte Real Air Base, Portugal, to fly the F-16OCU. Throughout his carrier has participated in several missions and international exercises, such as the Icelandic Air Policing, Baltic Air Policing and Assurance Measures. Graduated from the Tactical Leadership Program, Spain, in 2014. In the recent years has taken part on the flight test and development campaign of the Automated Air-to-Air Refuelling (A3R) System developed by Airbus. In June 2020 transitioned from being an F-16 MLU Instructor Pilot and Head of the Air Base Safety Office to become a Staff Officer at the NATO Deployable Air Command and Control Centre (DACCC), Italy.



© Andrey VP/Shutterstock.com

Electromagnetic Operations in 'Grey Zone' Conflicts

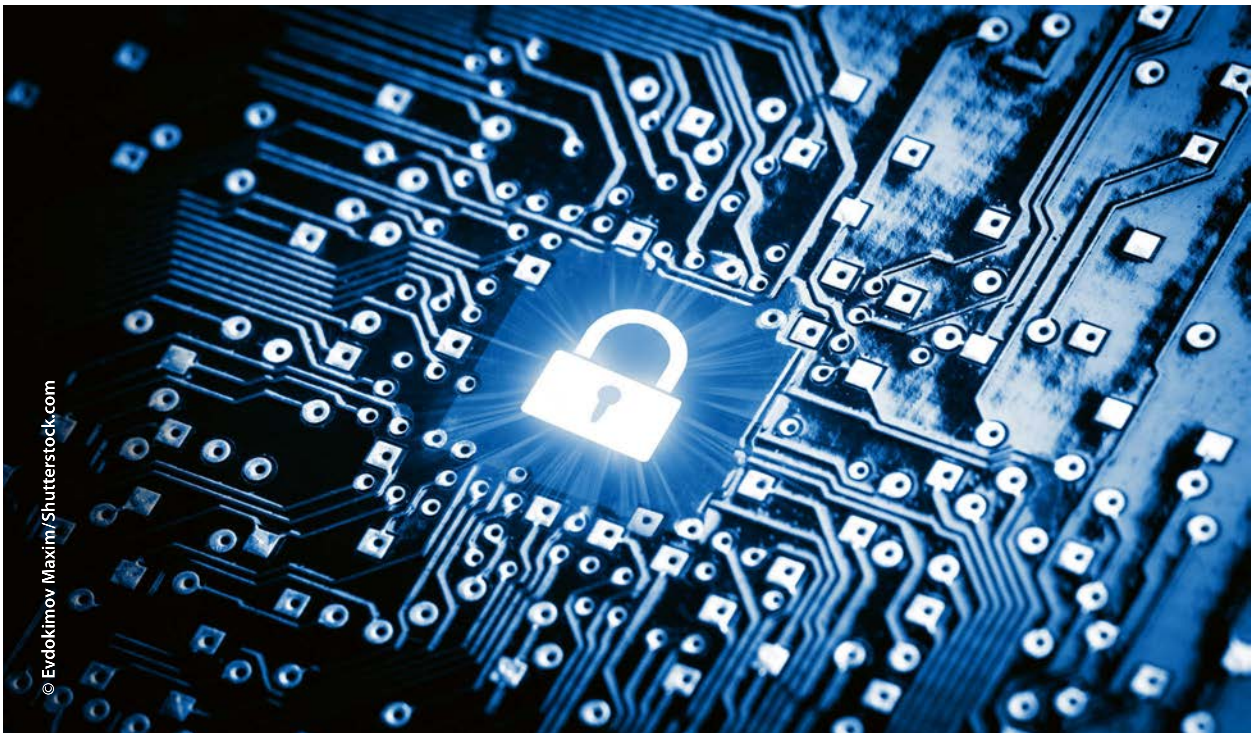
The Tool of Revisionist Countries to Confront the International Order

By Commander Ignacio Nieto, SP N, Spanish Joint Command

Introduction

The Future Security Environment will be dynamic and ambiguous, as well as increasingly complex and uncertain[1]. Evidence of this assertion are the recent conflicts in Crimea and Donbass area in eastern Ukraine. Both depict a whole new challenge; an undeclared form of warfare. These actions, carried out by the Russian Federation, with a clear revisionist approach, have been labelled in some western scholars' forums as a 'grey zone' conflict.

Great Powers[2] seek to revise the order of alliances and also solidify new norms of conduct within the globe. In doing so, some of the Great Powers, specifically the revisionists, can exploit 'grey zone' tactics to achieve their political objectives. 'Grey zone' tactics avoid providing Western countries[3] with sufficient rationale to carry out military intervention in support of their allies. Russia knows that the balance of power is favourable to the status quo since the United States (US) supremacy within conventional military conflict remains unsurpassed. This fact makes


© Evdokimov Maxim/Shutterstock.com

them move toward the 'grey zone' strategies while preparing for war. Eventually, the goal they are pursuing is changing the international distribution of power and influence.

Defining the 'Grey Zone'

'The grey zone is an operational space between peace and war, involving coercive actions to change the status quo below a threshold that, in most cases, would prompt a conventional military response, often by blurring the line between military and non-military actions and the attribution for events.'[4]

In short, the actions taken by the adversary do not clearly cross the threshold of war. These processes are probably attributed to three main reasons; the first one is the ambiguity of international law, the second one is the lack of attribution; and finally, the impact of the activities does not justify an overt military response. These three leading causes will guide the choice for specific actions.

