Joint Air & Space Power Conference 2020

Leveraging **Emerging Technologies** in Support of NATO Air & Space Power

8 – 10 DECEMBER **2020**

READ**AHEAD**

Joint Air Power Competence Centre

Leveraging

Emerging Technologies

in Support of NATO Air & Space Power

LEVERAGING EMERGING TECHNOLOGIES IN SUPPORT OF NATO AIR & SPACE POWER
JAPCC JOINT AIR & SPACE POWER CONFERENCE 2020

*READ**AHEAD***

Leveraging
Emerging Technologies
in Support of NATO Air & Space Power

Joint Air and Space Power Conference 2020

Acknowledgements
This read ahead is a JAPCC product realized in collaboration with the authors of the essays contained herein. The JAPCC would like to thank the numerous authors who took the time to contribute to this product in an effort to advance this topic for discussion within NATO.

Editorial Team
Brig Gen Giuseppe Sgamba
Col Brad Bredenkamp
Col Thomas Schroll
Lt Col Henry Heren
Lt Col Zenon Kot
Lt Col Livio Rossetti
Mr Simon J. Ingram
Sgt1 Lilian Brandon
Mr Daniel Reinemann

Disclaimer
The views expressed in this work are those of the authors. It does not represent the opinions or policies of the North Atlantic Treaty Organization (NATO), and is designed to provide an independent overview, analysis and food for thought regarding possible ways ahead on this subject.

Published and distributed by
The Joint Air Power Competence Centre
von-Seydlitz-Kaserne
Römerstraße 140
47546 Kalkar
Germany

M Denotes images digitally manipulated

Moderator’s Foreword

Esteemed Colleagues,

When our way of life is threatened, we look to science and technology to save us. This is as true of our most current crisis – the Covid-19 pandemic – as it was of other global threats in the past – wars, famines, expansionist regimes and so on.

The few paragraphs I have written here will take you (very approximately) 2.5 minutes to read. The read ahead material that my words precede will, I am sure, take you considerably longer. However, the enforced delay to the conference does allow you the extra time to do this. I do urge you to invest this time – it is a wise investment, in more ways than one.

This read ahead material represents the largest ever submission of articles from air and space power experts worldwide to a JAPCC publication. Many of these have been specially written for this year’s Joint Air and Space Power Conference. As you read and critically appraise the articles, you will want to make notes and (perhaps furiously!) underline and highlight those parts that you take issue with. Please do this! I well remember a professor who exhorted her students (myself included) to personalise their set texts by scribbling notes in every available blank space. Her assertion was that, only by doing this, could we engage sufficiently with the material and make it our own.

As a young man (so many years ago now!) one of my favourite UK television programmes was called Tomorrow’s World. During the 1970s, it attracted 10 million viewers a week and focused on the science and technology that we could look forward to transforming our lives for the better in the future. The final panel of the conference attempts to do something similar in terms of technological crystal ball gazing. As I still do not have my own personal jet-pack, I tend to treat any predictions for the future with healthy scepticism. I am writing this in late May 2020 and I would be very brave (some might say foolish!) to even try and predict what will be happening in the world as the conference takes place in December.

The only thing we can predict with any confidence is that bad things will happen. Unfortunately, we are not very good at saying what those bad things might be or exactly when they might happen. We must, therefore, set the conditions (and, above all, make the necessary investments) to ensure that we can pre-empt and prevent as many bad things from happening as possible. But for the bad things that do still leak through - Covid-19, for example – we have to remain agile and adaptive enough to first buy the time to analyse them before we can, ultimately and hopefully, defeat them. In addition to money, this requires clever, creative people who can work together to share, adapt and create new ideas and new solutions.

The four panels of the 2020 JAPCC conference cover a lot of ground, and air, and space for that matter – all of it completely fascinating. However, if you let the conference become no more than a collection of experts telling you what they think, then you risk wasting a lot of what the conference is really about. Above all, the JAPCC conference is a forum for debating and exchanging views with the ultimate aim of creating new ideas and knowledge. We should all contribute to that.

I have been part of many JAPCC conferences now, both as a JAPCC SME when I wore RAF uniform and as a civilian. One of the great things about the JAPCC conference is that, whilst we hear from the smart people on the platform, we also get to hear from some of the smartest other people in the room. By which I mean those of you sitting further back in the auditorium – and with (relatively) less in the way of gold braid on your hats and jackets. I am very aware that one of my most important roles as the moderator is to ensure that there is sufficient time to hear from you in the discussions that follow each panel. I think you will find that this year's agenda and format lends itself nicely to that increased audience participation. In the meantime, if as you read and think critically about the articles within you are moved to respond immediately, please reach out to me or to the JAPCC directly at conference@japcc.org.

I would like to conclude by thanking the JAPCC for inviting me back as Moderator for their conference again this year. This is, in no small part, due to the positive feedback from many of you who attended in 2019. So, thank you to you all and I look forward to meeting, and hearing from many of you, in December.

Bruce Hargrave BSc MBA
Independent Air and Space Power Consultant

Table of Contents

Table of Contents

Table of Contents

LEVERAGING EMERGING TECHNOLOGIES IN SUPPORT OF NATO AIR & SPACE POWER

JAPCC JOINT AIR & SPACE POWER CONFERENCE 2020

Space

Space Panel Introduction

1

NATO's Newest Recognized Operational Domain

By Lt Col Henry Heren, USA Air Force
Joint Air Power Competence Centre

Introduction

In 2020 the Joint Air & Space Power Conference will focus on how NATO leverages emerging technologies in support of Air & Space Power. Specifically, how do new capabilities operating in and through Space (NATO's newest recognized operational domain) integrate into NATO Operations; both from a standpoint of additional capability contribution as well as potentially new challenges?

In the closing days of 2019 NATO recognised Space as an operational domain, referencing its importance in keeping the Alliance safe and in addressing security challenges, in line with international law. As NATO continues to integrate terrestrial and extra-terrestrial operations, what will be NATO's role in ensuring freedom of movement in and through Space? Not only to ensure access to ever-increasingly important Space-based services to terrestrial operations, but also to enable operations in Space in pursuit of freedom of movement for extra-terrestrial operations. Additionally, as NATO currently possesses no indigenousness Space capabilities, and has no current plans to begin procurement of any such capabilities, how will NATO achieve an accord amongst the member nations to ensure reliable and consistent delivery of Space-based products and services? Will the answers to these questions come from additional personnel, or are there emerging capabilities NATO can leverage to manage the myriad inputs (from Space) its member nations provide in a manner useable for NATO HQs and the forces they lead in operations? This panel will tackle these issues at a time when NATO is just starting to address some of these questions, and perhaps only realizing the complexity of the new domain it has entered.

Advances into Space and Space's Recognized Relevance for the Military

On October 4, 1957, the Soviet Union launched the first man-made object, Sputnik-1, into orbit around the earth. The Soviet launch forever changed the world and moved Space to centre stage in the on-going Cold War between Western Democracies and Eastern Bloc Communist nations. As the Space-Race continued, the world watched as the US and Soviet Union engaged in an international effort to outshine one another with ever-increasing advances into Space. The competition culminated, for a time, on July 20, 1969 with 'Neil Armstrong's and Buzz Aldrin's first footprints in the lunar soil'.[1] While the political chest-thumping of the Space Race dwindled, military applications of Space-related capabilities continued to develop. However, unlike the direct rivalry seen in the Space Race, many militaries with access to Space capabilities did not see 'an entirely new mission, but rather, a new environment that can enhance traditional missions.'[2]

The ability of militaries to utilize Space-related capabilities was thrust onto the world stage during the Gulf War in 1991. Space 'assets provided navigation, communications, intelligence, and imagery that were essential to increasing the combat effectiveness of the allied coalition.'[3] In fact, 'Space was so crucial to nearly every aspect of the operation that some military leaders called it the first true "space war"'.[4] However, for all of the praise for contributions from Space in military operations, Space was seen as an utility for supporting those traditional missions on land, at sea, and in the air.

Within the burgeoning military Space community, particularly in the US, the belief that Space presented unique opportunities and challenges, and needed to be shepherded by professionals with expertise in Space Operations began to mature. This notion grew to the point the idea of a separate and independent Space Service began circulating, and gained traction in the US with the publication of the so-called Space Commission Report in 2001 which stated 'the US has not yet taken the steps necessary to develop the needed capabilities and to maintain and ensure continuing superiority.'[5] Many in the US Military saw this as a warning, if the current military structure did not address important issues related to Space then perhaps the organization should be changed.

Road to NATO's Recognition of Space

While the status of Space, and its associated organizations and agencies, has slowly evolved over time, the advancement of technological capabilities resident in Space Systems has continued unabated. In the midst of these advancements, NATO (as an organization) has largely remained on the sidelines. Nations, both internal and external to the Alliance, have been the driving force behind the development and fielding of new Space capabilities. While NATO has procured agreements for its member nations to share data, products, and services (DPS) from Space, these agreements largely entail nations determining what DPS they will provide to NATO ... with little to no requirements by the nations. Conversely, the nations (again both internal and external to the Alliance) have developed numerous sharing agreements regarding DPS, most often in the form bi-lateral arrangements, which may prove problematic in the event of a NATO-led military operation.

Supporting NATO's Growth in Space

NATO's recognition of Space as an Operational Domain does not include any planned or approved NATO procurement of Space-related capabilities, nor does it involve any increase in Space Personnel within the NATO Command Structure (NCS) yet; currently there are approximately 20 positions for Space personnel within the NCS. As NATO moves forward in its relationship with Space as an Operational Domain, it should do so in a manner commensurate with its (somewhat limited) capabilities and personnel strength. Rushing into bureaucratic decisions, which are often difficult to re-consider after the fact, without due consideration is fraught with peril.

NATO's primary shift following its recognition of Space as an Operational Domain is to pursue policy objectives, and to organize a Space Centre. The Space Centre, currently planned to be co-located with Headquarters Allied Air Command, is intended to serve as the coordination focal point for Space-related activities during NATO military operations. As the relatively small collection of dedicated Space Professionals within NATO strive to bring the Space Centre to fruition, new pursuits of technological development will remain with the Alliance nations. This places a premium on information regarding emerging technologies, and how the nations might employ them in support of NATO military operations.

Additional Articles

This section presents nine related articles which will introduce various ideas and issues related to the Operational Domain of Space, and the different challenges NATO faces therein. The ideas expressed in this article are meant to inspire some critical thinking to prepare those attending the 2020 Joint Air & Space Power Conference for the panel discussion on Space:

- In Space Situational Awareness Challenges, Professor Malgorzata Polkowska discusses efforts made by the Polish Space Agency (POLSA) in recent years. The paper details how POLSA's activities guide the Polish Military in terms of Space related tasks and responsibilities. The paper also discusses POLSA on-going work with various European Agencies, to include the European Space Agency and the European Union Space Surveillance and Tracking Consortium.

- The next paper, Commercial Constellations and/or Mega-Constellations of Small Satellites in Low Earth Orbits is written by Lt Col Tim Vasen (DEU Army). This paper focuses on the continuously changing commercial Space Market with emphasis on smaller more technologically capable satellites. It explores the impacts to satellite communications and intelligence collection, with regards to the change in the commercial market, for the military planning and operations.

- Paul Szymanski's What are Possible Conflict Termination Criteria that Define Winning the Next Space War appears next in the booklet. The paper provides a list of 15 possible Termination Criteria for consideration in a Space Conflict, briefly examining each of the proposed criteria and encouraging further discussion as to what the future will hold for conflict beyond the atmosphere.

- Space Connectivity for Air Combat 2040 is a collaborative work by Alain Frizon, Christian Calamarte, Christian Fournier, and Raphaël Ihamouine. This paper discusses the connectivity needs for operations spread across manned and unmanned platforms, flown by multiple services, and originating from different countries. The paper also touches upon technologies which can be considered to meet these needs.

- Stepping outside of NATO, Space Development and Changes on Traditional Power's Balance delves into the role Space plays in South American power dynamics. Written by Victoria Valdivia, a Chilean Space Professional, this paper explores the role of Space in political balancing within and between South American Nations, on the continent, and with those nations' interactions with global space powers.

- The contributions from outside of NATO continue with Cyber Threats to Space Systems, written by Gil Baram and Omree Wechsler of Tel Aviv University. This paper deals with Space from a perspective of maintaining an acceptable level of cyber defence of Space Systems. Detailing the cyber threats to the various segments of Space System, responses and mitigation actions, as well as NATO's role.

- Assessing the Impact of Space Traffic Management on Military Space Operations, by Marc Becker, describes what Space Traffic Management might look like in an age of significantly increased constellations. The paper goes into how multiple governments and government agencies are attempting to address the issue, as well as the essential role of the military in the process.

- With NATO's recent recognition of Space as an Operational Domain John J. Klein and Nickolas J. Boensch provide policy suggestions in Assured Access to Space through a Strengthened NATO Space Deterrence Strategy. Building upon deterrence theory for Space the paper examines ways NATO can implement a Space Deterrence Strategy and includes actions to be taken in the near-term.

- The final Space Panel paper deals with a topic new to many. In Applied-Field Magnetoplasmadynamic Thrusters, the importance of spacecraft propulsion is introduced along with an examination of new related technology. In this paper, Manuel Betancourt, Marcus Collier-Wright, Ryan O'Regan, David Hindley, Georg Herdrich, and Lamont Colucci discuss the operational impacts of new propulsion systems, as well as geopolitical background the need for NATO Cooperation going forward.

Lieutenant Colonel Henry Heren is a NATO Space & Cyberspace Strategist assigned to the JAPCC. He is a Master Space Operator with more than 27 years' active duty experience in the US Air Force. He is a Graduate of the US Air Force Weapons School.

Endnotes

[1] Sellers, Jerry Jon, Understanding Space: An Introduction to Astronautics, Third Edition. The McGraw-Hill Companies, Inc. New York, 2005. p. 49.

[2] Ibid., p. 61.

[3] Ibid.

[4] Ibid.

[5] US Report of the Commission to Assess United States National Security Space Management and Organization, 11 Jan. 2001, p. 10.

© CG Alex / shutterstock

Mega-Constellations

11

Commercial Small Satellite Constellation in Low Earth Orbit

By Lt Col Tim Vasen, DEU Army
Joint Air Power Competence Centre

Technical Developments

Emerging technologies offer wide opportunities for Space systems and their services. The ability to build spacecraft smaller and lighter due to technical developments have made Space activities more attractive to the commercial market. In addition launch costs for satellites have decreased considerably, while the number of potential launch providers has increased significantly. In the past even the commercial launch business was more or less 'state-driven,' whereas today it has been completely opened to the commercial market. Companies like SpaceX® (USA), Rocket Lab® (USA/NZL), Virgin-Orbit® (USA), iSpace® (CHN) or Galactic Energy® (CHN) are gaining more and more customers, and offer Space launch services in nearly all orbits. States are still in charge for the licensing and Space security during the launch phase but mainly because the commercial companies still rely on state-owned launch infrastructure. This may change in the future when more and more commercial companies operate their own launch infrastructure and operate out of more countries worldwide.

Besides the decreased launch costs, paired with the chance to build smaller spacecraft, a new threat assessment or philosophy for satellite constellation operations has been developed, especially by the commercial market. In the past, and still today for military or security satellites, the systems were built on high-security standards that include technical multilevel redundancies and the use of expensive Space environment-hardened equipment which all together raised the manufacturing costs tremendously. To get the best value, the longest possible lifetimes of the deployed systems were intended. This caused years-long design and manufacturing periods for a satellite, which often caused the satellite to be either technically 'obsolete' before it was launched or after a couple of years of operating. Today's emerging technological development allows building smaller and less robust and resilient spacecraft, because they will intentionally get replaced after only a few years of use. These changes in the development philosophy allow significantly shorter development and production times, not only for the satellite itself but also for the components which could be mostly commercial-off-the-shelf (COTS).

An additional feature that belongs to emerging technology is artificial intelligence. The current and foreseeable technical developments offer a high level of autonomy of individual satellites or even whole constellations, which reduces access points for potential cyber incidents and increases the overall resiliency of such systems. These developments, taken together, make it especially appealing cost-wise for commercial entities to invest in the Space sector.

Additionally due to the stated limiting factors, the idea of building large constellations of small and inexpensive spacecraft to ensure a persistent service is also of interest for the commercial market. While building, for example, a SATCOM service based in Geostationary Earth Orbit (GEO), only three satellites for a near-global coverage are required. Ensuring the same coverage with a constellation in LEO requires several hundred satellites. Smaller satellites that can be used in LEO decreased launch costs especially compared to GEO, due to emerging technologies which made this commercially affordable.

To remain current about the technically possible services, even when it is not anticipated to use them for military purposes, NATO and/or its member nations should monitor the commercial market to understand the opportunities and threats caused by emerging capabilities. NATO should additionally encourage the member nations to influence commercial companies registered in their countries, through licensing or project definition processes, to make services (in cases of conflict) unusable for potential opponents outside of NATO. This process has to be initiated early to ensure these kinds of regulations are accepted in the overall project definition as well as in the contract of potential customers. The major threat that has to be avoided is that potential opponents of NATO have the chance to use the service or data. Therefore companies registered in western countries also have to be in contact with the security entitles to identify 'undesirable customers'.