'EMO might be the key element for any future conflict …'

'Grey zone' conflicts have four characteristics[5] 'pursuing political objectives through cohesive and integrated campaigns, employ non-military tools, striving to remain under key escalatory thresholds to avoid outright conventional conflict and lastly moving gradually towards its objectives'.

One of the main points to be considered is that the Tactics, Techniques and Procedures in a 'grey zone' of conflict offer a showcase to others, in particular non-state actors or even nations that are not so militarily strong. They do not necessarily represent a risk for the international order. Still, they can use the 'grey zone' strategy or tactics to achieve their political goals since they are primarily based on low-cost Commercial-Off-The-Shelf (COTS) technology. Consequently, near-peer to NATO competitors such as Russia and China have the ability to conduct an uncoordinated war by proxy in support of fulfilling their goals against small NATO nations and partners.

International Order at Risk

The international order has been organized around economic freedom, multilateral institutions, security cooperation and democratic solidarity. The foundation of international security was and continues to be, based on a cooperation of nations (not restricted to military actions) under the leadership of the United States. Current transatlantic frictions may lead one to think that this order is in crisis due to the lack of strength of the past liberal internationalism.

Even though the backbone of Europe's security system was based on the NATO organizational structure, today this structure is at risk, since there is an evident lack of leadership and commitment of the lead nation hegemon. Potential adversaries are aware of that and are likely to wield 'grey zone' tactics to undermine Europe's security system. The potential for 'grey zone' progress relies on the degree to which the intended targets can respond in kind.

Actions taken by a 'grey actor' may convey an immediate impression of a non-winning scenario within the political sphere, contributing to the perception that they will never achieve a decisive objective in a relatively short period. Western nations are fearful of protracted conflicts, regardless of whether the conflict is violent or not. Moreover, in the 'grey zone' scenarios, the political level is fully aware of the severe constraints it has on actions when it comes to the use of force or the set of tools they need to employ to respond to any threat. It is not only restrictions to the use of military power in response to a threat, but having the political will to use it.

The inability of western nations to respond in kind to a 'grey threat' leads to this type of action becoming the norm and promotes a lack of international order. Any inaction by nations, whether due to embarrassment, lack of awareness, or lack of political will, is seen as a sign of weakness, which promotes and emboldens actors to continue with a 'grey zone' attrition strategy.

© DARPA

No single scenario is similar to that of another, every environment is markedly unique, ensuing that both strategy and response demand a tailored approach. The strategy to implement a response must be a living document that keeps pace with new adversaries' approaches following on the principle that the reality goes beyond any single prediction.

Electromagnetic Operations

It could be argued that Russia's strategy shifted from traditional military capabilities towards non-military means of fighting, which is not true. Russia's strategy consists of having the military in a supporting, not supported role at first. It is a matter of gaining influence with one means and at the same time, improving military capabilities.

The NATO agreed Term for Electromagnetic Operations (EMO) is 'All operations that shape or exploit the Electromagnetic Environment (EME) or use it for attack or defence including the use of the EME to support operations in all other operational environments.' In this vein, NATO countries have agreed to define EME as 'All of the electromagnetic phenomena occurring in a given place. In summary, the use of the electromagnetic energy to achieve offensive and defensive effects.'[6]

Strategies that fall under the umbrella of EMO are normally outside the purview of international laws and norms. These strategies are usually non-attributable and best suit the 'grey zone' concept since they remain below the threshold of western countries' armed reactions. NATO's increased reliance on wireless Command and Control and connectivity has created a vulnerability that is also being exploited within the Electromagnetic Spectrum (EMS), which is what makes these strategies so dangerous.

'Grey zone' strategies use both the coercion itself and the risk of escalation as a source of leverage. An EMO toolbox can shape the decision-making leadership to convince them not only to de-escalate, but also not to intervene at all. The challenge of responding to EMO aggression is further complicated by the lack of will from NATO countries to respond, which may expose their own EME for security purposes.

EMO tactics are part of the coercive threat. For instance, Russia's deterrence strategy aims to persuade Westerners not to act against them.

The EMO in Support of 'Grey Zone' Strategies

Without any doubt, one country annexing another country might have seemed highly unlikely some years ago. However, the Ukraine crisis was an eye-watering showcase of 'grey zone' activity and has paved the way for another entirely different approach in one's arsenal to achieve political goals. Once Crimea was invaded, Russian forces built up, along with a different array of military or non-military measures, and a complete strategy aim to achieve not only a contested, but also disrupted and denied EME. The Russian annexation of Crimea was a major surprise for the entire western world[7].

Russia seeks to master Global Navigation Satellite System (GNSS) denial techniques and dominate Positioning, Navigation and Timing (PNT) environments. It is a matter of the utmost importance in terms of international relations and for national security. The potential loss of money due to GNSS disruption has been laid out by the United Kingdom in a recent report of the London Economic.[8] Likewise, deliberate GNSS disruption has pan-global impacts that could affect all economies. Both the European Union (EU) and NATO are unlikely to be able to compel Russia to stop jamming the GNSS signals. Furthermore, international law will not support any aggressive line of action, taking into account the lack of attribution of this setback. This must be considered by any nation when it comes to a conventional response. The EMO effects could involve political and economic coercion, and will be in the foreground of any decision-making at the political level.

Military forces in this environment will commonly have their communications disabled due to jamming techniques and also have their frequencies intercepted. The smartphones are tapped, and families may receive threatening messages through social networks. Allied soldiers have also received messaging inviting them to surrender.

Lieutenant General Ben Hodges, former commanding general of the US Army Europe, remarked in 2016 'the capabilities we've seen the Russians display in Crimea – EW capability at a tactical level [is something] that we absolutely don't have.'[9] More recently, the head of US Special Operations Command, General Raymond Thomas declared Syria 'the most aggressive EW environment on the planet from our adversaries. They are testing us every day …'[10]

When military experts are called to advise the political sphere about a single military response option, the political appetite vanishes into the haze. Based on their assessment and advice, military experts keep the Salamanca School[11] core principles in their minds. Notably, when they consider whether there are conditions enough for victory in this scenario, it is difficult to assess and balance the chance of a military success against the potential costs and losses, which may not be favourable.

Hence, the EMO provides in some sense a shield from any military intervention. This environment prevents NATO countries from taking any military action since the result is not easy to predict. Western countries have a low tolerance for risk, which proves the efficiency of EMO in 'grey zone' strategies.

NATO is turning the tide and developing actions to ensure EMS superiority across the entire range of military operations. The recent NATO EMS strategy bridges the near, medium and long-term strategic approach and aligns ends, ways and means of the Alliance toward paving the way for fighting in the 'grey zone' scenarios.[12]

Conclusion

EMO might be the key element for any future conflict, in particular among near-peer competitors, whereas our adversaries place a growing emphasis on developing these capabilities, and they recognize this to be a terrific cost-effective solution. NATO military leaders and planners must understand all threats in a conflict environment to be able to effectively operate with a significant electronic warfare threat.

EMO has become an integral part of Russia's modern warfare doctrine. This question is of great importance since other countries, with forces less capable than Russia's forces, are *'learning by watching'* and can apply the same strategies in our neighbourhood. Russia has implemented a new strategy by challenging the sovereign EMS of neighbouring states, including NATO nations. Russia's political acceptance for military actions against sovereign territories (EMS included) to create leverage makes future manoeuvres, warnings and indicators harder to identify and understand.

Western scholars should focus on ways to combat the individual elements of hybrid warfare, and foster debate about what actions Russia is likely to take next in the 'grey zone' in their quest to once again become a Great Power. They also need to acknowledge that EMO have a vital role to play in the Russian revisionist approach. NATO has already stepped forward and regained the initiative in this regard with a variety of tools and instruments, including a new EMS strategy that will make the Alliance capable of conducting an appropriate fight in the 'grey zone' to keep the international order alive.

1. NATO Allied Command Transformation, Framework for Future Alliance Operations 2018, https://www.act.nato.int/images/stories/media/doclibrary/180514_ffao18-txt.pdf.
2. For the purpose of this article, Great Power is a sovereign state that is recognized as having the ability and expertise to exert its influence on a global scale.
3. Western countries were somehow the sponsors and protector 'security community' built up around the liberal order and under the leadership of the United States.
4. Morris, L., Mazarr, M., Hornung, J., Pezard, S., Kepe, M. (2019). Gaining Competitive Advantage in the Gray Zone. RAND Corporation.
5. Mazarr, Michael J. (2015). Mastering the Gray Zone: understanding a changing era of conflict. US Army War College.
6. NATOTerm is the official NATO Terminology Database, https://nso.nato.int/natoterm/content/nato/pages/home.html?lg=en.
7. Sandor, Fabian (2019). The Russian hybrid warfare strategy – neither Russian nor strategy. Defense & Security Analysis.
8. Sadler, G., Flytkjær, R., Sabri, F., Herr, D., 'the economic impact on the UK of a disruption of the GNSS'. In LE London Economic. Available from UK Gov., https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/619544/17.3254_Economic_impact_to_UK_of_a_disruption_to_GNSS_-_Full_Report.pdf.
9. Pomerleau, Mark (2018). Threat from Russian UAV jamming real, officials say, https://www.c4isrnet.com/unmanned/uas/2016/12/20/threat-from-russian-uav-jamming-real-officials-say/.
10. Clark, Collin (2018). Russia Widens EW War, 'Disabling' EC-130s OR AC-130s In Syria. Breaking Defence, https://breakingdefense.com/2018/04/russia-widens-ew-war-disabling-ec-130s-in-syria/.
11. The School of Salamanca is the Renaissance of thought in diverse intellectual areas by Spanish theologians, rooted in the intellectual and pedagogical work of Francisco de Vitoria. They laid the foundations of the just war.
12. Recently, the lines of actions to be taken once the strategy is up and running were discussed during the 107 plenary meeting of the NATO EW Advisory Committee (NEWAC).

Commander Ignacio Nieto

joined the Navy in 1989 and trained to become an Electronic Warfare specialist. After having served years in several EW postings he joined the Spanish SIGINT community posted either on board a SIGINT vessel or as an expert within the Naval Headquarters. In 2016 he joined the NATO SCHOOL, Oberammergau as the EW/SIGINT Subject Matter Expert (SME) both acting as such and as the course director of several courses, such as the Electromagnetic Operations Course, Joint EW Course or Suppression of Enemy Air Defences (SEAD) Course. Nowadays he is the head of the Electromagnetic Battlestaff Center in the Joint Operations Command in Spain.