Space Services Currently of Interest in this Context: Satellite Communication (SATCOM)

SATCOM constellations in LEO offer military relevant advantages that have to be considered. LEO applications offer a more robust coverage compared to GEO outside the regime between 70^0 North and 70^0 South. Outside of this geographical regime the visibility of GEO satellites is limited due to very low antenna angles of ground stations to the horizon. Especially in geographical challenging areas like mountainous regions or urban areas, signals of GEO applications are often shaded. Using constellations in LEO offers shortened transmission distances, which allows for either lower required transmission power or a higher data throughput compared to GEO constellations. For SATCOM applications in LEO, due to the expected large number of users and the assessed high amount of data throughput, mega-constellations seem to be more efficient. Lower transmission power also allows for usually smaller user terminals; there is a chance that future SATCOM terminals will be the size of large cell-phones or even smaller. It is assessed these smaller terminals will offer comparable or better performance than today's systems, which are mostly vehicle-borne. Solutions to either cross-link users inside the constellation or the continuous login to passing satellites ensure a constant signal transmission. The overall goal is that the user recognizes no difference compared to GSM applications. Commercial providers that invest in mega-constellations often advertise with slogans that allow or promise internet anytime and everywhere. Talking about resiliency and security, LEO constellations are more difficult to jam in the up-link, because the number of satellites give a certain amount of system redundancy. All together mega-constellations offer opportunities, but also risks. To make the SATCOM services of LEO constellations usable for NATO a number of existing ground infrastructure will have to be upgraded.

Actually, there are different commercial companies which invest in the development of SATCOM applications based on mega-constellations in LEO. Some of them are already in the building phase. The systems, according to their development, licensing and deployment status, which will most likely be first in operation are:

OneWeb® (GBR) – An GBR registered company which planes a constellation that will consist of 648 small satellites, each with a mass of around 150 kg. It will be deployed in LEO with an altitude of 1,200 km. The first prototype satellites were launched in February 2019, the deployment phase of the regular satellites has started on February 6th 2020, deploying the first 34 ones. For 2020 at least two but up to ten more launches have been planned, carrying 34 satellites each, while IOC for the service was planned for late 2021. In late March 2020, after a second successful launch of 34 more satellites, the company went in financial troubles and declared bankruptcy. It is highly probable that the system can and will be deployed after new investors are identified.

Starlink® (USA) – Is a sub-company of SpaceX. The planned constellation will consist of up to 12,000 small satellites each with a mass of around 230 kg. They will be deployed in three orbital regimes in LEO. The first

1,500 satellites are planned in an orbit of 550 km. The first prototype satellite was launched in May 2019, the deployment phase has started in December 2019 deploying the first 60 satellites. For 2020 there are up to 20 launches planed, carrying 60 satellites each. Up to now there are 240 satellites deployed, with IOC optimistically planned for late 2020; which requires at least seven more successful launches in 2020.

On the military side the US Defense Advanced Research Agency (DARPA) is currently developing with Blackjack® a demonstration SATCOM constellation that offers secured communication for military needs, which is planned to be IOC in 2022. DARPA is trying to decrease the development and production cost by monitoring the market and using already developed components of the commercial mega-constellation's mass production process such as the satellite bus for example. Only the needed components for the secured military applications are specifically bespoke developed. This constellation should then interact with a commercial mega-constellation to ensure resiliency by redundancy. This kind of combination between a secured military-operated constellation which then interacts with a commercial constellation seems to be the most efficient way to make these services usable for military and security users.

Intelligence, Surveillance, and Reconnaissance (ISR)

Mega-constellations or large constellations offer a high revisit rate for ISR applications. In particular, change detection or nearly continuous monitoring are potential military usable services. Large constellations of small satellites are limited in ground resolution. The small and compact design of the satellites limits the optics or Synthetic Aperture Radar (SAR) sensors either in size or in transmission power. However, a large number of Space-based assets are harder to counter whether with dazzling or jamming compared to a lower number of higher capable systems which increases the resiliency of the whole architecture. Applications that offer change detection or nearly continuous monitoring services have become more interesting for the commercial market because these data can be merged with navigation data that provide the user always actual images of the environment. On the other hand, services like this increase risk to NATO operations when potential opponents are able to access the data. It has to be ensured that data, provided by commercial companies registered in NATO member nations or nations that have close cooperation with NATO, do not offer military relevant and usable data to potential opponents, especially when this data covers areas of NATO operations.

The US-registered company Planet® already operates one mega-constellation that consists of 120+ small satellites which are the size of a shoebox. This constellation offers nearly continuous monitoring data in medium[1] resolution. The high revisit rate allows change detection and is advertised by the company to 'mitigate risk with persistent monitoring'. The company also operates a constellation of small high-resolution satellites that interacts with the mega-constellation.

The US-registered company Hawkeye360® is the first commercial provider which offers Signal Intelligence (SIGINT) service. The constellation is currently in the deployment phase and will consist, as of now, of 18 satellites. Besides the main purpose to detect interferences and support frequency optimization, the data can also be used to locate emitters. Outside the NATO member nations there is currently no project in the final stage of the development, but it will soon be expected when the commercial constellations gain success.

Overall Assessment

The commercial market of Space services is continually emerging due to smaller but more capable technology that can be used in satellites and due to an increased market for commercial Space launch providers. The services based on mega-constellations in SATCOM and ISR already exist, currently in the deployment phase or under development. These offer advantages and threats to NATO, and all military operations. A constant monitoring of the commercial market, identifying usable services and adapting them, as well as the need to find means to ensure that these services are not usable for potential opponents will be a challenge for military and security services in the future.

Sources

Final Report of the NATO STO SCI-309 workshop on 'Opportunities/Implications of Large Scale Commercial Small Satellite Constellations to NATO Operations'.

- **OneWeb®:** https://www.oneweb.world/
- **Starlink®:** https://www.starlink.com/
- **Blackjack®:** https://www.darpa.mil/program/blackjack
- **Planet®:** https://www.planet.com/
- **Assessment on the performance of the Planet constellations:** https://digitalcommons.usu.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=3016&context=smallsat
- **Hawkeye360®:** https://www.he360.com/
- **For all technical specifications of launch vehicle and satellite when not covered by the companies' information:** https://space.skyrocket.de/

Lieutenant Colonel Tim Vasen is a career Intelligence Officer who had several assignments, including Chief Space Intelligence at the GSSAC. Since October 2017 he serves as a Space SME at the JAPCC responsible for Space Support in NATO Operations.

Endnotes

[1] Medium resolution in this case means 3 to 5 metres.

102
$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$
$2x + 4\,dx = 3x^3 + x^2 + 4x + C\Big]_0^3 = 102$

©WHYFRAME/shutterstock

Conflict Termination Criteria

III

Defining How to Win Wars in Space

By Mr Paul Symanski
Space Strategies Center

Introduction

The importance of outer space satellites and their supporting systems cannot be overstated. Their use in the civil, commercial and military worlds to provide communications, weather, navigation, timing, warning and Earth resources monitoring provides major advantages to those who employ the information generated by these systems. However, due to the global reach of these space systems, advantages are provided to both friendly and adversary militaries. Beginning with the use of space systems to support military operations during the Arab-Israeli conflicts, and in Desert Storm, both major and minor players are considering how denial of space capabilities to their adversaries will be a force multiplier on terrestrial battlefields.

As with most military planning, we fight the last wars that are understood well. That is probably the biggest problem outer space warfighters have in conceptualizing how a future conflict might play out. We just have not had that much experience in true space warfare. This makes it very difficult to predict how such combat will actually occur. Much as the concepts of air power were being developed in the 1920s–30s, the true power of space warfare is currently not well understood. To help solve these strategic issues, the author, based on his 46 years experience in missile and space warfare, has determined possible criteria that would define 'winning' or at least 'terminating' the next space war.[1] This is a difficult area to study because traditional terrestrial criteria for peace may involve returning territory, Prisoners of War, and economic restitution, but these do not necessarily apply to space warfare. This article will discuss these possible conflict termination criteria, which are so important to define before any military space operations commence, or any military space war goals are developed (in accordance with Joint Publication 5-0, 'Joint Operation Planning').[2] This is part of the significant contribution of JP-5. Before any warfare planning is initiated, the criteria that would satisfy war aims and goals ('conflict termination criteria') must be defined, and all subsequent planning would then flow from these fundamentals.

The future of outer space warfare is rapidly approaching. There is significant buildup of space warfare capabilities by some major countries who rely on space systems for their defence or perceive that their potential adversaries depend too much on space capabilities to conduct terrestrial warfare. Because of the lack of significant experience by countries in this new military domain, it is difficult to fully understand what the best doctrine, strategies and tactics are to win a future space war. Based on the author's study of military history for the past 55 years, and his direct involvement with space warfare programs for the past 43 years, he has developed general principles by which the next space war will be conducted.

Due to the large distances (tens of thousands of kilometres) between the Earth and military satellites, it is difficult to track and fully image these systems to assess their abilities as potential threats to national security.

In addition, very few countries possess the world-wide space surveillance assets to track movements of suspicious space objects that may be manoeuvring towards critical national assets. Even for those few countries that possess significant space sensor systems, it is very difficult to continuously track satellites that initiate their manoeuvres in areas with no sensor coverage (such as Antarctica). A recent computer simulation by the author showed that 95% of possible space attacks could be completed within 24 hours, which is before any reactions on the ground can be contemplated, approved or completed. A conclusion of this simulation is that, due to the remoteness of space, countries that take actions against an adversary's satellites can do so under a cloud of secrecy, without the general population of the world becoming aware of these aggressive actions. Thus, space warfare adds new, and more subtle rungs on the conflict escalation ladder, where countries can express intent and resolve to their adversaries without necessarily inducing terrestrial conflict.

Possible Space Conflict Termination Criteria

The below is a partial list. See Space Operational Art and Design (SOAD)[3] for a complete list.

1. **The balance of power in space between Red and Blue is sufficient to deter Red from any near-future space attacks for the next 10 years:** Deterrence is always better than complete destruction of all military space capabilities. Especially since it is too difficult to find all adversary offensive capabilities in space.

2. **Red will and ability to continue fighting in space has been severely restricted:** The definition and assessment of Red willingness to continue space attacks will be difficult to determine. This is particularly true due to the obscurity of space events. It is difficult to know

with precision and certainty that satellite outages are attributable to adversary attacks, or natural phenomena. More than likely, small pinprick attacks may still occur that test satellite defences and response times, much like Cold-War airplane incursions in adversary territory tested air defences.

3. **Red on-orbit military space assets supporting current conflict region (Area of Responsibility – AOR) manoeuvring capability reduced by 50 %:** One of the major factors in space wars is satellite manoeuvrability. More than likely, quick military actions in space can only be accomplished by assets in the immediate target region or AOR. This makes orbital refuelling depots and maintenance refuelling satellites critical assets for space superiority.

4. **Red on-orbit ASAT (anti-satellite) capabilities reduced to 10 % remainder (capabilities de-orbited):** Possibly hard to verify, but at least shows the right adversary attitude if known ASAT's are eliminated.

5. **90 % of Red space assets have been visited by Blue inspector satellites and verified in compliance:** At least known adversary space assets can be directly viewed by allied inspector satellites. This may take too much fuel and resources for allied nations to conduct, and hidden adversary ASAT's will always be of concern.

6. **Red provides war reparations for Blue and Gray space systems degraded / destroyed:** Reparations would include both space-based and terrestrial-based systems destroyed by adversary actions during the conflict. Blue may be reluctant to admit damage to hidden space assets, or reveal vulnerabilities of critical assets. These reparations can include Red assets handed over to Blue control, such as communications satellites that can be manoeuvred to new, blue-optimized, orbital slots.

7. **Red develops program to clean up space debris caused by their military actions:** Red may contract with commercial concerns to remove orbital debris in prime orbits, cause by Red military actions, or mistakes.

8. **Red surrenders some of their internationally-assigned geosynchronous orbital position slots:** These orbital locations over key Earth regions are assigned by international bodies, and their loss would be a major blow to the losing side. This may also cause conflicts further down the road that enable adversaries to reclaim their lost 'territory,' much like territorial conflicts on Earth.

9. **Red deactivates / de-orbits all on-orbit space mines:** De-orbiting is best for verification of loss of these assets. One can never be sure that a space weapon has been 'deactivated'. De-orbiting only really works for low Earth orbits, and is not practical for geosynchronous orbits. Sending a satellite into a graveyard geosynchronous orbit does not verify its deactivation, and may only be in sleeper mode, while allowing this potential asset to drift to new targets.

10. **Red does not approach any Blue critical satellites within 100 metres:** This may be problematic, as many satellites and general space junk naturally orbit close to other satellites. It is also an issue on how will this be enforced. Does this allow the offended party to 'shoot down' the offending satellite?

11. **Red does not initiate any new missile launch development programs for 5 years:** Probably easier to verify with overhead space assets than verify whether an object already in space is an ASAT.

12. **Red required to place tracking beacons on all future launched satellites. Blue establishes declaratory policy to immediately neutralize any Red satellites without these tracking beacons for**

the next 10 years: An interesting concept for space traffic control and warning of potential ASAT's.

13. **Red national leader publicly declares his country will no longer pursue space weapon development programs:** Useful, but not terribly verifiable.

14. **Blue and Allied forces achieve absolute control and authority over the orbital space near its satellites, including the ability to maintain freedom of action in, from, and to space, sufficient to sustain mission assurance and deny the same to the adversary and its Red allies during the terrestrial conflict. Space superiority may be localized in time and space, over the immediate AOR, or it may be broad and enduring:** The definition of achieving space superiority, even for a small orbital space, awaits further doctrinal development. The vastness of space allows potential adversaries to create many surprise attacks on space forces that are lulled into thinking they have localized supremacy. Those that win many military battles learn less than those who are the losers of these very same battles.

15. **Blue and Allied space resources are positioned in key jump-off orbital locations (in accordance with future Blue space COA's), have sufficient fuel reserves, have on-board batteries fully charged, and appear to have avoided Red and their allies' space surveillance sensors detection:** This is certainly an ideal that may be difficult to define or achieve.

Conclusion

The future of outer space warfare is upon us, but the theory, doctrine, strategies and tactics are uncertain. A quote from Leon Trotsky is appropriate here: 'You may not be interested in war … but war is interested in you.' Whether you believe in outer space warfare, or are desperately trying to prevent it, conflicts in space will happen nevertheless, as space is way too important to remain a sanctuary while major military conflicts are raging on Earth. Space remains critical to the ultimate outcome of the terrestrial battlefield and may indeed induce fewer casualties by limiting extended conflicts on the ground.

Most importantly, before any major military conflict is initiated on the Earth, a smart adversary would position his space assets at key jumping-off points in space to better enable surprise attacks. If countries invest in Space Situational Awareness (SSA) sensor networks (RADAR and optical) on the ground and in space, they can be pre-warned of impending space attacks, and are then presented with the opportunity to confront the adversary at the United Nations, and possibly prevent the ensuing terrestrial conflict.

Paul S. Szymanski (CMU: M.S. Experimental Physics, '74) for 46 years has been conducting military operations research analyses for the US Department of Defense. He has focused exclusively in outer space program analysis, management and development of space warfare theory, policy, doctrine, strategies, tactics and techniques.

Endnotes

1. Joint Publication 5-0, 'Joint Operation Planning': 'Termination criteria describe the conditions that must exist in the operational environment at the cessation of military operations.'
2. Joint Publication 5-0, 'Joint Operation Planning', https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp5_0_20171606.pdf
3. Space Operational Art and Design (SOAD), https://1drv.ms/x/s!AneNT48wK1EsikKQS1pelSe9R3jx?e=g45b0F

© AIRBUS

Space Connectivity for Air Combat 2040

IV

***By Mr Alain Frizon, Mr Christian Calamarte,
Mr Christian Fournier and Mr Raphaël Ihamouine***
Airbus Defence and Space

Introduction

Connectivity is a key requirement for a Future Combat Air System (FCAS). The amount of secured information to be shared among forces is increasing. Data access and processing capability appear as a game-changer to improve situational awareness leading to decision and action superiority. The Space segment can be seen as a major cornerstone of the End-to-End connectivity for air combat systems. In the following article, the author will highlight the main system requirements to be considered for such a satellite communication system, taking into account service needs from an end-user perspective, and will provide preliminary system design to answer operational forces' needs. A roadmap will also be proposed, with associated technological developments.

Main System Requirements

Airbus is building complex systems for both commercial and military applications and is gathering customers' requirements and needs to define a suitable space aero-connectivity solution. Based on first inputs, the space system shall comply with the following requirements.

Secured high data rates communication services. Security is a key requirement for military forces. Furthermore, the amount of data to be collected by fighter aircraft should increase in the future mainly because of distributed computation, storage (cloud-based approach) and information size (e.g. high-resolution images). Low Probability of Intercept (LPI) and Low Probability of Detection (LPD) capabilities are also requested for the communications services.

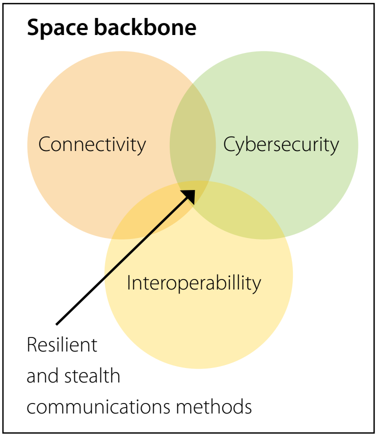


Figure 1: Services requirements of Space system.

Global coverage. Areas for military operations may not be local (limited to a given country). The system shall be able to cover the full Earth, including polar areas.

Near real-time connectivity. Time to receive information and to react are important to achieving and maintaining superior speed of action in combat. The system shall support latency lower than tens of milliseconds.

Reconfiguration capability. Communication systems are evolving (e.g. new air interfaces, new routing concepts). Furthermore, the system shall be able to support coverage, frequency and power flexibility allowing fighters to be covered everywhere, every time. The connectivity system shall be able to be reconfigured in real-time, taking into account the air platform's position and capacity requests during the different operational phases (training, blue areas, red areas)

Multi-customer operations capability is needed to allow joint forces to share connectivity resources in complex military operations.

Preliminary System Design

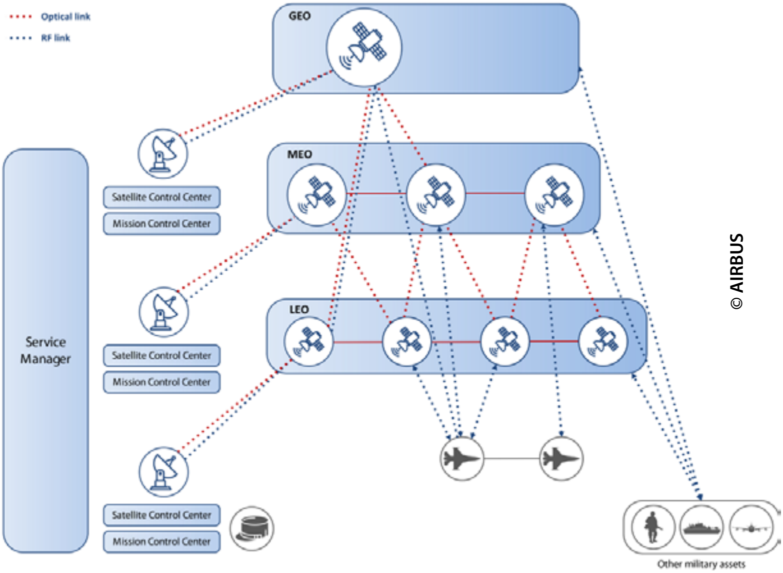
The authors are advocating a Military/Governmental multi-layer constellation system that will allow forces from different countries to share network and radio resources (military & governmental highway connectivity system).

The need for global coverage will basically be fulfilled through a polar constellation (Low Earth Orbit – LEO or Medium Earth Orbit – MEO). Each satellite shall be considered as a network node of a global combat cloud system providing advanced connectivity concepts. The emerging and increasing secured services needs for military aero-connectivity will lead to an increase in satellite performance in the future. This concerns at least three aspects:

- An **increase in system capacity** which can be achieved through investigation of several means such as more beams, more power, more gain or more spectrum (mainly a growing size approach of the space segment) but also through a more efficient satellite architecture and associated resource management.

- An **increase in flexibility** to better serve non-uniform traffic distribution and in particular the hot spots. The flexibility requirements relate to several aspects such as power, coverage and spectrum flexibility.

An **increase in system security** through advanced and reconfigurable air interfaces including ciphering aspects and stealth features (avoid detection from red forces). The space system configuration and monitoring links will be hardened to secure satellite and system operations. Furthermore the space system will be designed to provide communication resiliency (maintain connectivity links in case of system failures – e.g. satellite loss), a key requirement for information war.



© AIRBUS

Figure 2: Multi-layer constellation system for military aero-connectivity.

Main Technologies to be Considered

In that context, several technical trends and new technologies appear of interest for an advanced secured satellite communication system design. At least five of them have been identified as promising concepts:

- Advanced routing with **satellite processors** embedding network routing capabilities, on-board modulation and demodulation. The more recent satellite communication technologies are key elements for information and traffic management – most notably by ensuring on-board autonomy and decision making, and thus optimizing system flexibility and resiliency.

- Advanced **interference management.** Jamming detection, spectrum monitoring and geolocation features are key assets for a secured air connectivity. Space solutions can be used to detect and localize potential threats thanks to advanced processing functions. In addition, use of active antennas can provide a key advantage to suppress interference or jammers and to avoid signal interception (stealth communication).

- Radio and network **reconfiguration capability.** These advanced technologies already deployed in ground systems are candidate solutions to support data links evolution and backward compatibility (e.g. capability to support at the same time new air interfaces as well as current Link-16). User terminal technology and tactical data links may change in the future and software communication techniques, such as Software Defined Radio (SDR) and Software Defined Network (SDN) would be candidate solutions to support these evolutions.

- **Optical inter-satellite links.** Interconnection within all the layers of the satellite communication system will avoid deployment of a ground-based relay and thereby reduce end-to-end latency. A space backbone distributed among the different orbits of the space segment (GEO, MEO, LEO) will provide full and rapid connectivity between several points of the Earth (tactical network with beyond line of sight capability).

- **Dynamic resource management.** Allocating radio and network resources to the end-users in real-time is critical, and a complex resource management system is needed which takes into account end-users' connectivity needs, requested data rates, end-to-end latency, and jitter. Furthermore, in order to reduce the time to access space systems and shared resources among different countries, distribution of resource management functions between space system, next-generation fighters, communication ground equipment, (user terminals, gateways) and several operational centres is foreseen. It may also be possible to consider Artificial Intelligence to provide system resources in real-time (machine-learning concepts). Hybrid Ground, Space, Air resource management system will improve system resource allocation according to user needs and constraints.

Road to Next-generation Connectivity

Next-generation fighters systems are foreseen post-2035 in Europe. Space-based aero-connectivity needs to be fully operational at this time. However an incremental approach could be proposed to secure space system development and to allow current forces to access space connectivity prior to end of this decade. FCAS will be an incremental journey with several planned target architectures to achieve full collaborative combat. First set of capabilities are planned before 2030 preparing for the full FCAS vision with entry into service in 2040 of the New Generation Fighter teaming with Remote Carriers. Proposing technology demonstrators for such satellite system could be considered as a first step of a next-generation space connectivity system.

For instance, a first generation of satellite processor and optical inter-satellite connection could be used to test new air interfaces and network communication techniques prior to the development of a multi-layer Non-Geostationary Satellite Orbit (NGSO) constellation after 2030.

Conclusion

Taking into account requirements to be fulfilled by a Future Combat Air System made of connected manned and unmanned platforms, a space-based system would provide key required capabilities. Connectivity can drastically be improved (up to Beyond Line Of Sight – BLOS) allowing a collaborative air combat solution – forces from several countries sharing the same infrastructure. The vision then is that a detailed system design should be initiated, jointly with aeronautical forces from different countries, to deliver the best technical solution taking into account connectivity specific needs from each party. Space systems can also be used to propose additional services to fighter aircraft such as Intelligence, Surveillance and Reconnaissance (ISR), in addition to aero-connectivity.

Alain Frizon – Airbus Defence and Space – Space Systems – Vice President Defence and Institutional Activities for Telecommunication Systems, covering both programs under development and future programs (e.g. the ones that will support military aeroconnectivity in the next decades).

Christian Calamarte – Airbus Defence and Space – Space Systems – Head of End-to-End telecom system solutions, involved in several geostationary or non-geo stationary satellite communications proposals and projects. In charge of ground segment systems engineering and development for commercial operators and for military applications.

Christian Fournier – Airbus Defence and Space – Space Systems – Program manager within Telecommunication Systems Business Unit, with experience in multiple satellite programs and proposals ranging from Geostationary Earth Orbit (GEO) satellites to Medium Earth Orbit (MEO)constellations and Low Earth Orbit (LEO) mega-constellations.

Raphaël Ihamouine – Airbus Defence and Space – Space Systems – End-to-end network architect working on the definition of the communication logic of future satellite systems, from the network protocols and technologies to the resource management and orchestration functions to be supported.

© NicoElNino/shutterstock

Cyber Threats to Space Systems

V

By Ms Gil Baram and Mr Omree Wechsler
Tel Aviv University

Current Risks and the Role of NATO

A growing reliance of civil and military sectors on space services has led to a growing array of cyber threats to space systems. Amid the growing threat landscape to the space sector, NATO may assume a leading role in coordinating a comprehensive unified framework to address the emerging challenges.

The Weaponization of Space: a Worrisome Trend

Recent years have seen a growing arms-race in space, with nations striving to develop and test offensive space capabilities, and space force-building processes taking place within their militaries:[1] In December 2018, the US Air Force's National Air and Space Intelligence Center published a report, arguing that both China and Russia are developing space weapons.[2] During 2019 the US and France have established dedicated space commands.[3] In March 2019, India conducted its first test of an anti-satellite weapon. The case of India, a country without a history of offensive space activities, illustrates the magnitude of the space arms-race. With space becoming increasingly weaponized, the vulnerabilities of space systems, initially built without basic or sufficient security mechanisms, are becoming both apparent and dangerous, rendering them exposed to cyber threats.

In December 2019, NATO foreign ministers formally declared space as an 'operational domain,' extending the alliance's range from land, sea, air and cyberspace to operations in space. Cyber threats to space systems run the wide range from vulnerabilities in the physical ground and space segments to the satellites' data links and supply chains. As cyber warfare and hybrid threats become the 'weapon of choice' for state and non-state actors, and global economy and daily life grow increasingly dependent on space, space systems may well become the next front in cyber conflict.

This paper suggests a comprehensive approach to this threat landscape, and offers integrated strategic solutions for the cyber defence of space systems.

Existing Cyber Threats to Space Assets

Space systems are usually divided into three technological and operational segments, which are responsible for different functions and are therefore exposed to different cyber threats: the ground segment, the space segment, and the link segment.

The ground segment consists of all the ground elements of space systems and allows command, control and management of the satellite itself and the data arriving from the payload and delivered to the users.[4]

Due to their role in collecting data, the ground stations and terminals are exposed to the threat of cyber espionage from states and non-state actors.

Moreover, the military aspect of satellites and their importance to national security render them prime targets for hostile takeover, disruption and shutdown. Most cyberattacks on the ground segment exploit web vulnerabilities and allow the attacker to lure ground station personnel to download malwares and Trojans to ground stations' computers.[5]

Infiltrating the ground station's network can allow the attackers to access the satellite itself. Hostile access could enable the attacker to execute a Denial of Service (DoS) attack[6] and may involve taking over Industrial Control Systems (ICS) in order to control the satellite and damage it.[7]

The space segment consists of the satellites themselves. Major security gaps within satellites' architecture exist in both old and new satellites. Old satellites with life spans of decades were built with no awareness for cyber security; today, small satellites manufacturers tend to prioritize fast and cheap production, in which the investment in cyber security is perceived as a hurdle.

Cyber threats to space segments usually derive from vulnerabilities in ground stations, in network components, and in the receivers which receive the data from the satellite, thus allowing the attacker to infiltrate to the network and remain undetected. Another threat may involve the introduction of a malware into the satellite's hardware in the supply chain, in order to compromise ground units at a later stage.[8]

Consequences of cyberattacks on satellites could also be aggravated due to the rising connection and use of Internet of Things (IoT) devices. An attack on a communication satellite could cause wide disruptions to communication channels across countries, cause panic, and endanger national security.[9]

The link segment consists of the signal transmission between the satellite and the ground station, as well as between satellites.

The most common threat is GPS jamming. As GPS systems rely on radio signals sent from the satellite in order to determine the location of the users, GPS jammers send signals over the same frequency as the GPS device, in order to override or distort the GPS satellite signals. GPS jammers are widely accessible and cheap to purchase, rendering them available also to poorer state-actors. In November 2018, Russia was suspected of disrupting GPS signals in northern Norway and Finland as the two nations participated in NATO's Trident Juncture exercise.[10] Another type of attack is 'spoofing' – faking signals by broadcasting incorrect GPS signals, structured to resemble genuine ones. Spoofing is harder to carry out than jamming, but if executed effectively, can be much more dangerous, mainly because the victims do not necessarily know that they are being spoofed. According to a 2017 US Maritime Administration report, the GPS systems of at least 20 ships were spoofed, leading the ships 32 kilometres inland to the Gelendzhik Airport in the Black Sea, away from the original destination. The incident raised assumptions among experts that Russia had been experimenting new GPS spoofing techniques as part of its electronic warfare capabilities.[11]

While some experts define jamming and spoofing as physical threats as they involve disrupting or tampering with frequency signalling, an attacker could also intercept unencrypted satellite traffic.

As cyber threats are becoming more substantial, the lack of procedures and policies is hampering efforts to mitigate the threats. However, several solutions have been suggested in recent years.

Threat Response and Mitigation

Mitigating cyber threats to space systems can be divided into technological solutions, which consist of introducing new technologies as well as upgrading existing ones, and policy solutions, which consist of actions and protocols of conduct.

Technological Solutions

In response to the rising cyber threats to space systems, many state agencies, contractors and commercial companies have started developing new technologies, or upgrading existing ones which were not secured by design. In December 2018, Lockheed Martin was awarded a US Air Force contract to modernize GPS ground control systems to support an anti-jamming GPS signal named M-Code, which will allow the Air Force to continue operating the GPS3 constellation with existing ground systems until 2025.[12] In January 2019, NASA announced that it would start testing an open-source Blockchain platform in order to address potential issues of privacy and to prevent spoofing, DoS and other attacks.[13]

In March 2019, Lockheed Martin announced it had developed a new software-defined satellite architecture called SmartSat as a space segment solution, which will enable more capabilities and greater control of in-orbit satellites for ground operators. This architecture is expected to gain operators greater precision in diagnosing problems such as cyber incidents, as well as to allow satellites to back each other up. Operators will also be able to update on-board cyber defences to address new threats.[14]

While the technological solutions being developed will mitigate cyber threats, these tend to address very particular threats. In addition, being provided by a host of different entities, these are difficult to bring together within a unified, coordinated framework. A comprehensive problem requires a comprehensive, unified and systematic policy solution to guide the efforts to protect space assets and services.

Policy Solutions

As the military space sector increasingly relies on commercial technologies, a comprehensive policy solution should focus on commercial space companies and government acquisition contracts. A possible solution which could include both civilian and military space assets and activities would be introducing strict cybersecurity requirements for all components of space systems and their supply chains. A recent example of such requirements is the Cybersecurity Maturity Model Certification (CMMC) which was introduced by the US Department of Defense for all defence contractors, including small vendors.[15] A smart model system which defines different levels of requirements for different products and technologies would demand a high-security level for inherently vulnerable products, without imposing a disproportionate burden on smaller companies. Such a model of cybersecurity standards should be a threshold condition for bidding for government contracts. Additionally, employing strict standards in government contracts is likely to usher in changes across the whole industry, and will therefore help promote the security of commercial and off-the-shelf technologies.

The Role of NATO

NATO as an Alliance was founded for providing a collective defence and cooperative security for its member states. So far, research has suggested that the EU may prove a more suitable entity for promoting new industrial approaches, due to its economic and regulatory authorities.[16] However, NATO has an important role to play in any inclusive comprehensive solution due to the importance of the US. Any industry standards mechanism should include the US space industry, as Europe's production relies heavily on US-produced components and technologies which should endeavour to design for trans-Atlantic interoperability[17]. NATO's leading role as a coordinator and mediator is crucial, as the US is likely to resist any standards mechanism that would push American vendors out of the European space market. NATO's role would therefore derive from its position as a transatlantic alliance with connections to both Europe and the US, and its ability to require common standards and compliance across the alliance. As a unified standards mechanism should be agreed by all member states, NATO could act as a forum for negotiations between its member states and the industry, as well as between Europe and the US. Discussions and consultations as well as further research can take place in conjunction with NATO's Industry Advisory Group (NIAG) and NATO's Industry Cyber Partnership (NCIP), as final results would be incorporated into the NATO Defence Planning Process (NDPP).

Gil Baram is the Head of research at the Yuval Ne'eman workshop for science, technology and security, and a research fellow at the Blavatnik Interdisciplinary Cyber Research Center (ICRC), Tel Aviv University. Her PhD research deals with political attribution and national decision making during cyber conflict.

Omree Wechsler is a senior researcher for cyber security policies and strategy at the Yuval Ne'eman Workshop for Science, Technology and Security in Tel Aviv University. His research fields include information operations, elections cyber security, national cyber strategies, cyber threats on space systems and cyber weapons proliferation.