© Aeronautica Militare

Italian Bio-transport During COVID-19

Blueprint for the Alliance – How the Italian Air Force Managed Bio-transport During the Pandemic

By Lieutenant General Domenico Abbenante, IT AF, Head of the Air Force Military Health Corps
By Captain Massimo Di Milia, IT AF, JAPCC

Introduction

The Italian Air Force (ITAF) contributes to the Ministry of Defence Coronavirus DISEASE 2019 (COVID-19) pandemic plan of action with various capabilities and structures. A key example of this is the implementation of the Bio-containment team of the Pratica di Mare main infirmary, composed of doctors and nurses specialized in air transport of infectious patients. This is a unique capability of the ITAF and fundamentally important in this emergency scenario, being ideal for quickly and safely transferring infectious patients from one hospital to another. In providing this service, it gives remarkable support to the treatment centres in northern Italy, one of the areas most affected by the pandemic. The ITAF's experience with Bio-transport, coupled with the lessons learned from the COVID-19 pandemic, highlight the NATO Alliance's need for this capability and provides key lessons for the future.

Biological Challenges

Viruses, bacteria and fungi are studied because they represent a critical issue in the multinational collective defence system. When considering Bio-containment, one must regard every single bacterium or virus as having an operational potency that is superior to the best weapon system. The presence of just a few cases of an illness that could be transmitted by air, represents a dangerous threat to all the servants in operations.

Any outbreak has a great impact on operational sustainability for the following reasons:

- Limits the manoeuvrability of the forces in the field;
- Imposes a withdrawal in the territory, which results in a lowering of the operating effectiveness;
- Requires substantial healthcare resources;
- Could hinder the tactical response capability of the Role 2-Plus[1];
- All individuals become potential carriers of the contamination.

Known bacteria and viruses are always present in the environment and the potential exists for a myriad of undiscovered contagions, hibernating in the glaciers of the poles, to be released for which people have no immune defences, nor the possibility of creating a vaccine. This could be likened to fighting asymmetric warfare where the actors move quickly all over the world without distinguishing borders or combatant status. They could hit and disappear randomly and without warning, act on a large scale, and no intelligence service can determine if they have been defeated or when they may return.

No single organization is able to deal with an epidemic on a national scale, since it requires health resources at a national level that have never been structured or designed to face a moment of crisis of such magnitude. Each nation manages to deal with chemical and geological disasters, but the biological element presents a critical challenge that could deplete or collapse the resources of a nation. The biological aspect has several consequences: it is a moment of social disintegration, it is an economic brake, it has a devastating psychological impact, and it can drain all health resources. However, biohazards must be analysed according to a multiphase, multi-purpose principle that begins with the strategic approach and ends with the tactical. It is much more complex because of what could happen if a NATO member, or an area that is of strategic interest to NATO, was attacked by an international actor during or after a serious crisis. There have been examples of attacks of this nature in areas where the country's opposition leader was poisoned. This, in turn, caused the national emergency services to respond in a multi-faceted nature. The impact on national security is not a remote hypothesis, it is a concrete reality. Today the great pandemic of the COVID-19 is a legitimate worldwide threat, but people should consider a context in which numerous biological threats could take place. Any notion that this type of scenario would be best managed by nations turning inward and acting only at a national level not only confirms what NATO foresaw in the late 1990s, but is immediately dispelled by the inefficacy of the national responses seen to date regarding COVID-19.

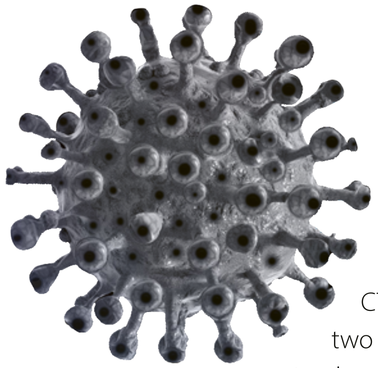
Implementation During the Pandemic

Transport aircraft that are normally used for different types of missions – from search and rescue to support for special operations–become real 'flying ambulances' when emergencies take place. They are capable of transporting patients in Bio-containment mode through special isolated stretchers called Aircraft Transit Isolators (ATI), as well as assisting patients with respirators during the flight.

The ITAF developed this particular transport capacity several years ago, when it first realized that this specialisation would fill existing gaps in capabilities, and the history proved it right when it became crucial during the difficulty times of the Ebola or the Severe Acute Respiratory Syndrome (SARS).

The first experiment occurred in 2005, while the first operational flight followed on 24 January 2006 when a C-130J aircraft rescued a patient suffering from a severe form of pulmonary tuberculosis resistant to any drug treatment.[2] It is a valuable activity that the ITAF has carried out for over fifteen years, and made them a leader in the field of air transport in Bio-containment.[3] However, the current demand for patient transport has significantly increased. For this reason, the 'Reparto Sperimentale Volo' (RSV) which is one of the three departments within the Experimental Flight Centre, was involved in increasing both the transport capacity of patients in isolation and the number of medical support teams.

By using the Technical-Operational Certification (CTO), the RSV launched a series of studies, research and experimentation activities aimed at producing the necessary documentation to expand the ability to transport different types of stretchers, both on transport aircraft for long-range flights, and on helicopters for short-distance connection. Thanks to the teamwork between pilots, engineers and experimental mechanics, the RSV released the CTOs in less than two weeks in the simplest cases, while in more technically complex situations, they physically built and adapted electro-mechanical pieces to allow the use of the different stretchers on multiple types of aircraft. This considerably enhanced the bio-containment capabilities of the KC-767A, C-27J, C-130J and numerous helicopters, such as the HH-101A, HH-139A and HH-212.