Endnotes

1. Shapira, Z., & G. Baram, 'The Space Arms Race: Global Trends and State Interests,' Cyber, Intelligence, and Security, vol. 3, no. 2, 2019, pp. 3-5.
2. National Air and Space Intelligence Center, Competing in Space (website), Dec. 2018, pp. 14-15, https://www.airforcemag.com/PDF/DRArchive/Documents/Competing%20in%20Space.pdf (accessed 20 Feb. 2020).

3. Burns, R., 'Trump declares new Space Command key to American defense,' AP News, https://apnews.com/19f021f991844b348dc716f6f8851f7c, 30 Aug. 2019, (accessed 10 Feb. 2020); A. Liptak, 'France's Air Force is getting a space command,' The Verge, https://www.theverge.com/2019/7/13/20693087/france-military-air-force-space-command-president-emmanuel-macron, 13 Jul. 2019, (accessed 10 Feb. 2020).
4. Elbert, B., The satellite communication ground segment and earth station handbook, Artech House, Boston, 2014, pp. 1-3.
5. Bichler, S., 'Mitigating cyber security risk in satellite ground systems', a research report submitted to the faculty in partial fulfillment of the graduation requirements, Apr. 2015, pp. 13-14, https://apps.dtic.mil/dtic/tr/fulltext/u2/1012754.pdf (accessed 10 Feb. 2020).
6. Hutchins, R., 'Cyber Defense of Space Assets', Tufts University, 2016, p. 13, http://www.cs.tufts.edu/comp/116/archive/fall2016/rhutchins.pdf (accessed 10 Feb. 2020).
7. Livingstone, D. & P. Lewis, 'Space, the Final Frontier for Cybersecurity?'. Chatham House, https://www.chathamhouse.org/sites/default/files/publications/research/2016-09-22-space-final-frontier-cybersecurity-livingstone-lewis.pdf, 2016, pp. 22-23, (accessed 11 Feb. 2020).
8. Ibid. 5.
9. Werner, D., 'Who's keeping satellites safe from cyberattacks?'. SpaceNews, https://spacenews.com/whos-keeping-satellites-safe-from-cyberattacks/, 19 Apr. 2017, (accessed 13 Feb. 2020).
10. Woody, C., 'Finland and Norway are telling airline pilots to be ready to fly without GPS, and some think Russia is up to something', Business Insider, https://www.businessinsider.com/finland-norway-tell-pilots-to-fly-without-gps-and-some-blame-russia-2018-11, 9 Nov. 2018, (accessed 13 Feb. 2020).
11. Hambling, D., 'Ships fooled in GPS spoofing attack suggest Russian cyberweapon', NewScientist, https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/,10 Aug. 2017, (accessed 15 Feb. 2020).
12. Erwin, S., 'Air Force to upgrade existing GPS ground control system while next-generation OCX lags.' SpaceNews, https://spacenews.com/air-force-to-upgrade-existing-gps-ground-control-system-while-next-generation-ocx-lags/, 9 Jan. 2019 (accessed 15 Feb. 2020).
13. Kaur, N., 'NASA adopts Blockchain to battle aerospace cyber attacks'. CryptX, https://cryptx.eu.com/nasa-adopts-blockchain-to-battle-aerospace-cyber-attacks/, 19 Feb. 2019, (accessed 15 Feb. 2020); T. Fish, 'NASA embraces bitcoin BLOCKCHAIN tech to battle aerospace cyber attacks'. Express, https://www.express.co.uk/news/science/1073236/nasa-bitcoin-blockchain-cryp-to-cyber-attacks, 16 Jan. 2019, (accessed 15 Feb. 2020).
14. Hill, J., 'Lockheed Martin Accelerates Transition to Software-Defined Space', Via Satellite, https://www.satellitetoday.com/innovation/2019/03/21/lockheed-martin-accelerates-transition-to-software-defined-space/, 21 March 2019, (accessed 15 Feb. 2020).
15. Office of the Under Secretary of Defense for Acquisition & Sustainment. Cybersecurity Maturity Model Certification. https://www.acq.osd.mil/cmmc/ (accessed 2 Jun. 2020).
16. Besch, S., 'The European Commission in EU Defense Industrial Policy,' Carnegie Endowment for International Peace, https://carnegieeurope.eu/2019/10/22/european-commission-in-eu-defense-industrial-policy-pub-80102, Oct. 2019, (accessed 16 Feb. 2020).
17. European Commission, Technologies for European Non-Dependence and Competitiveness (Critical Space Technologies): Guidance Document for Horizon 2020 Work Programme 2018-2020 [website], 26 Oct. 2017, p. 23, https://ec.europa.eu/docsroom/documents/26326/attachments/1/translations/en/renditions/pdf.

© Johan Swanepoel/shutterstock

Space Traffic Management

VI

Impact of Large Constellations on Military Operations in Space

By Mr Marc Becker
DLR Space Administration, Bonn, Germany

As Space Actors Consolidate their Approaches to Space Traffic Management, What is the Role of the Military?

Space Traffic Management (STM) is currently one of the hottest topics in space policy. While a consensual definition of the term is yet to emerge, it becomes increasingly clear that the international community has to find ways to protect space infrastructure and guarantee the safe and sustainable use of outer space in the long run, amid an ever-growing number of actors and objects in the space domain. Often seen as a primarily civilian function, a future STM regime could affect military space operations and space support to operations in a number of ways. Military stakeholders should therefore assess the challenges and opportunities associated with STM and become more engaged in the ongoing debate.

What Will Space Traffic Management Look Like?

The advent of large constellations launched by commercial providers such as SpaceX has created a sense of urgency that has put STM on top of the space policy agenda in recent years: US President Donald Trump issued the first national STM policy (Space Policy Directive-3) in June 2018; the United Nations Committee on the Peaceful Uses of Outer Space approved 21 guidelines for long-term sustainability of space in June 2019; and Germany launched an initiative towards a common European approach on STM during its European Union (EU) Council Presidency in the second semester of 2020, to name only a few recent initiatives.

Academic and technical concepts of STM, however, date back at least to 2006, when the International Academy of Astronautics (IAA) released its first Cosmic Study on Space Traffic Management. The study defined STM as 'the set of technical and regulatory provisions for promoting safe access into outer space, operations in outer space and return from outer space to Earth free from physical or radio-frequency interference'.[1] In broad terms, STM may cover everything from the coordination of satellite manoeuvres and the allocation of frequencies and orbital slots to the prevention and mitigation of space debris.

Following the publication of the IAA study, some in the field have come to expect the emergence of a legally binding international STM regime, similar to how air traffic in the civil aviation domain is governed and controlled today. However, given the slow decision- and law-making processes, especially in times of political stalemate, at the United Nations bodies in charge of governing the uses of outer space, a legally binding STM regime with effective enforcement mechanisms appears extremely unrealistic in the short or medium term. Moreover, an effective STM regime cannot focus exclusively on civilian space activities. Other than in the aviation domain, civilian missions in space cannot be easily distinguished and separated from military missions, which take place at the same time and in the same orbits – even in times of crisis.

A Multifaceted Concept

Recent studies pointed out that regulation is only one of several relevant functions of the STM concept. Other functions include space traffic monitoring and coordination, which will likely continue to be performed on the basis of non-binding standards and cooperation between the different stakeholders.[2] In fact, US Space Policy Directive-3 envisions a binding regulatory approach on the national level only, covering issues like space debris mitigation. Stating that STM shall mean 'the planning, coordination, and on-orbit synchronization of activities to enhance the safety, stability, and sustainability of operations in the space environment,'[3] the policy makes clear that in the global context, the US should focus on establishing best practices and norms of behaviour.

In some ways, the EU seems to move in a similar direction: The European External Action Service launched a public diplomacy initiative aimed at promoting sustainable behaviour in space in 2019. In terms of space monitoring, the EU has consolidated a unique governance model for its operational European Space Surveillance & Tracking (EU SST) capability. A consortium of member states in cooperation with the EU Satellite Centre provides a growing user community of over 60 organizations with free services including collision avoidance, fragmentation and re-entry analysis. Today, the services protect over 130 European satellites from the risk of collision. Under the new EU Space Regulation, EU SST will evolve into a European space situational awareness (SSA) programme, which in the words of EU Commissioner Thierry Breton should be seen 'as the precursor of a European Space Traffic Management system.'[4]

All this indicates that whatever we will call STM in the future will likely consist of a mix of existing activities and programmes, emerging norms and best practices, and some degree of national (and perhaps also international) regulation. All relevant stakeholders – government and industry alike – are therefore well advised to shape the ongoing debate on STM according to their interests.

While military actors may not be particularly interested in how exactly civil and commercial space activities will be coordinated in the future, it is clear that they will continue to play a significant role in the operational SSA capabilities that are needed to underpin any form of STM, whether for general traffic monitoring or for verifying compliance with norms and regulations. Indeed, while US Space Policy Directive-3 envisions a transfer of basic STM services such as collision avoidance support to the US Department of Commerce, the authoritative catalogue of space objects – including those that are classified – will remain with the Department of Defense, which operates the US Space Surveillance Network. Similarly, Europe's civil EU SST framework is based on a functional specialisation of the participating member states, which retain full control over the contributing radars, telescopes, and lasers as some of these sensors are operated by militaries and provide sensitive data.

Essential Military Contributions

Precisely because military capabilities and contributions will continue to be essential for any form of STM, it makes sense from a military perspective to assess how a changing environment may affect military space operations and space support to operations in the future. If the projected unprecedented launch of tens of thousands additional satellites over the next ten years materializes, more precise SSA data will be needed to manage the increased traffic and avoid disastrous collisions in orbit. The number of close conjunctions between objects in space is already remarkable today: In 2018 alone, the US military issued roughly nine million conjunction notifications to satellite owners and operators.[5]

As the number of close conjunctions continues to rise, we may be starting to see a paradigm shift towards ever more transparency in the space domain. In fact, the US government recently started to provide orbital elements for a number of previously classified objects through its public catalogue at space-track.org. However, SSA experts have pointed out that some 500 objects remain restricted for national security reasons.[6]

In the coming years, there could be an incentive to declassify additional data in the interest of safety of flight. After all, it is difficult to disguise some objects without increasing the risk of collision for all, especially when the respective orbits get much more congested. Operators of military satellites therefore will have to reconcile new transparency requirements and national security constraints in their approach to SSA data sharing. As more and more countries and even commercial providers develop their own sensor capabilities, it becomes increasingly likely that such data will be available elsewhere, perhaps beyond the respective state's control. Amateur astronomers have little difficulty in tracking the trajectories of many classified satellites today, and so it won't be a problem for potential adversaries either. However, if Western militaries started to publish precise and timely orbital information of their reconnaissance satellites, for instance, this would allow a broader audience to infer spacecraft capabilities, operational procedures, and mission objectives. In their approach to STM, militaries will therefore have to strike a balance between promoting space safety and protecting legitimate security interests, which for example could be reflected in the quality and time accuracy of the data released for certain objects.

Considering Challenges and Opportunities of Space Traffic Management

STM standards and norms could be another area in which Western militaries will need to sharpen their approach, even if a future STM regime may largely grant freedom of action for military space activities. In a more crowded orbital environment, particularly in Low Earth Orbit (LEO), commercial spacecraft could increasingly get in the way of military satellites. Operating and maintaining the planned mega-constellations will require much more frequent launches, as well as regular orbit raising and re-entry manoeuvres that cross LEO regions which are commonly used by reconnaissance and other national security satellites.

Operators of military spacecraft need to carefully analyse what the increase in traffic will mean for military space operations and space support to operations. For example, one can imagine a situation in which the availability of geospatial intelligence of a crisis region could be delayed as reconnaissance satellites need to coordinate their manoeuvres with commercial operators of mega-constellations and are forced to prioritize collision avoidance manoeuvres over operational needs. National security entities will have to include such potential delays in their calculations.

While emerging STM norms and best practices could place new burdens on military operators, they also have a lot to gain from rules of the road in the space domain. Once established, compliance with norms of behaviour in cases of close conjunctions between space objects can be more easily verified as more SSA data becomes available. Consequently, any indication of non-compliance will help to single out potentially hostile behaviour in orbit.[7]

Despite little progress in recent years in the international debate on norms of responsible behaviour in space, military actors should continue to push for such norms. Western militaries in particular can bring their long-standing operational expertise to the discussion table, from which best practices can be derived as a starting point for norm development.

Even though many of the exact characteristics of a future STM regime remain murky, now is a good time for all stakeholders including militaries to analyse the challenges and opportunities associated with different scenarios of how STM could play out. This will allow them to prepare early for future developments and enable them to get more closely involved in the debate where their interests are affected.

Marc Becker is a policy officer in the department of space situational awareness at DLR Space Administration in Bonn, Germany. He chairs the European Space Surveillance & Tracking (EU SST) Consortium's internal Security Committee. Mr Becker studied international affairs and security at the Hertie School of Governance and Georgetown University.

Endnotes

1. Contant-Jorgenson, C., P. Lála, and K.-U. Schrogl. Cosmic Study on Space Traffic Management, Paris: International Academy of Astronautics, 2006: p. 10.
2. Moranta, S., T. Hrozensky, and M. Dvoracek. Towards a European Approach to Space Traffic Management, Vienna: European Space Policy Institute, 2020: p. 8.
3. White House, 'Presidential Memoranda, Space Policy Directive – 3, National Space Traffic Management Policy'. Jun. 2018. Available from https://www.whitehouse.gov/presidential-actions/space-policy-directive-3-national-space-traffic-management-policy; accessed 25 Feb. 2020.
4. European Commission, 'Closing Speech by Commissioner Thierry Breton, 12th Annual Space Conference'. 22 Jan. 2020. Available from https://ec.europa.eu/commission/commissioners/2019-2024/breton/announcements/12th-annual-space-conference-closing-speech_en, accessed 25 Feb. 2020.
5. de Selding, P.B., 'U.S. Space Surveillance Unit: Few Issues with SpaceX Starlink; Universities are Toughest Cubesat Owners for Us'. In Space Intel Report, 17 Jul. 2019. Available from https://www.spaceintelreport.com/u-s-space-surveillance-unit-few-issues-with-spacex-starlink-universities-are-toughest-cubesat-owners-for-us, accessed 20 Feb. 2020.
6. Kelso, T.S., 'Keynote Address, 6th Space Traffic Management Conference'. In CelesTrak, 20 Feb. 2020. Available from https://celestrak.com/publications/STM/2020, accessed 25 Feb. 2020.
7. Schaffer, A. M., 'The Role of Space Norms in Protection and Defense', Joint Forces Quarterly, no. 87 (2017): pp. 88-92.

© 3rieart/shutterstock

Assured Access to Space

VII

Strengthening NATO's Space Deterrence Strategy

By Dr John Klein and Mr Nickolas Boensch

While the role of space in NATO's operations has traditionally received much less attention than the alliance's other domain responsibilities, NATO's recent attention to space issues is a welcome change. The NATO Parliamentary Assembly stresses that 'NATO's collective defence and economic prosperity rely on space-based infrastructure, and an attack on the space assets of one Ally would impact the security of all. As such, NATO needs a whole-of-alliance approach to protect its interests in space to enhance resilience and deter any threat to its space-based capabilities.'[1] This sentiment was followed by NATO's first space policy, announced June 2019, which emphasized vigilance and resiliency in space in the face of increasing threats targeting the NATO's access to space.[2] Perhaps most significant is NATO's acknowledgement of space as an operational domain, alongside the air, land, sea, and cyberspace domains.[3] Following these developments, NATO serves as the preeminent forum to develop a multi-lateral space deterrence strategy. A strengthened NATO space deterrence strategy will help convey the futility of aggressive actions in space, thereby promoting assured access to space for the betterment of the international community.

Deterrence Theory for the Space Domain

Because NATO member states derive strategic advantages from satellites and potential rivals may seek to deny this advantage, the concept of space deterrence is relevant. Space deterrence refers to persuading a potential enemy that it is in its own interests to avoid certain courses of activity in, through, or from space.

One of the most essential distinctions in deterrence theory is between deterrence by punishment and by denial.[4] Deterrence by punishment concerns the threat of credible and potentially overwhelming force or other retaliatory action against any would-be adversary to discourage potential aggressors from conducting hostile actions. Deterrence by denial refers to deterring an adversary by presenting a credible capability to prevent it from achieving the potential gains adequate to motivate the action.[5] Deterrence by punishment and denial each have relevance for the space domain.

Deterrence by punishment is one part of the broader US space strategy. The 2017 US National Security Strategy conveys that harmful interference or attacks targeting US satellites will be met with a deliberate response in the time, place, manner, and domain of its choosing.[6] Given the strategic importance of space capabilities in NATO's ability to defend itself, the alliance has the opportunity to institute similar declarations. This may include NATO clearly conveying the capability and credibility to respond to an attack against a member state's space systems and communicating the specific behaviour to be discouraged.[7] The alliance may also decide under what conditions an attack in space would trigger the organization's Article 5 provisions on collective defence.

A key challenge for NATO instituting a space deterrence by punishment strategy is the concern that aggression in space would not rise to levels that warrant a terrestrial military response. The non-casualty generating effects of space actions does not preclude a deterrent effect. Article 2(4) of the U.N. Charter describes the need to refrain from the threat or use of force against a state's territorial integrity, which may be interpreted as a state's physical property. For this reason, self-defence and retaliatory threats to deter a potential armed attack against a NATO member's satellites are appropriate and justified.

A deterrence by denial strategy for space seeks to frustrate or complicate the adversary's plans by introducing greater costs and reducing associated benefit. Over the past several years, there has been greater emphasis on the role of deterrence by denial in US space strategy. The same could hold for NATO space strategy. Rather than threatening retaliation against the aggressor's satellites or terrestrial assets, a deterrence by denial space strategy conveys the futility of attacking NATO members' satellites.[8]

Much of a deterrence by denial approach necessitates preparing for potential conflict during peacetime. This presents an opportunity for NATO to expand its deterrent effect through peacetime military space preparedness.[9] Military space preparations preceding a conflict may include hardening against cyber threats and signal jamming, protecting remote sensing satellites from dazzling lasers, increasing the mobility of satellites, and distributing capability across a number of satellites.[10] One method of frustrating an adversary's plans may include training military forces to fight under degraded conditions in space, thereby depriving potential aggressors the appeal of attacking satellites.[11] These preparations can have significant deterrent effect and may convince a potential aggressor that the prospects for success are too costly and result in little benefit.

Strengthening NATO's Space Deterrence Strategy

In many areas, NATO is ideally positioned to bolster deterrence in space through its cooperative alliance. Strengthened alliance activities and coordinated military space preparedness can persuade a potential adversary to avoid aggressive behaviour in space.

A NATO space strategy should create a strategic performance and deterrent effect that is stronger than the sum of the individual parts. Despite the preference for national space assets, expanded multilateral space deterrence discussions within NATO can emphasize the cooperative impact of these assets on the alliance.[12] The alliance's space deterrent would be enhanced if member states can complement and supplement each other's own capabilities, through data-sharing agreements, interoperability, or even by assisting in the reconstitution of lost space capabilities. Increasing military preparedness of space assets as a part of a deterrence by denial strategy can become a financial burden to a state attempting to make preparations unilaterally.[13] By providing an organizational structure where members can leverage assets across the alliance, NATO can provide a significant deterrent effect at a lower cost than the sum of member states acting individually.

While collective security has its dilemmas terrestrially at times, space may be the ideal domain for such an agreement. Because of the character of space warfare and its unique geographic attributes, states and stakeholders outside of the immediate conflict may have their satellites affected negatively should deterrence fail and conflict ensue. NATO members that may not normally feel threatened by an aggressor's actions may have their space security worsened by orbital debris from kinetic attacks or by indiscriminate radio frequency jamming. Moreover, the state subject to an attack may provide a global or multinational space-derived service, such as from the US Global Position System or European Galileo satellites, which if attacked could potentially draw other members reliant on this service into the conflict against the aggressor.[14] Should NATO strengthen its focus on space deterrence, an aggressor may be hesitant to attack space systems because it may have to contend with a unified and coordinated NATO response.[15]

Recommended Near-Term Actions

Given the significant benefits of a strengthened NATO space deterrence strategy, recommendations include:

1. **Elevate the role of space in traditional military exercises and wargames, collaborate with member states on indigenous space wargame efforts, and establish space-centric wargames and military exercises within NATO.** As part of this recommended action, NATO member states should leverage lessons on space integration from previous Trident Juncture and Defender military exercises and expand these exercises to reflect space's status as an operational domain. NATO and its member states should also continue to participate in the US Space Flag exercise and Schriever Wargame. Through the expertise of its Joint Warfare Centre, NATO should develop its own space wargames to educate and train member states' space professionals and use these events as an opportunity to communicate the effects of space warfare to the NATO command staff.

2. **Incorporate the capabilities and services of the commercial sector into space deterrence strategies, planning, and military exercises whenever possible, recognizing the crucial role of commercial space sector in conveying the futility of aggressive action against a member state's satellites.** The commercial sector (satellite operators, launch service providers, and manufacturing supply base) should play a significant role in NATO's space deterrence strategy. Having a broad framework that extensively uses the commercial sector will help promote a deterrence by denial of benefit strategy, thereby assuring access to space during times of hostilities.

3. **Create a publicly available NATO space strategy that explicitly covers NATO's space deterrence strategy and describes how the**

alliance will work together to assure access to space. Recently, several NATO members have produced new space strategies and are in the process of reorganizing their space forces to meet the changing threat environment. Because of the shared space security interests, NATO should host discussions between member states to align national strategies with NATO's multilateral space strategy and objectives to avoid duplication and realize efficiencies.

4. **Include space as a topic in future discussions on countering, responding to, and deterring hybrid threats and military activities that fall short of war.** Just as potential adversaries seek ways to achieve relative gains without triggering escalation within terrestrial domain, this condition is replicated in space as well. This includes Russia's proximity and inspection activities on French and US national security satellites.[16] Including space strategies on how to counter and deter this behaviour, along with its terrestrial analogues, will help ensure NATO has a relevant strategy to defend its member states' space interests.

Space imparts many strategic benefits that enable NATO's military and non-military activities. While NATO has indeed taken meaningful steps toward a more robust space deterrence strategy by acknowledging space as an operational domain, much more needs to be done. The alliance is well-positioned to promote assured access to space among its members, take a leadership role in developing a multi-lateral space deterrence strategy, and carry out a strategy for the betterment of all NATO member states. Space has a critical role in international security because all the world's major powers are also great space powers that seek to broaden their use of space. Given the lessons of history, the strategic effect derived from space-based capabilities will not remain unchallenged. A strengthened NATO space deterrence strategy can play an important role in ensuring peace and stability within the space domain.

Dr John J. Klein is a Senior Fellow and Strategist at Falcon Research, Inc., and Adjunct Professor at George Washington University's Space Policy Institute. He is the author of the books Understanding Space Strategy: The Art of War in Space (2019) and Space Warfare: Strategy, Principles and Policy (2006).

Nickolas J. Boensch is a Program Analyst at Bryce Space and Technology.

Endnotes

[1] NATO Parliamentary Assembly, 'The Space Domain and Allied Defence', (Oct. 2017), https://www.natopa.int/download-file?filename=sites/default/files/2017-11/2017%20-%20162%20DSCFC%2017%20E%20rev%201%20fin%20-%20SPACE%20-%20MOON%20REPORT.pdf.

[2] 'Space is essential to NATO's defence and deterrence', NATO, 14 Oct. 2019, https://www.nato.int/cps/en/natohq/news_169643.htm.

[3] Banks, Martin., 'NATO names space as an 'operational domain,' but without plans to weaponize it', Defense News, 20 Nov. 2019, https://www.defensenews.com/smr/nato-2020-defined/2019/11/20/nato-names-space-as-an-operational-domain-but-without-plans-to-weaponize-it/.

[4] Snyder, G. Deterrence and Defense, Princeton: Princeton University Press, 1961.

[5] Krepinevich A and Martinage R, 'Dissuasion Strategy', Center for Strategic and Budgetary Assessments (2008), https://csbaonline.org/research/publications/dissuasion-strategy.

[6] The National Security Strategy of the United States of America, The White House, 2017.

[7] Morgan P. Deterrence: A Conceptual Analysis, Beverly Hills: Sage Publications, 1977.

[8] Vedda J, Hays P, 'Major Policy Issues in Evolving Global Space Operations', The Mitchell Institute for Aerospace Studies (2017).

[9] 'Space Domain Mission Assurance: A Resilience Taxonomy', Office of the Assistant Secretary of Defense for Homeland Defense (2015), http://policy.defense.gov/Portals/11/Space%20Policy/ResilienceTaxonomyWhitePaperFinal.pdf?ver=2016-12-27- 131828-623.

[10] Kueter J and Sheldon J. 'An Investment Strategy for National Security Space', The Heritage Foundation, Special Report No. 129, (2013).

[11] Harrison R, Jackson D, Shackelford C, 'Space Deterrence: The Delicate Balance of Risk', Space and Defense 3, no. 1 (2009): p. 1-30.

[12] Europe, Space and Defence: From 'Space for Defence' to 'Defence of Space', European Space Policy Institute, ESPI Report 72, (2020).

[13] Coletta D, 'Space and Deterrence', Astropolitics 7 no. 3 (2009): p. 171-192.

[14] Harrison R, Jackson D, Shackelford C, 'Space Deterrence: The Delicate Balance of Risk', Space and Defense 3 no. 1 (2009): 1-30.

[15] Sheldon J, 'Space Power and Deterrence: Are We Serious?', The George C. Marshall Institute, Policy Outlook, (2008).

[16] Leicester J, Mehta A, ''Espionage:' French defense head charges Russia of dangerous games in space', Defense News, 7 Sep. 2018, https://www.defensenews.com/space/2018/09/07/espionage-french-defense-head-charges-russia-of-dangerous-games-in-space/; Erwin S, 'Raymond calls out Russia for 'threatening behavior' in outer space', Spacenews, 10 Feb. 2020, https://spacenews.com/raymond-calls-out-russia-for-threatening-behavior-in-outer-space/.

© NASA Earth Observatory image / Joshua Stevens

When Geopolitics Meets Technologies

VIII

Space Development and Changes on Traditional Power's Balance

By Mrs Victoria Valdivia Cerda
Chilean Air Force

Space Development in the South America Region

South America as a geographical region and the individual nations, have traditionally been exploited by global powers because of their global position and abundant natural resources. However, South America is also challenged because it has not been able to develop a regional governance structure due to difficulties with regards to integration and collaborations between the various countries. These difficulties originate from unresolved territorial conflicts and the challenges from generalizations that all the countries remain in the category of 'undeveloping' with one huge heterogeneous population.

At the beginning of the Space Race, space activities in South America, remained under national control, being part of international organizations as The Committee for Peaceful Uses of Outer Space (COPUOS), signatories of Corpus Iuris Spatialis and then part of the Office of Outer Space Affairs of United Nations (UNOOSA). Also, due to previous historic interactions, there is evidence of early cooperation with Space Powers.[1]

In the 1980s, Chile started with the development of indigenous space capabilities. This was accomplished in the context of national control, specifically Chile's authoritarian government and its links to the army. The vision at the government level involved the understanding of outer space as a new domain for military operations, and a way to reach local superiority and not be vulnerable in a potential local conflict.[2]

With the end of 'pax Americana era' in the 2001, and the decrease of entry barriers to space technology, the region began to acquire space capabilities[3], but the technological gap (product of technology evolution) revealed the necessity to cooperate with a 'Space Power'[4] in order to acquire knowledge, technology and experience. However, the technological transference, even the acquisition of technological systems and knowledge, involved the mechanisms of international cooperation. The relevant element for the analysis on space development within the region remains the formulation of the normative infrastructure. This meant space policies, laws, and infrastructure were somewhat organically created, because of the defined goals and vision of the State concerning space development and was a sign of how the region moved into the new century.

Why South America Remains a Relevant Geographical Zone

Throughout more than 60 years of development, Space-based capabilities have demonstrated their great influence in geopolitical processes through a direct relation between the increase of human dependence on Space-related technologies and the globalization of communications and information sharing capabilities. In this sense, Space infrastructure becomes critical to the development of day to day activities around the world; to include planning for economic development, urban growth, and military mobilization.

Space-related technologies have allowed for more effective action from the central planning of nations, involving the decrease of expenditures and allowing for a more rational public investment. With a better use of public resources, nations have been able to re-distribute public expenditures and begin to develop solutions to significant public challenges related to social infrastructure and the resilience of society. That is why nations look to Space, and over time Space has been increasingly recognized as a domain and a natural extension of international system[5].

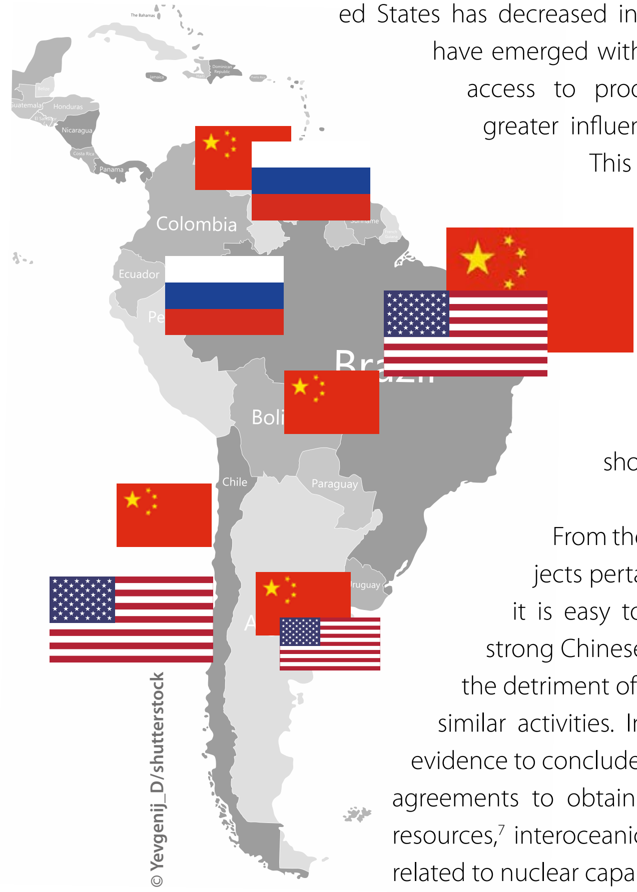
Space, and the ability to operate therein with a human presence, are deeply linked with the emergence of new international powers. These rising powers have looked to specific geographical zones, such as South America, which are critical for their Space programs[6].

The absence of an existing Space infrastructure in the southern hemisphere, created an opportunity and competition among Space Powers to secure ground infrastructure to support their Space missions and requirements, usually through traditional mechanisms of collaboration with host nations. In this new era of Space Powers, South America is highlighted in importance because the geographical position of the region allows the tracking of satellites through their orbits over the southern hemisphere, improving mission safety and security. In addition, the region contains natural resources crucial to advanced technologies which are of keen interest for Space Powers.

This new era of geopolitical interest represents an opportunity for South American Nations to increase their own national power and prestige through Space activities. These nations have found a chance to reduce the technology gap by gaining access to Space-related capabilities in order to improve their national infrastructures through collaboration and trade with Space Powers.

As South America enters a process of acquisition of Space technology based upon their individual national interests, most of them have adopted space policies, laws, and organic infrastructure created to host the newly acquired capabilities. However, as the influence of United States has decreased in the region, other nations have emerged with offers of agreements and access to products that provide them greater influence across South America. This shift in influence by global power within South America, driven by Space-related technologies and capabilities, has carried over into other elements of influence and cooperation as shown in the adjacent picture.

From the image, which depicts projects pertaining to space capabilities, it is easy to conclude that there is a strong Chinese presence in the region, to the detriment of United States' influence on similar activities. In addition, there is strong evidence to conclude China has leveraged these agreements to obtain access to other strategic resources,[7] interoceanic trade, and developments related to nuclear capabilities.



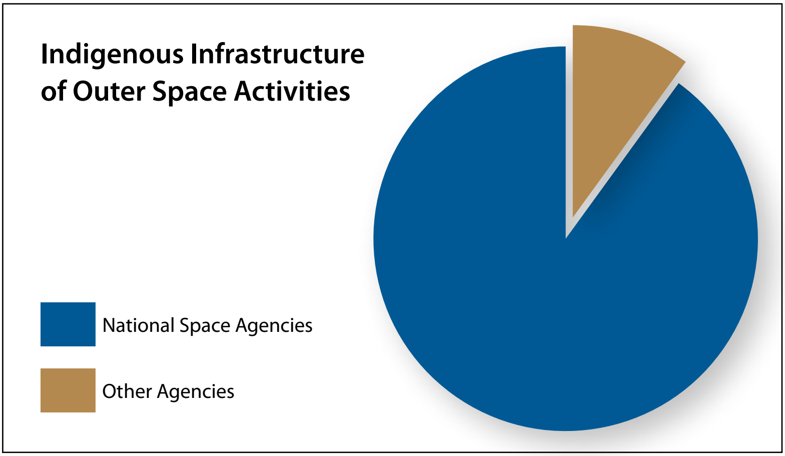
© Yevgenij_D/shutterstock

The increasing presence of Chinese interests in South America related to Space matters also has revealed deep connections to military Space activities, this form of technological transfer could have significant impact on the balance of power within the region, which can be traced through the formulation of Space-related policies in the various nations.