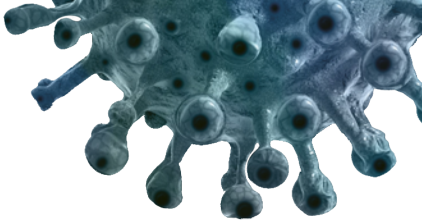
© geralt/Pixabay.com

During air transport, the patient travels inside special Aircraft Transit Isolator System (ATI). In general, an ATI consists of a frame (rigid or semi-rigid), a Polyvinyl Chloride (PVC) casing (so-called envelope) that allows observation and treatment of the patient in isolation, a battery-powered motor that allows maintenance of negative pressure inside and High Efficiency Particulate Air (HEPA) filters that prevent the entry of potentially infected micro particles at the inlet and outlet, guaranteeing the safety of healthcare workers who assist the patient.

The team consists of a Team Leader, at least two medical officers and six non-commissioned officers. The Team Leader is a senior medical officer who has the task of coordinating the mission, managing relations with the civil entities involved, and supervising the progress of operations. The medical officers are an anaesthetist and an infectious-disease specialist who are responsible for the health management of the patient, while the six non-commissioned officers assist the patient and carry out the transport procedures.

Air transport in Bio-containment is a military capability, available for civil use and purposes (dual-use). Numerous civil and military organizations, both national and international, have requested specific training activities from the Air Force on the management and transport of highly infectious patients to acquire the skills and the techniques needed to manage transport situations in risky bio-containment environments.

Beginning in 2013, the Bio-containment team participated in the NATO exercises: VIGOROUS WARRIOR 2013,



© Aeronautica Militare

2017, 2019 and TOXIC TRIP 2019, incorporating NATO's Allied Command Transformation's (ACT) intent to overcome several limits to interoperability through the process of technological and capability innovation to operate in multinational contexts.[4] The experience gained during the Ebola emergency, participation in NATO's health exercises and exchange activities with foreign nations (The Netherlands and United Kingdom) led the ITAF to identify a new mission and vision for the use of the structure of Bio-containment in the operational context of Global Bio-security. Everything hinges on the operational concept that pandemics are a global problem where if a 'Readiness Action Plan' or a 'Bio-responsiveness High Readiness Multinational Task Force' type construct fails to adequately address the risks, then Global Bio-security problems may arise. A large-scale epidemic could shake the foundation of international health security by creating areas of vulnerability which could interfere with the sustainability of NATO's defensive framework, in case we should face a scenario consisting of multiple massive proportion emergencies simultaneously. Moreover, one must consider the importance of assistance to allied nations troops affected by infectious diseases while deployed in areas where

AIRCRAFT	Missions	Sorties	Flight Hours	Patients
KC-767	7	21	141.11	26
C-130	25	87	125.25	69
C-27	1	4	03.16	1
HH-101	3	11	10.36	3

there is no health care facility available capable of providing treatments with the same level of accuracy. For this reason, the ITAF has equipped its air transport systems with biological isolation capability, that allows them to operate with the maximum safety and protection for flight crews.

Lessons Learned for the Entire Alliance

COVID-19 is a biological threat that affects the Euro-Atlantic zone and their areas of strategic influence with the unconventional characteristics of asymmetric warfare. This highlights the need to continuously remodel the operational planning process by calibrating it in relation to the affected areas, the number of people to be evacuated, the reconfiguration of field hospitals and the need to guarantee the sustainability of supplies.

The key factor is time, which allows one to act by transporting affected patients promptly to the reference care centres before the disease progresses. It is essential to create a strategy to respond to a pandemic based on prevention, identification of the threat, its geolocation, isolation and evacuation of patients. One of the primary mechanisms for responding to civil emergencies in the Euro-Atlantic area is air support. In addition to the purely logistical aspects, nations should keep in mind that NATO forces may need to be redeployed using air assets to safer areas for health reasons whenever the need arises.

Service members that continue prosecuting the mission must be given the certainty that, in case of contamination, they will be assisted and treated promptly. For this reason, Bio-containment shall be considered as a fundamental pillar within the Strategic Airlift International Solution (SALIS) and the Biological Strategic Airlift Capability (BSAC).[5] It will have to be considered a reality that should have its tactical role within NATO's Air Mobility operations. There is a need to create NATO doctrine on air operations, specifically in Bio-containment where the capacity of the Alliance forces can have, through sharing of resources, a joint multinational force capable of operating in an intercontinental context. The maximum speed of effectiveness in transferring infected patients can definitely help to reduce the area and spread of infection. This is an ambitious goal, a new operational capability for NATO, which will have to be shared within the Alliance and its partners to train, practice and operate effectively together, carrying out assigned missions and tasks.

There are two types of fundamental factors in interoperability between nations: core and enhancement. They consist of promoting a series of elements which are crucial for the success of each mission. These include the terminology, the doctrine of Bio-containment on a multinational basis, the ability to identify

© Aeronautica Militare

a multinational mission and vision on common objectives with allied forces, and to reshape industry to produce ATIs that have compatible standards, so that any aircraft in the NATO transport fleet could use them.