Space Policy Formulation: Signs of Changes in Powers Balance Emerge of Old Geoconflicts

In order to capture the development of the region in terms of changes to power balances, this paper will be focused on a review of six study cases: Argentina, Brazil, Bolivia, Chile, Perú, and Venezuela. The selection of these cases considered the logic of non-probabilistic selection utilizing the following criteria:

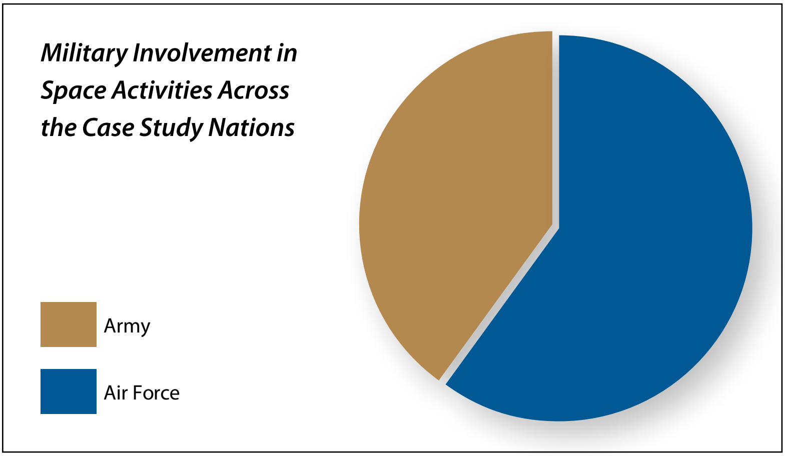
A States in possession of at least one Space system under national administration for the last eight years.
B States with at least one public instrument to regulate national Space activities.
C States with at least one active territorial dispute.
D States that are members of geographical zone of South America.
E States with at least one reserve of geostrategic natural resources.


Indigenous Infrastructure of Outer Space Activities

At a macro level, there is strong evidence that in all of these case studies, Space activities evinced a high level of national participation. This is shown by the activity being conducted by an organization dependent on central government administration, such as a nationally controlled Space Agency.

With regards to the nations' purposes for engaging in Space activities, in case studies, the nations relied upon a public policy instrument that focused Space activities into one of the following terms: country development, improvement of their position within the international order, or improvements related to some national planning priorities[8]. This is relevant because it reveals the intentional increase of capabilities from the nations based on the incorporation of space technology[9]. Also, there is no evidence of the inclusion of'peaceful uses'terminology into the formulation of public policies. Instead, the principle of good faith[10] of any actor is accomplished through international compromises acquired by the corpus Iuris Spatialis.

Based on an analysis of indigenous infrastructures of existing Space organizations, with some form of active space capabilities, the evidence shows that in the majority of cases militaries are involve in these activities,



in some cases exerting significant influence on the processes and activities. This also means national Space capabilities within South America are often considered to be dual-use capabilities, regardless if the principal declared mission is for civil purposes. This link with militaries indicates that Space systems contribute to defence sector and are susceptible to being considered as weapon systems.

Finally, as the evidence showed Space capability links with the defence sector, the research continued for evidence of policies formulated related to supporting these activities. In each case, there is ample evidence of formulation of these types of policies related to Space systems. The result in each case study, therefore, is formulation of employment concepts and modernization of militaries in order to incorporate Space-based technology into their daily duties. Additional evidence for this assertion is found in evidence of Space capability and/or technology-related training of military forces.

At this point, South America may seem like any other group of nations with regards to Space development. Which implies that regardless of the stage of national development of indigenous space capabilities, the relevant issue is how to incorporate Space technology into the defence sector. With a focus on reaching national goals and reducing the technological gaps that increase the vulnerability of those nations bereft of these technologies during potential future conflicts.

Foresight and Challenges for Peaceful Uses of Outer Space

The study of normative policies and technology acquisition of countries in South America has reveal that modernization of associated battlefield capabilities is not only given by the indigenous development of those capabilities, but also is influenced by international players. In this sense, there is no evidence that the status quo of space activities will remain if the international situation shifts from traditional powers. In the case study, there is a strong tendency to move from traditional relationship in search of new allies, motivated by increased incentives for collaboration in order to acquire more advanced technological components which that can have a positive impact in their domestic power. Regardless of previous relationships, the evidence shows that the technological cooperation with actors, like China has improved the Space programs within the region. Even more, there are countries that have a Space program derived entirely from collaboration with China.[11]

Specifically, countries in the region have demonstrated the ability to identify Space-based technology as dual-use assets, improving all their instruments of national power. Brazil and Bolivia, in particular, are more resilient in the face of new hazards and security challenges than either were just ten years ago.

Admittedly, not all states reach the same level of influence within their respective regions or within the larger international community. There are some nations, such as Brazil and Argentina, that are seeking a position of regional leadership, and there are also cases, like Bolivia, in which the focus is on gaining the upper-hand in small-scale cross-border conflicts.

Regardless of the level of influence sought, the modernization of one nation into new domains (such as Space) changes the terms of engagement and stimulates their neighbours to ensure what they see as the proper balance the power. Due to security implications exacerbated by active territorial controversies, these changes in power dynamics can involve all nations in the region into an escalation of Space Power development.

From the outside looking in, this dynamic in South America can be seen is profitable to new actors with global aspirations, such as China, because of perceived lower associated costs. These actors believe the shifting power dynamics allow them easier access to influence a new region, access made easier by the decline of traditional cultural norms and other indicators of soft power of traditional powers. At the same time, more influence in the region means more opportunities to access strategic geographical zones thus improving their own capabilities, like command and control of lunar missions, and contributing to their national goals.

Finally, based on traditional geopolitical dynamics, the collaboration between some South American Nations and China, as it pertains to Space, should be seen as a short-term relationship. This is because the origin of these collaborations is linked to the reduction of the technology gap in these nations, so they might increase their national power. This means that in the long-term, in order to maintain these relationships, China will need to provide additional stimulus to indigenous Space capability development in order to maintain a relationship. All the while, there are new Space Powers emerging who might offer a better deal, with lower costs with regards to exploitation of natural resources (that will be demanded by their own space industries process) and more acceptable terms with regard to issues related to national sovereignty.

Ultimately, the use of Space, and its associated technologies, for any nations remains focused on national goals and desires with regards to the needs associated with a Space Program. The Space domain is like any other domain, in that how it is seen and utilized has an impact on National Power, because it is linked to social dynamics between society and perceived technological benefits. Changes in social dynamics, including those from small to large scale conflicts, will be increasingly affected by space activities and eventually multi-domain operations as technological advances are realized.

The existence of states without indigenous Space capability is only evidence of the economic gap that exists in some regions, but should not be confused with a lack of interest of those nations in realizing the benefits from space capabilities in order to increase their respective national power, particularly through military applications, as these portend security and reduce uncertainty in potential future conflicts.

Victoria Valdivia Cerda holds a Master's degree in International Studies and has a Political Scientist postgraduate in Strategic Intelligence. Conducted research on Center for Strategic Studies on Aerospace Affairs-Chilean Air Force at the National Academy of Political and Strategical Studies. She is currently employed as a Policy Advisor on Space Affairs at the General Staff of the Chilean Air Force.

Endnotes

1. Only in two cases (Brazil and Argentina), the space era began with the development of space technology, also they both have declared their origin of space activities as a key asset to their change into the International Order, searching the increment of National Power.
2. In addition, there is early evidence of space activity in Peru in the same decade, at least at the level of plans and policies formulation.
3. This conduct is explained in the context that the end of pax Americana era, and the end of United States hegemony increased uncertainty levels in the international dimension. It is possible to change hegemon, so it is possible to change the position on the International Order, putting on the edge old geopolitical conflicts and prompting States to modernize their capabilities in order to add new elements in the definition of National Power.
4. Space Power will be understood as those states that by virtue of their Space capabilities have influence in the international system and on other state actors.
5. TESIS: 1. Valdivia, Victoria. 'El espacio ultraterrestre como factor para el desarrollo y su presencia en la Política Internacional. La situación de Chile y América Latina. Hacia la profundización de una política espacial con perspectiva estratégica para nuestro país'. Tesis para optar al grado de Magíster en Estudios Internacionales, Universidad de Santiago de Chile, 2016.
6. BOOK: 1. Al Rondhan, Nayef. 'Meta-Geopolitics of Outer Space: An Analysis of Space Power, Security and Governance', United Kingdom, edited by Palgrave-McMillan, 2012.
7. As with the element tantalum, high-value geostrategic mineral for the development of the technology industry, a key component in the development of high technology industry.
8. Like the case of Argentina and Brazil both define their goals in outer space activities in order to improve their own position in the International Order. In the case of Chile, space policy defines the national interest in order to improve national capabilities for national development (linked to the increase of national capabilities and the National Power because it means an increase in economic, political, diplomatic, social and technological Power).
9. Ibid. 5.
10. Principle of good faith refers to that principle of international relations by means of which it is assumed that the conduct of a state will be in the terms of public international law.
11. Like the case of Bolivia. In this case all space infrastructure is product of cooperation with China. It includes: space platforms, ground-based systems and instruction´s programs.

[M] Earth: © **Johan Swanepoel/shutterstock**, Satelite: © **Northrop Grumman Corporation**

Space Situational Awareness

IX

The Challenges of Space Security Policy in Poland

By Prof Małgorzata Polkowska
University of War Studies, Poland

Safety and security have always played an essential role in Poland's state strategy and policy. Although the activities related to Space Situational Awareness (SSA) have been present in Poland from the beginning of the space era, they had been practically constrained to Research and Development (R&D) only. The idea of building-up SSA operational capabilities at the European level has received firm national support from its beginning. Poland, as a European Union Member, has not only advocated for the European Space Surveillance and Tracking programme but also joined it in 2018[1]. The transition from R&D to the operational domain was, and is, a tedious process. In particular it was linked with creation of the Polish Space Agency (POLSA)[2], declaration of the National Space Strategy (2016), and the creation of POLSA's SSA dedicated structure (2017)[3] together with the National SSA Operational Centre[4].

The activities of POLSA were (under the act from 2014) under the auspices of the President of the Council of Ministers. As of these writings, due to modification and update of the procederes, the Agency is under auspices of the Ministry of Development. The POLSA Council consists of representatives of the government, one from each administration and four representatives of scientists and industry with recognized achievements in research or business who are chosen based on their knowledge competence in areas concerning POLSA activities. One of the main areas of POLSA activities is international cooperation. POLSA is committed to multilateral cooperation in the framework of the European Space Agency (ESA) and the European Union (EU). POLSA supports especially Polish actors who apply to the space programs. They have already started efforts to integrate the national industrial sector in projects implemented by the European Organization for the Exploitation of Meteorological Satellites (EUMETSAT). POLSA also provides active bilateral cooperation with ESA Member States, the EU and other countries, primarily in the field of space exploration.

POLSA supports the Polish space sector and facilitates exchanges, by organizing competitions for advisory services. The entities receive professional support in the form of consultation with experts. Entrepreneurial subject matter experts (SME) receive support in applying to competitions organized by the European Space Agency. POLSA activities aim at contributing to the growth of innovation and competitiveness of Polish companies in the space sector. POLSA encourages the involvement of high-tech or Information Technology (IT) operators in the space industry, and it also promotes solutions supporting the Polish state administration at central and local government levels. These result in enhanced efficiency of the administrative work by using everyday services based on satellite data and satellite technology, including earth observation, navigation and telecommunications. With regard to R&D, POLSA supports the Polish scientific institutions and companies who are active in R&D in the field of fundraising for scientific and industrial research. POLSA assists in conducting work on space applications and space technology development.

In addition, POLSA carries out educational activities in the field of popularization of knowledge of space research at secondary education and high school in Poland. It covers the subject of space engineering and astronomy, as well as initiates and supports with its expertise the creation of new courses of higher education. Last but not least, one of the main priority tasks of the Polish Space Agency is to provide security for Poland and its citizens by increasing Polish defence capabilities through the use of satellite systems. To this direction, the Polish Space agency aims to ensure the security of the state and its citizens and to contribute to the Polish defence potential through the use of satellite systems. Therefore, an important area of the agency's activity is the coordination of activities aimed at the effective use of space technologies and satellite applications for defence purposes.

The tasks resulting from the above-mentioned priorities are carried out by the Vice President's Division for Defense Affairs. The Division consists of the Department of Military Satellite Technologies and the Department of Defense Projects. The Military Satellite Technologies Department consists of the earth and space satellite recognition team, the satellite navigation team, and the satellite communications team.

Starting from 2019, Poland, as a full member of the European Union Space Surveillance & Tracking (SST) Consortium, shares benefits from services at the national level and especially adapts nationally to the possible future contribution. That is why, to both stimulate and secure economic growth and to protect European citizens, there is a strong need for continuous dialogue to better shape the boundaries of a more comprehensive future SSA programme. Joining the SST Consortium will allow for the enhancement of national capabilities related to observation and awareness-building in space, increase the national space sector competences and their role in current and future programmes of the European Union and ESA, as well as strengthen Poland's position in the international arena. Therefore, the establishment, development, and exploitation of the national system of situational awareness in space has been included as one of the five large projects in the National Space Programme for the years 2019–2021[5]. In this context, the SSA area in Poland will be addressed across the board, covering structural, legal, operational, and R&D issues. In particular, it will present the environment in which POLSA operates in the context of the European Union, ESA, other states in Europe and entities currently engaged in activities in the field of ESA, as well as the results of research work. International cooperation including Polish Allies, and international organizations in civil and military domain, in space security domain is extremely important.[6]

Prof Małgorzata Polkowska – Associate Professor of International Law, specialization Aviation and Space Law, Security and Defense, University of War Studies, first permanent Council Representative of the International Civil Aviation Organisation (ICAO) for Poland and the Central European Rotation Group (CERG) 2013 – 2016.

Endnotes

1. Decision No 541/2014/EU of the European Parliament and of the Council of 16 Apr. 2014 establishing a Framework for Space Surveillance and Tracking Support), 27 May 2014, L 158/227).
2. Act of 26 Sep. 2014, Dz. U 2014, poz. 1533.
3. Polish Space Agency, https://polsa.gov.pl/en/
4. Polkowska M., Polish Space Agency pursues task of developing countries' space expertise, Room, The Space Journal nr 2(8) 2016, p. 68–69.
5. Polkowska M, Space Situational Awareness (SSA) for Providing Safety and Security in Outer Space: Implementation Challenges for Europe 2019, https://doi.org/10.1016/j.spacepol.2019.101347; Space Policy Journal, available online 20 Dec. 2019, 101347.
6. Chimicz A. (2018) POLSA, 13th Military SSA Conference presentation, April 2018, London, Enhancing Space Capabilities for the Polish MOD: SSA System Development; Konacki M., (red), Optical, laser and processing capabilities of the new Polish Space Situational Awareness Centre, Conference presentation, Sep. 2019, Maui.

© University of Stuttgart – Institute of Space Systems / http://electricrocket.org/2019/585.pdf

Applied-Field Magnetoplasmadynamic Thrusters

X

The Ambition from the East

By Mr Manuel La Rosa Betancourt, Mr Marcus Collier-Wright, Mr Ryan O' Regan, Mr David Hindley, Prof Georg Herdrich and Prof Lamont Colucci

The New Age of Space Situational Awareness

The critical dependence of terrestrial defence applications on space assets and satellites has positioned space as the next frontier where the struggle for global dominance will take place. The rapidly evolving nature of satellite capabilities is defining the requirements of future defence space assets while the ever-growing popularity of small satellites and satellite constellations in Low Earth Orbit (LEO) demands the consolidation of communications and monitoring satellites in Geostationary Earth Orbit (GEO). The result of such action dictates that the next generation of defence satellites will be larger and heavier, more capable, and will require more power.[1]

Rapidly changing conditions and situations on the ground demand responsive and versatile space assets to provide the necessary military support. For defence applications, the manoeuvrability and lifetime capabilities of these space assets are of critical importance in order to determine their responsiveness, robustness, and lifespan. Furthermore, the establishment of a consolidated yet sustainable space asset network necessitates recovery and repair systems as a contingency measure to minimize the impact of both physical and cyber-based attacks on key space assets.[2] Looking ahead at the medium and long-term defence landscapes, the capacity to transport large quantities of military cargo beyond Earth to the Moon and Mars will play an important role in military space operations, and will further increase the demands on spacecraft size and power consumption. These new requirements and applications call for the utilisation of more advanced and capable propulsion technologies.

The Importance of Spacecraft Propulsion

The choice of propulsion system is key to determining the manoeuvrability and lifetime capabilities of the spacecraft, and the impact of this choice becomes even more significant as spacecraft become larger and heavier.[3]

Spacecraft propulsion systems can be broadly defined within two categories: Chemical (CP) and Electric Propulsion (EP) systems. Chemical systems are capable of providing high thrust to spacecraft, which enhances their manoeuvrability and responsiveness. However, they utilize fuel very inefficiently, which greatly limits their lifespan – the spacecraft can only perform a certain number of manoeuvres before running out of fuel. In addition, this greatly reduces the available payload on a spacecraft, leading to a reduction in spacecraft capability in terms of in-orbit computational power and communications, and hence reducing the effectiveness of defence against cyber-attacks.[4]

Electric systems, on the other hand, are far more efficient, but their low thrust limits their responsiveness and manoeuvrability. Moreover, current

EP technologies rely on expensive and rare propellants, and scale poorly to higher powers, making them unsuitable for larger and heavier spacecraft due to an increase in complexity, mass, and cost. A more advanced technology, which offers greater operational flexibility and is capable of scaling to larger spacecraft, is required.