A Look into the Future

There is always an opportunity for improvement and that is particularly true in those areas that are high technology and rapidly changing. The 2020 pandemic emphasised that the Alliance should definitely consider developing Bio-transport capability as it has been crucial in managing the pandemic. The ITAF has accrued fifteen years of experience in this field and was ready to face the imminent situation, being able to carry back to the home nation several personnel from remote areas. The ITAF, among others with this capability, was able to further validate its Bio-transport, gaining valuable teachings such as the need to continuously reshape the operational planning process by adapting it with regard to the affected areas, the number of people to be evacuated, the reorganization of field hospitals and the necessity to ensure the sustainability of supplies. For all the reasons highlighted above, NATO should take into consideration to add this doctrine to the broad arsenal already owned. As much as one might hope that the COVID-19 pandemic will be the last pandemic humans will endure, pragmatism demands that member nations ready the Alliance for the next occurrence by further developing Bio-transport and implementing mutual exercises. Preparation, including development of tactics, techniques and procedures is a far more effective strategy than reaction. ●

1. Lynn, D.C., Lesemann, R.K., Detro J.F., and Seery, J.M. (2014) Employment of the 'Role 2-plus': lessons learned in a time of high OPTEMPO. Military Medicine, 179 (12) 1412–1418.
2. Allied Command Transformation invitation letter of 22 Mar. 2018, NATO UNCLASSIFIED. Internal ref.: 7730/TSC TPX 0220/TT 180372/Ser:NU0207.
3. Cenciotti, D. (2020) How Air Evacuation of Patients Under Biosafety Containment Works. Available from https://theaviationist.com/2020/02/10/coronavirus-this-is-how-air-evacuation-of-patients-under-biosafety-containment-works/ [accessed 6 Aug.2020].
4. Sanzani, M. (2019) The transport of a highly infectious patient aboard an Italian Air Force C-130J was the focus of the largest NATO health exercise in Romania. Blog Before Flight Staff. Available from https://www.blogbeforeflight.net/2019/04/vigorous-warrior-2019-italian-air-force-trains-bio-containment-transport.html [accessed 26 Apr. 2020].
5. North Atlantic Treaty Organization (2020) Strategic airlift. Available from https://www.nato.int/cps/en/natohq/topics_50107.htm [accessed 21 Jul. 2020] .

Lieutenant General Domenico Abbenante

graduated from the University of Florence in 1981, Degree in Medicine and Surgery, and was commissioned a first lieutenant at the Italian Air Force Application School in Florence. His first assignment was as a Medical Director at Perdasdefogu Experimental Training Polygon, Sardinia in 1982. Since then, he has served in a variety of command and staff positions to include: Aeromedic Center for Psychophysiological Selection Chief at Italian Air Force Medical Institute, Director of Italian Air Force Medical Institute in Rome and President of Medical Legal Board of Defense. He has also served as Logistic Command Health Service in Rome and since 2020 he serves as the Head of the Air Force Military Health Corps. Lieutenant General Abbenante holds also a graduate degree in Laws, Economics and Management Sciences.

Captain Massimo Di Milia

joined the Italian Air Force Academy in August 2004, where he obtained a degree in Political Science. As of 2009, he was a Military Pilot starting at Specialized Undergraduate Pilot Training in Vance AFB (USA) and later 46th Air Brigade, 2nd Squadron (Air transport), where he obtained 'Combat Readiness' on the C130 aircraft in Pisa. From 2011, his training was complemented with special skills e.g. airdrop, air-to-air refuelling, night vision goggle flight, and assault operations. As a pilot, he was much involved in air support to missions abroad in Afghanistan 2011-2015, Kosovo 2012, Lebanon 2013, Libya 2014 and Iraq 2014. Furthermore, he participated in multinational joint exercises including Special Forces. Since Sep 2019, he serves in the JAPCC as Subject Matter Expert for Air Transport.


© Lockheed Martin

NATO Joint All-Domain Operations

JAPCC Subject Matter Experts (SMEs) have begun earnestly working on a new centre-wide project titled 'NATO Joint All-Domain Operations'. In order to adequately describe the project, some background is provided below.

Joint All-Domain Operations (JADO) is an evolution of the concept of Multi-Domain Operations (MDO). MDO highlighted the massive potential of a truly joint force, able to tap into capabilities across the entire spectrum of current and emerging systems available in our military services. However, when considering the future of warfare, MDO has a few critical flaws. First, the term MDO can be confusing since most national services already operate in multiple domains with their own, service specific capabilities. Second, considering the entanglement of systems and interconnected capabilities spanning the domains in today's state-of-the-art militaries, it can be argued that our traditional structuring of services based on their principle operating domain may not be very useful in many future scenarios, where the victor will emerge as the force able to manoeuvre easily in and through all domains in a synchronized manner at a speed which the opponent cannot match. With these considerations in mind, it is easy to conclude that MDO places too much weight on the domain, thereby reducing emphasis on the joint challenge of multiple services seamlessly working together across all domains. Additionally, MDO does not account for the reality that globally, the vast majority of militaries plan for, and rely on, their ability to conduct operations in a combined environment, as is certainly the case for Allied nations.