A Key New Technology

The most promising technology for these high demands is the Applied-Field Magnetoplasmadynamic (AF-MPD) Thruster, which uses a combination of magnetic and electric fields to generate thrust. This technology offers several unique characteristics, including throttleability, defined as the ability to operate over a wide range of conditions. This function enables variation in the thrust produced, providing the flexibility and versatility demanded by new space defence requirements. Meanwhile, the scalability of the technology enables applications to larger satellites while avoiding the mass and complexity penalties that limit other EP technologies. In addition to these benefits, the thruster technology is robust, offers greater thrust vectoring control, and can operate on propellants which are far cheaper and more readily-available than current options.[5]

For these reasons, the technology has experienced over 60 years of research heritage in 6 different countries around the world, but to date has been limited to only three spaceflight missions due to the large mass and low efficiency of the copper electromagnets used to generate the magnetic field. In contrast, High Temperature Superconductors (HTS) have reached industrial maturity and act as a key enabling technology for AF-MPD, drastically reducing the mass and power consumption of the electromagnets while increasing the efficiency and lifetime of the thruster.

The Effect on Space Operations

AF-MPD enables the responsiveness, operational flexibility and robustness demanded by the new defence environment and maximizes the effectiveness and potential of defence assets in space. For a large satellite in GEO, AF-MPD can offer high efficiency and minimal fuel consumption for standard operations, switching to a high thrust mode of operation when rapid satellite repositioning or manoeuvring is required. In the context of an in-orbit servicing vehicle, the use of AF-MPD can enable optimized spacecraft operations, leading to fuel savings and thus an increased number of servicing operations over the mission lifetime, while still offering fast responsiveness in the case of urgent operations. In-orbit servicing is among the most feasible of options to provide a recovery service to spacecraft. Spacecraft capable of offering such a service have similarly stringent requirements on operational flexibility and manoeuvrability in order to maximize their effectiveness. In the case of cargo missions, the use of

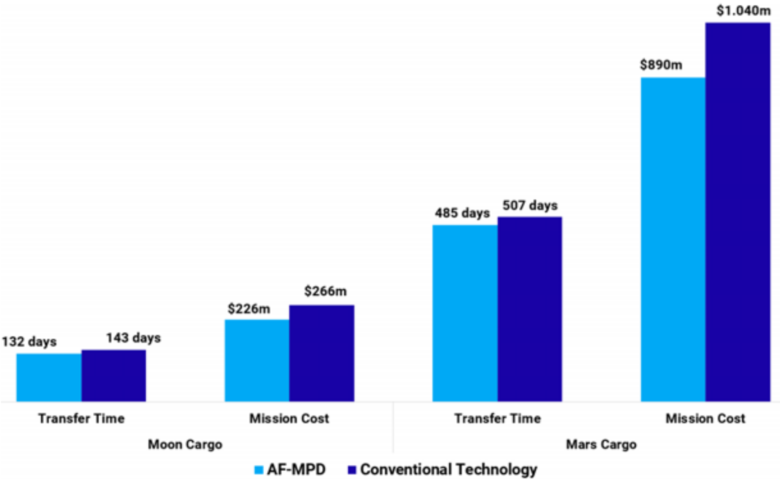


Figure 1: *Mission time and cost comparison between AF-MPD and conventional technology.*

AF-MPD can achieve cost and time savings on cargo transfer to the Moon by $40 million and 11 days and $150 million and 22 days for a Mars cargo scenario when compared against conventional technologies.[6] These two cases indicate that AF-MPD has a highly beneficial impact on space operations and therefore defence capabilities.

The Geopolitical Background

The unique proposition offered by this technology has motivated its development as a global technology. The first activities were concentrated in Germany and the USA in the 1960s, while significant research was also conducted in Japan and Russia in the 1980s and 1990s, alongside three flight experiments proving operational capability in space. Today, the Institute of Space Systems at the University of Stuttgart in Germany, and Nagoya University in Japan, are the two main centres of MPD research worldwide. In Stuttgart, the 100 kW class SX3 thruster has demonstrated the best experimental performance of any AF-MPD prototype to date.[7] Despite the prominence of AF-MPD programs at NASA and the production and testing of several prototypes between 1965 and 1996, American research on the technology has diminished greatly, and the US has lost its world-leading position in AF-MPD.[8]

The Threat from the East

In the past decade, AF-MPD research has also taken place in Italy and China. In particular, the activities in China are increasing at a rapid rate. China has made clear its ambition to be the leader in economic and military use of outer space by 2045, and has dedicated substantial funds to building the infrastructure needed to articulate a fast-track development program.[9] China has implemented a roadmap to appropriate and exploit AF-MPD technology by monitoring and analysing the work in Nagoya and Stuttgart. They have understood the challenges involved in solving the paradigm of high power in space and have already set in motion the necessary instruments to gain leadership and non-dependency with a prototype copy of the SX3 thruster at Beihang University.[10] Additionally, efforts are being undertaken to develop a 500kW class thruster at the Shanghai Institute for Space Propulsion. Furthermore, they are already embarking on research into the use of HTS in their thrusters. The assessment of Prof. Georg Herdrich, the leading authority on AF-MPD technology in Europe, estimates that the Chinese will be able to attain in-orbit demonstration capabilities within 3 to 5 years.

Russia was one of the main players in R&D efforts for the technology until 2010, after which activities fell to a minimum. Nevertheless, they have achieved industrialization levels in HTS technology by gaining access to European markets. They have also developed the necessary capabilities for Nuclear Electric Propulsion, adding additional pressure on Western countries to develop similar strategies for high-power missions. Based on their continuing manpower expertise, they could articulate a program for development of the technology within 5 years. Table 1 shows the different thruster power classes and the corresponding spacecraft missions.

EP Tech-nologies	Small Satellites	GEO Satellites	Auto-mated Transfer Vehicle	Refuels Orbital Vehicles	Military Asteroid Deflec-tion	Moon cargo transfer from LEO	Mars cargo transfer form LEO	Mars manned Mission
HET	80W-5kW	5-20kW	20-30kW	20-30kW	35kW	20-100kW	100kW	
GIE	30W-5kW	5-20kW	-	-	-	-	-	
SUPREME	750W-5kW	5-20kW	20-50kW	20-50kW	50kW	20-100kW	100-500kW	500kW
VASIMR						200kW	200kW	200kW

Table 1: *Comparison of thruster power classes per mission.*

The Need for NATO and FIVE EYES Cooperation

The rich AF-MPD research heritage of Germany and the US, coupled with the extensive capabilities of EP and spacecraft system development across Europe and North America, means there is a decisive opening for NATO member states to achieve a dominant position in future space activities by securing AF-MPD technology.[11] The FIVE EYES group is positioning itself towards this through recent developments: the establishment of the United States Space Force in 2019[12] and the commitment to the Lunar Gateway ARTEMIS mission (50kW)[13]; the endorsement of AF-MPD technology by the New Zealand Space Agency; the launching of the Moon to Mars initiative by the Australian Space Agency; and the increased focus on space applications and disruptive space technologies by the UK government in the wake of Brexit.[14]

In Europe, the move towards this progressive position is slowly gathering pace, with the EU recently committing €3.4 million in funding towards the development of a superconductor-based spacecraft system for re-entry shielding. Nevertheless, despite the technological maturity of the superconductor industry and the disruptive potential it provides across industries and applications, significant entry barriers have left it unable to integrate into the European space market.[15] Despite the move towards high power missions, as seen in the ESA Mars Sample Return mission (40kW), the lack of an entry scenario for both HTS and AF-MPD technology in Europe threatens to allow the technology to fall into the hands of Russia or China.

It is difficult to understate the strategic implications for NATO if this technology is not developed in time. AF-MPD promises immense value for space military applications and mastering superconducting technologies will have huge impacts in aviation[16], defence and naval applications[17]. With the arrival of the high-power market, the development of such technology is fundamental in securing a leading position in the future of space. In the past, Europe and the USA have been leaders in the development of this technology. Today, this R&D has been forced to take a back seat due to current political trends and the European and American inability to face global challenges.

It is consequently of paramount importance that NATO exercise pressure and take leadership, with the aim of mitigating the risk of losing this technology to Russia and China and minimizing the implications this would have for both the US and Europe. In other words, the western alliance cannot afford to allow potential adversaries to gain this propulsion technology before they do; NATO must lead the space race, and not simply be a part of it. It is fundamental that a joint assessment of both the technological status quo and the impacts on the space and military programmes of Europe and the USA is conducted. A combined technology review by the US, the EU and the FIVE EYES group would serve to create a favourable environment for further development of the technology, and also avert the risk that other powers gain the upper hand in the race to secure dominance in space.

Concluding Remarks

Entering into the expanse of space beyond the Earth’s atmosphere will be the next frontier in which to assert global dominance. However, such radical advancements require radical technological breakthroughs and the innovation in research to foster their development. The strategic situation is changing as nations like China discuss colonizing and claiming the Moon. AF-MPD is a strategic game-changer as space becomes the most important realm of national security from both a military and economic perspective. It is surely one of the most critical variables that will place the western alliance ahead of potential adversaries and opponents. The major parties within NATO must articulate a joint strategy to co-develop the technology together with the FIVE EYES group and, where possible, NATO countries must look at the positive impact of superconductors on their strategic advantages. For without political support, private investors will not face the risks associated with securing the technology alone. It is therefore in the interest of all NATO parties to work together to develop stronger coalitional ties regarding space policy and take the necessary steps to explore radical technologies such as AF-MPD.

Manuel La Rosa Betancourt is an entrepreneur and material science engineer with a masters' degree in business innovation with over 15 years' experience in the chemical industry. Since 2014 Founder of Pi Integral Solutions Limited, an innovation consultancy firm in the aerospace sector focused on plasma technologies, superconductors, and materials.

Marcus Collier-Wright is an aerospace engineer with a specialisation in electric spacecraft propulsion. At the University of Southampton, he built an ECR Microwave Gridded Ion Thruster neutraliser, and he previously worked at ArianeGroup on Microwave Electrothermal Thrusters and the RIT 2X ion thruster.

Ryan O' Reagan holds a bachelor's in international modern Languages (German and Spanish), currently a Blue Book Trainee at the European Commission. He worked as Project Development Support at Pi Integral Solutions and has gathered experience in business processes and communications working across various industries.

David Hindley is chartered engineer with over 35 years of experience in the space industry, including at QinetiQ, with responsibility for successful delivery of the T5 ion thruster deployed on ESA's GOCE mission. Formerly an Engineering Manager at the National Physical Laboratory with close involvement in atomic clocks and GPS.

Prof Georg Herdrich is the Head of Electric Propulsion and Plasma Wind Tunnels at the Institute of Space Systems, University of Stuttgart. In this position, he has overseen the AF-MPD R&D program and experimental testing of the SX3 thruster, the most advanced MPD prototype in the world.

Prof Lamont Colucci is a Professor of Politics and Government at Ripon College where he lectures on United States national security and foreign policy, coordinates the National Security Studies program and teaches courses on national security, foreign policy, intelligence, terrorism, and international relations.

Endnotes

1. Wirt, Uwe, 'Deployment of Robotics Technologies for Orbital Operations and Spacecraft Design', International Symposium on Ensuring Stable Use of Outer Space - Enhancing Space Security and Resilience – 3-4 Mar. 2016, Tokyo.
2. Lal, Bhavya, Asha Balakrishnan, Becaja M. Caldwell, Reina S. Buenconsejo, Sara A. Carioscia, 'Global Trends in Space Situational Awareness (SSA) and Space Traffic Management (STM)', Science & Technology Policy Institute, IDA Document D-9074.
3. Czysz, P. A., C. Bruno, B. Chudoba, 'Future Spacecraft Propulsion Systems and Integration Enabling Technologies for Space Exploration', Springer-Verlag Berlin Heidelberg, 2018.
4. Betancourt, M. La Rosa, A. Boxberger, G. Herdrich und M. Bauer, 'High Temperature Superconductors as game changers for Plasma based Space Propulsion Systems for GEO Satellites, Drag Compensation of Large Space Structures and Beyond Earth Orbit Missions', Space Propulsion Conference, Sevilla, Spain, 2018.
5. Betancourt, M. La Rosa, M. Collier-Wright, M. Girard, R. O' Regan, S. Hofmann, B. Ballester Massuti, G. Herdrich, J. Tanchon, J. Lacapere and M. Bauer, 'Superconductor-Based Applied-Field Magnetoplasmadynamic Thrusters - SUPREME - as an Enabling Technology for the Next Generation of Space Missions', 17th Reinventing Space Conference, Belfast, 2019.
6. Collier-Wright, M., M. La Rosa Betancourt, M. Girard, R. O'Regan, B. Ballester Massuti, G. Herdrich, J. Tanchon, J. Lacapere and M. Bauer, 'Systems Architecture and Business Opportunities for Applied-Field Magnetoplasmadynamic Thrusters', 36th International Electric Propulsion Conference, Vienna, 2019.
7. Boxberger, A., A. Behnke and G. Herdrich, 'Current Advances in Optimization of Operative Regimes of Steady State Applied Field MPD Thrusters', 36th International Electric Propulsion Conference, Vienna, 2019.
8. Boxberger, A., G. Herdrich, 'Integral Measurements of 100 kW Class Steady State Applied-Field Magnetoplasmadynamic Thruster SX3 and Perspectives of AF-MPD Technology', 35th International Electric Propulsion Conference, Atlanta, 2017.
9. Wolcott, Robert C., 'Space Cowboys, China's New Long March, Interplanetary Opportunities And Existential Risks – Our New Age In Space', Forbes [Website], 2019, https://www.forbes.com/sites/robertwolcott/2019/11/19/space-cowboys-chinas-new-long-march-interplanetary-opportunities-and-existential-risks--our-new-age-in-space/#335ec77d4d17.
10. Wang, B., H. Tang, Y. Wang, C. Lu, C. Zhou, Y. Dong, G. Wang, Y. Cong, D. Luu und J. A. Cao, 'A 100 KW Class Applied-field Magnetoplasmadynamic Thruster J. Vis. Exp. (142), e58510, DOI: 10.3791/58510', 2018.
11. Unal, Beyza, 'Space-based cybersecurity challenges for NATO', Room Space Journal of Asgardia [Website], 2019, [https://room.eu.com/article/space-based-cybersecurity-challenges-for-nato].
12. Colucci, Lamont, 'A Space Service in support of American grand strategy', The Space Review [Website], 2019, [https://thespacereview.com/article/3664/1].
13. 'NASA Awards Artemis Contract for Lunar Gateway Power, Propulsion', NASA [Website], 2019, [https://www.nasa.gov/press-release/nasa-awards-artemis-contract-for-lunar-gateway-power-propulsion].
14. 'Will the UK Get a Space Command?', Global Defence Technology [Website], 2020, [https://defence.nridigital.com/global_defence_technology_mar20/will_the_uk_get_a_space_command].
15. O' Regan, R., 'Europe shuts door on revolutionary electric propulsion technology', LinkedIn [Website], 2019, [https://www.linkedin.com/posts/pi-integral-solutions-limited_europe-shuts-door-on-revolutionary-electric-activity-6624969769248399360-06c3].
16. Betancourt, M. La Rosa, M. Bauer, 'Status Quo on material and process technology for Type 2G High Temperature Superconductors: Technology trends and challenges for prototype development within the aerospace industry', Electric & Hybrid Aerospace Technology Symposium, Cologne, Germany, 2017.
17. Betancourt, M. La Rosa, M. Bauer, 'Type 2G High Temperature Superconductors: Technology Trends and Challenges for Naval Applications', 31st Undersea Defence Technology Conference, Glasgow, Scotland, 2018.

Information Environment

Information Environment Panel Introduction

XI

Competing in the Information Environment

By Lt Col Livio Rossetti, ITA Army

Joint Air Power Competence Centre

Introduction

According to the US Department of Defense's 2018 National Defense Strategy, 'we are facing increased global disorder, characterized by decline in the long-standing rules-based international order – creating a security environment more complex and volatile than any we have experienced in recent memory. Inter-state strategic competition, not terrorism, is now the primary concern in US national security'.[1] A new phase has started for the US and NATO, a phase that will be characterized by an intensification of strategic competition with several rivals.[2] This competition is expected to take place mainly below the threshold of the recognised armed conflicts to which one has long been accustomed, in an area that is sometimes referred to as the 'gray zone' between peace and war.[3] Gray zone can be described as a zone in which tactics such as subversion of political systems, psychological warfare, and secret and informative paramilitary operations are used to affect public perceptions and exert influence, on and through, instruments of power. American analysts have shown that some of the tactics of the gray zone which have been employed by Russia and China are relatively new in shape and effect, and significantly different from each other.[4] This diversification presents a differentiation of the scope of the threat posed, as well as types of potential responses, and represents a serious strategic issue for the Alliance. Giving NATO a coherent competition strategy will require integrating all of instruments of power – diplomatic, information, military, and economic. NATO must be ready to address different aspects: hybrid operations, technological improvements in conventional forces, and prevention of escalation to use of nuclear weapons. One of the fundamental aspects that can contribute to success in the gray zone is successfully competing in the Information environment. This will also include the Electromagnetic Spectrum (EMS), which is indispensable in modern military operations. This results in unavoidable questions as to how NATO secures and exploits Information, and Information Flow, and in which way this contributes or affects Air and Space capabilities.