In order to put emphasis on the **challenging reality of operating jointly in a combined environment,** the JAPCC has created a new expansive project entitled NATO JADO. 'NATO' gives the combined environment sufficient priority, whereas 'JADO' places emphasis on the problem of operating jointly, while also circumventing the structured ideas of domains since it includes them all. The aim of NATO JADO is to identify and provide solutions to the problems associated with accessing and tasking assets from all countries' services that may contribute forces to a NATO operation, *'Joint All-Domain Operations (JADO) is an evolution of the concept of Multi-Domain Operations (MDO).'*

in order to create synergistic effects that cause multiple dilemmas across a myriad of contact points while outpacing an enemy's decision cycle.

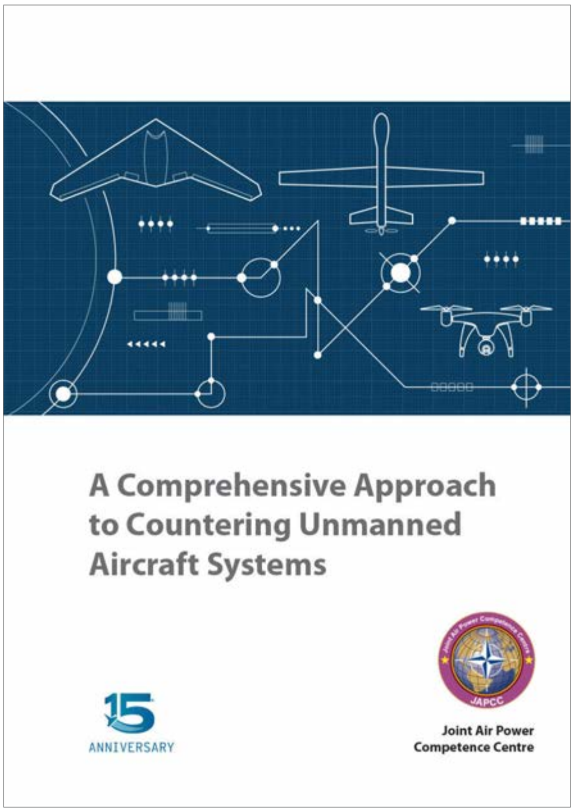
This internally-driven project has many burgeoning synergies with initiatives in progress throughout national warfighting institutions and in NATO organizations including the Strategic and Component Commands, Joint Analysis and Lessons Learned Centre, the Joint Warfare Centre, NATO Defence College, and other Centres of Excellence. Working closely with these partners, the project is identifying the requirements, capabilities, and training models NATO should be developing now in order to move from our current state of interoperability to a level of integration able to conduct JADO within the next 10–20 years. NATO JADO is focusing on the most achievable and critical topics from the joint air and space power perspective. The scope of the project includes critical nodes, desired capabilities, Command and Control, interoperability requirements, and (perhaps most importantly) the training necessary to optimize the leadership model and promote alliance-wide understanding. Mobilizing our diverse set of joint SMEs, the JAPCC is well positioned to collaborate, contribute, and help align priorities across the Alliance leading to a more interoperable and effective fighting force.

Countering Unmanned Aircraft Systems

The JAPCC recently published a comprehensive book on the subject of countering unmanned aircraft and drones.

Unmanned Aircraft Systems (UAS) have become an integral part of NATO operations and have matured into invaluable assets for Intelligence, Surveillance, and Reconnaissance, as well as for combat missions.

This has not gone unnoticed by both state and non-state actors, which has led to an enormous effort by these players to catch up with or at least mimic the Western level of technology. Over the last decade China, Russia, and to a certain extent Iran, have all considerably advanced their development of UAS and their latest models seem to have performance characteristics similar to Western models. Russian and Chinese inventories comprise the full range from small and tactical UAS, through medium- and high-altitude long-endurance systems, to replicas of US and European stealth prototypes.



At the same time, the consumer drone market is one of the world's fastest growing businesses, making drone technology literally available for everyone. The market for commercial drones with a significantly higher performance than consumer models is also steadily growing. Due to their increased proliferation, the number of incidents with drones in the vicinity of airports, public events and military installations has raised the attention and concern of the respective civil authorities responsible for public safety and law enforcement.

Countering military UAS and consumer drones is a challenging task, both in the military and civil domain. Therefore, it is important to incorporate all available means and to exploit any vulnerabilities to achieve this task. However, most UAS and drone defence applications are focused solely on the unmanned aircraft itself rather than exploiting the weaknesses of the entire system, which typically also comprise mobile or stationary remote-control equipment, radio communication links, and human personnel.

It is also important to note that countering UAS and drones is already a task in peacetime whereas most military defence applications are intrinsically designed for a conflict scenario. Additionally, the legal frameworks for operating in peace, crisis or conflict differ significantly and as such, adopting civil approaches to this challenge and incorporating civil authorities is required when the employment of military force is restricted or prohibited.

This recently published work addresses these and many other challenges across the military, civil, and legal spheres and is available online at ***www.japcc.org/C-UAS.*** ●

The JAPCC Hosts 7th Annual JASPN Meeting in a Virtual Environment

Collaborating During the Pandemic

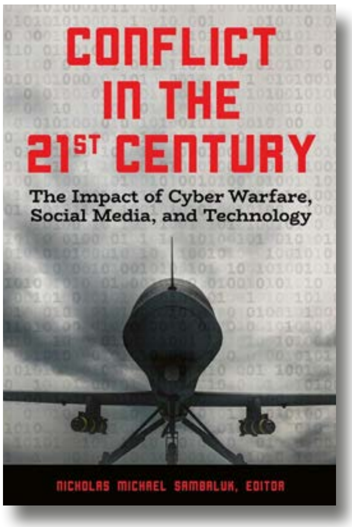
As NATO's Centre of Excellence for Air and Space Power, the JAPCC strives to enhance synergy to collectively provide innovative timely advice and subject matter expertise to the development of Air and Space related concepts and capabilities, and to provide focused support to NATO training and major exercises.

The Joint Air and Space Power Network (JASPN) Meeting has proven to be a productive venue for collaborative discussion and to promote synergy within the Air and Space Power Community. Due to the pandemic situation throughout Europe, this year's JASPN Meeting was held in a virtual setting from 10–11 November 2020. The JASPN brings together international organizations with an inherent interest in Air and Space that are of particular relevance for our militaries. This year, we had valuable participation from the Allied Air Command, Air Operations Center of Excellence, Competence Center for Surface Based Air and Missile Defence, European Air Group, European Air Transport Command, European Defence Agency, Integrated Air and Missile Defence Centre of Excellence, Movement Coordination Center Europe, NATO Headquarters, NATO Science and Technology Organization.

Following two days of virtual, yet very collaborative discussions, we have provided an urgently needed transparency on our respective programmes of work. This allows us to identify areas of common interest with the potential for collaboration and the avoidance of unnecessary duplication. Areas of particular interest, to many participants, included aspects of interoperability, hypersonic, space cooperation, rapid air mobility, modelling and simulation, artificial intelligence and big data.

Although the meeting demonstrated that virtual collaboration can help within the constraints of a pandemic situation, all partners were convinced that a meeting in full presence provides an additional value to ensure the necessary exchange of thoughts. We are therefore looking forward to next year where we hope to welcome our colleagues to the JAPCC conference facilities in Kalkar, Germany.

‘Conflict in the 21st Century’

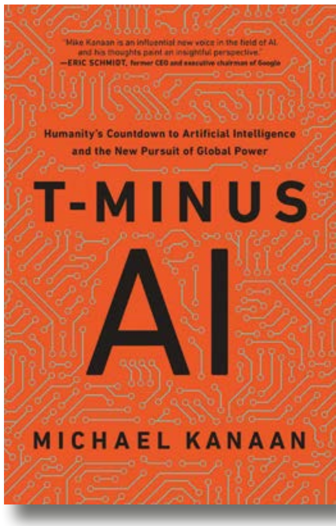


By Nicholas Michael Sambaluk;
ABC-CLIO; August 2019
Reviewed by:
Lt Col Tim Vasen,
GE AF, JAPCC

Conflict in the 21st Century is a collection of essays on Cyber Warfare, Social Media and Technology and of the latter's role in supporting the first two realms. Each of the three chapters begins with a short topic overview, which is followed by several in-depth essays. The essays build upon introductions of the specific systems or their impacts. They then describe the nature of Cyber effects and the employment of social media systems in support of campaigns. Some important persons from sovereign nations to terrorist groups, who are behind the development of these new tools of warfare are introduced. The book is very interesting and understandable to readers with no previous technical knowledge on the topics, but who are interested in their impact on modern society. Examples of malicious Cyber activity, as in the case of Julian Assange and WikiLeaks, along with the effectiveness of previously employed malware, such as the WannaCry-virus, are discussed, as is the effectiveness of several different secure networks in response to such malware. The examples of Social Media introduce systems such as Telegram and explain how ISIS employs propaganda. Instances where modern Technology is exploited are described including 3D printers and high-end weaponry which, when proliferated globally, will require a synthesis of nationally employed means to counter them. Overall, this collection of essays allows an interested reader to gain insight on the mechanisms, risks and threats from these areas that the world must face now and in the future. This book is recommended as a rich repository for non-linear means of modern warfare, even for subject matter experts. ●

‘T-Minus AI’

In a fast-paced world dominated by information overload, it is all too common an occurrence when professionals across specialties engage in conversations which have them second-guessing their understanding of hot buzzwords and often talking past one another. The result, as Kanaan remarks, is ‘too many confusions are never clarified and too many more are created’. (p. 5) Artificial Intelligence, or AI, while currently a trending discussion topic is more than a buzzword, it represents a key concept of technology that is increasingly ingrained into our daily lives. It is therefore incumbent upon each of us to ensure we understand what AI is, how it affects us today, and what it will mean for the world of tomorrow. Thankfully, T-Minus AI provides answers to these questions, and in a way that is both approachable and easily digestible. Michael Kanaan's initial foray into the world of publishing utilizes a building block approach which allows all readers to start with the same basic understanding of the history, evolutionary development, and aspects of AI. He then expertly weaves in social and political considerations, as well as elements of bias, while still connecting to the lives of everyday people seeking to learn more about AI and its implications for our shared future. For the military operators and planners who think they understand AI, T-Minus AI provides a complete run-down of AI-related background and information that is crucial for participating in discussions which will shape and guide our operational reality in the years to come. As Kanaan notes ‘The full implications and effects of AI and machine learning technologies remain to be seen in the months, years, and even decades ahead.’ (p. 232) ●



By Michael Kanaan;
BenBella Books; August 2020
Reviewed by:
Lt Col Henry Heren,
US Space Force, JAPCC


MQ-9B SkyGuardian