A New Way to Plan and Execute Operations

In future military operations, the way in which commanders understand, visualize, and describe the battlefield to their subordinate units will be a determining factor for achieving victory. The rapidity and availability of information sharing will be crucial to speed up the decision-making process, exploit the initiative, and create a position of relative advantage. As stated by David G. Perkins, a retired United States Army General, '… interoperability of information … means shared appreciation of Command and Control (C2) as a weapon system, a common sense of which data are critical, and how to protect and leverage that data …'[5] Competing in the information environment will include the struggle to keep information flowing, to safeguard the integrity of information, and to deny the use of information to opponents. This strongly binds the information flow on access to, security of, and control of the EMS through which the information flow occurs. The 2018 US National Defense Strategy anticipates that Anti-Access and Area-Denial (A2/AD), among all, is one of the critical issues that will be dealt with in the event of a high-end conflict with peer adversaries.[6] NATO must be ready to develop a new approach to battle management and the supporting C2. This approach should enable rapid planning and execution of operations, using the capabilities available through all operational domains in a synchronized, cooperative, and efficient manner. Allies also need to be able to combine all datasets, and rapidly interpret all information available to improve situational awareness and provide better information to strategic, operational, and tactical decision-makers. New solutions must be found in order to allow the Alliance to rapidly find, fix, and engage the relocatable systems which competitors employ for creating robust A2/AD networks. The US Joint All Domain Command and Control (JADC2) concept embraces all these ideas. More than just new equipment, JADC2 is a new approach to C2. Unlike the existing approach, which is still a 'system of deconfliction', JADC2 is an innovative 'system of integration'.[7] Almost the same operative philosophy is expressed by the concept called 'Mosaic Warfare'. Developed by the Defense Advanced Research Projects Agency (DARPA), 'Mosaic Warfare' creates a force package by putting together all warfighting platforms. A new strategy that will enable Allies to overwhelm enemy forces by sending a huge quantity of weapon and sensor data, and create a complexity that can be turned into an asymmetric advantage.[8] NATO must understand the information environment, be prepared to compete when it is contested, and rapidly identify and counter malicious actions. Moreover, NATO must develop and adopt new flexible C2 designs, and better-integrated communications systems able to merge all available forces in all operational domains.[9]

NATO Electromagnetic Spectrum Strategy

NATO recognizes and reaffirms that its military freedom of action on the contemporary battlefield is only guaranteed if a sufficient degree of superiority within the electromagnetic spectrum is maintained.[10] The EMS is a key element of NATO armed forces strategy with which deterrence and defence can be achieved with respect to the three core tasks of the Alliance (Collective Defence, Crisis Management, and Cooperative Security). NATO EMS Strategy aims to exploit, access, and control the EMS where and when needed to achieve NATO Military Strategic objectives; and ensure it will remain the superior military force, postured to take advantage of the EMS with the ability to exploit, mask, and manoeuvre within a congested and contested electromagnetic environment (EME).[11] NATO's strategy proposes to revitalize realistic collective training and exercises under contested EME conditions, reinvigorate an institutional commitment to personnel capacity, training, and education across the range of EMO and continue to invest in essential capabilities. The strategy's overarching goals are: (1) institutional awareness and advocacy, (2) effective joint EMO, and (3) robust EMO capabilities. EMO includes any kind of activities which deliberately transmit and receive electromagnetic energy in the EME for military operations[12] and involves multiple disciplines such as Spectrum Management, Navigation, Electronic Surveillance (ES), Electronic Attack (EA), Electronic Defence (ED), and Signal Intelligence (SIGINT). EA, ED, and ES collectively comprise Electronic Warfare (EW).[13] Today, EMO represents the real cornerstone to link and integrate military forces not only within each operational domain but also across all domains by enabling them to develop Multi-Domain Operations (MDO); a new paradigm in developing future JADC2. While NATO is still pursuing the concept of MDO or JADC2, superiority may not be achieved in the future battlefield unless EMO can be effectively employed in the EME.

Conclusion

One of the most important characteristics of air power is speed. Nevertheless, it seems clear that in the future, more than by the speed of its flying systems, air power will be affected by its speed and ability to communicate and to transmit, evaluate and use available information. Highly flexible and agile structures and technologies applied to modern concepts of C2, such as JADC2 and 'Mosaic Warfare', are needed. Such systems must be able to integrate all information available, rapidly detect changes in the situation and therefore provide a timely, powerful, and coherent response. 'Future commanders will have a profound breadth and depth of information and access to capabilities providing cross-domain effects, manoeuvre, and fires.'[14] Information competition and dominance in the electromagnetic spectrum will play an important strategic role. This necessarily causes questions as to how NATO secures and exploits information and information flow. Considering the impact of the information competition across all domains of operations, potential challenges include: the necessity to increase expenditures on research and innovation in order to bridge capability gaps that have arisen due to the tremendous growth of adversaries' capabilities; the evolution of new technologies and emerging enablers that support our ability to secure and control the EMS; and the increasing the resiliency of Space, Cyberspace, and legacy infrastructures. These emerging challenges will be thoroughly explored during the upcoming JAPCC Air and Space Power Conference. The following articles will introduce the reader to some important aspects of these challenges which will be the focus of a panel discussion during the JAPCC Conference:

- Lt Col Panagiotis Stathopoulos, GRC AF, JAPCC, Electronic Warfare Subject Matter Expert, will highlight the high value of EMS in support of Multi-Domain Operations by discussing the necessity of integrating EMS disciplines and functions in a synergistic and symbiotic approach. More importantly, he details why NATO needs to integrate and unify all EMS capabilities, entities, and disciplines under a single domain of operations.

- Mr Stephen Tournageau, Vice President, Warrior Support Solution, LLC deals with the subject of the EMS dependency. His paper elucidates the potency of the threat of spectrum denial. It also reveals how nearly all militaryies' Tactics, Techniques, and Procedures (TTPs) are 100 % dependent on the availability of the spectrum. Mr. Tournageau explains the need to understand how to operate on the modern battlefield and proposes new TTPs, based on some of those from the Cold War era, centred on using our current capabilities to operate in a denied spectrum environment.

- Ms Whitney McNamara summarizes the article 'Winning the Invisible War: Gaining an Enduring Advantage in the EMS' (Clark B. et al, 2019). She presents a new approach to EMS operations focused on asymmetries between the US and opposing militaries. The report recommends how the US and its allies can use these asymmetries to gain an advantage against Russia and China in the electromagnetic spectrum, including capability requirements, operational concepts, and an overall electromagnetic spectrum strategy.

- Général d'armée aérienne André Lanata introduces the themes addressed during the last SACT's Conference 'The NATO Information and Communicators' Conference (NICC) held in September 2019. In it will be found food for thought regarding the modern interconnected and networked world and the important role played by information, or more accurately, disinformation used as instrument by our adversaries in their approach.

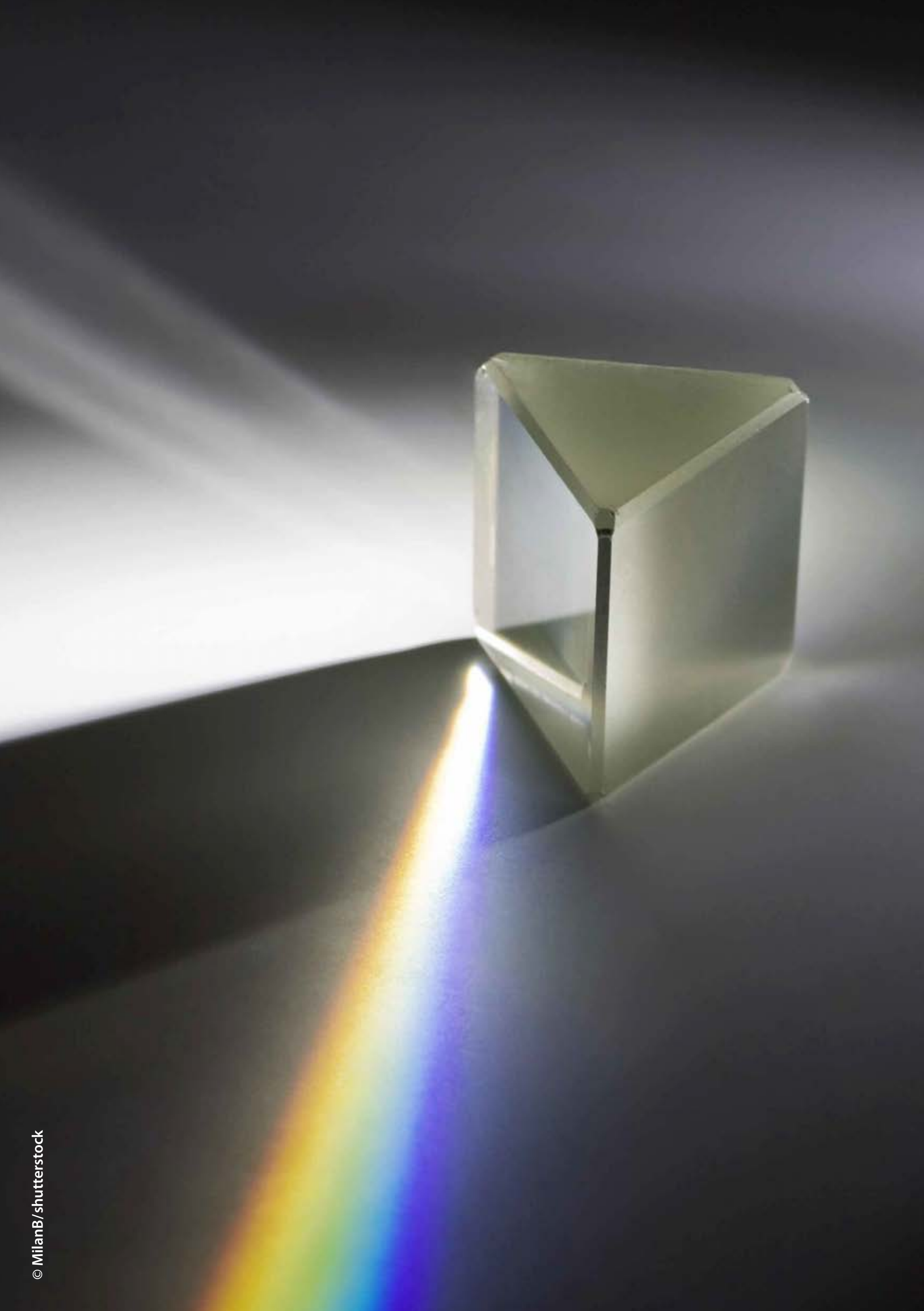
- Last but not least, the Defence Advantage Research Projects Agency (DARPA) in its article 'DARPA Tiles Together a Vision of Mosaic Warfare', introduces this innovative concept. A new revolutionary warfighting platform built upon an interconnected and interoperable force package able to leverage the best characteristics of different platforms. A kind of system of systems characterized by dedicated new interfaces, communications links, and precision navigation and timing software that can allow all the platforms to work together. This could easily overwhelm the enemy forces creating an asymmetric advantage, but there are still many problems to solve because, as known, 'today's weapon systems are not built to function this way'.

While awaiting the conference, these readings will propitiously present the arguments to the reader and at the same time stimulate a constructive and highly desirable curiosity.

Lieutenant Colonel Livio Rossetti is currently stationed at the JAPCC, Kalkar, as Air-to-Land Integration expert in the Combat Air Branch. He is a rotary-wing pilot with more than 27 years' active duty experience in the ITA Army. He has flown utility helicopters as well as combat helicopters.

Endnotes

1. Summary of the 2018 National Defense Strategy of The United States of America, p 1. Available from https://www.defense.gov/Explore/News/Article/Article/1419045/dod-official-national-defense-strategy-will-enhance-deterrence/ [accessed 9 Apr. 2020].
2. Lyle J. et al (2019) Gaining Competitive Advantage in the Gray Zone. Santa Monica Calif.: RAND Corporation, iii. Available from https://www.rand.org/content/dam/rand/pubs/research_reports/RR2900/RR2942/RAND_RR2942.pdf [accessed 5 Mar. 2020].
3. Ibid. 1.
4. Ibid. 1.
5. Perkins D. and Holmes J. (2018) Multidomain Battle – Converging Concepts Toward a Joint Solution. Joint Force Quarterly, 88 14-21. Available from https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-88/jfq-88.pdf
6. Niewood E. (2019) A new battle command architecture for Multi-Domain Operations. The MITRE Corporation, 2. Available from https://www.mitre.org/publications/technical-papers/a-new-battle-command-architecture-for-multi-domain-operations [accessed 5 Mar. 2020].
7. Ibid. .
8. 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 9 Mar. 2020].
9. Ibid. 5.
10. Ibid. 8.
11. EME is the environment where EM effects are created. The EME enables the radiation, propagation, and reception of EM energy across the entire EMS11. NATO conducts Electromagnetic Operations (EMO) to enhance the effective use of the EME and at the same time, to prevent the adversary's use of it.
12. von Spreckelsen, Malte, Commander (2018) Electronic Warfare – The forgotten Discipline. JAPCC Journal, Edition 27 p. 41-45.
13. NATO Electronic Warfare Policy, 4 Jul. 2018.
14. Ibid. 5.



© MilanB/shutterstock

The Dimension of the Electromagnetic Spectrum

XII

The High Value Domain of Operations!

By Lt Col Panagiotis Stathopoulos, GRC Air Force
Joint Air Power Competence Centre

Electromagnetic Spectrum Disciplines

Apart from the traditional physical domains of Air, Land, and Maritime, in the last decade NATO has also declared Space and Cyberspace as domains of operations. While Electronic Warfare (EW) used to be the traditional warfighting element of the Electromagnetic Spectrum (EMS), the 21st century has ushered in a tremendous technology revolution leading to the emergence of new advanced capabilities and functions in the EMS such as Directed Energy Weapons (DEW) and low emission radars. During this same period, Cyberspace[1] has become an attractive domain of operations for power projection as well.

Both state and non-state actors demonstrated in latest Syrian conflict that the dominance in Land, Maritime, Air, Cyberspace, and Space starts with the integration and harmonization of all EM disciplines including: EW, Signal Intelligence (SIGINT), Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR), Navigation Warfare (NAVWAR), and Battlespace

Spectrum Management (BSM). To put it simply, the EMS is the invisible physical space of waves, which bridges all domains of operations, enabling missions and supporting the campaign goals.

While NATO Strategic Foresight Analysis (SFA) highlights the complexity of the future battlefield, and NATO Future Framework for Alliance Operations (FFAO) aspires to allied forces' dominance of the EMS, NATO leaders and planners are still considering the necessity of integrating EMS disciplines and functions under a single coherent approach. Consequently, this article will explain why NATO needs to integrate and unify all the EMS capabilities, entities and disciplines under a single domain of operations, the EMS including Cyberspace.

The Symbiotic Relationship of Electromagnetic Spectrum Disciplines

Since the invention of aircraft and during the last century passed, air operations have been touted as an essential prerequisite contributing to other domains' successful operations in order to achieve their desired end states.

However, the latest battles in Syria and Libya highlighted that airpower is often not abundant enough to achieve the desired campaign end state by itself. The EMS functions such as the electromagnetic and cyberspace activities, were found to be the most attractive operations for power projection on the Syrian battlefield. On the one hand, the low-cost of employment, the 'stealth' attributes, the remote presence and posture, and the ability to fight without a defined Forward Edge of the Battle Area (FEBA) are some of the reasons for the popularity of the EMS capabilities' on the battlefield. On the other hand, the tremendous speed of EMS-dependent applications and the numerous EMS disciplines and functions that are being employed without cohesion and coordination, contributes to a 'blizzard'[2] of EMS effects, where decision-makers might be incapable of making time-critical decisions.

NATO recognizes the EW capability as an essential tool for the full spectrum of operations and other tasks undertaken by the Alliance[3] and NATO Cyberspace policy remains focused on Defensive Cyber Operations (DCO),[4] as NATO has not yet embraced a concept of Offensive Cyber Operations (OCO). In contrast, the Russians demonstrated both in the Crimea annexation and in Syria that they have likely developed doctrine to employ cyberspace capabilities integrated and synchronized with EW and SIGINT activities during their military operations at all levels of war, political, strategic, operational and tactical. In particular, it is highly likely that Russia's EW and Cyber capabilities have been merged[5] under single domain of operations.

However, the 'Alliance Joint EM Strategy' dictates the need for synergy through greater integration of the EME core functions and related activities including those of Cyberspace and Space. The perfect example of the interdependency of EME activities, in particular the EW and Cyberspace, was clearly highlighted during a September 2007 Israeli strike on a North Korean supported nuclear weapons facility in Syria. More specific, a cyberstealth attack was delivered by an Israeli airborne electronic attack platform which allowed Israeli forces to virtually take control of the Syrian integrated air and missile defence system, and let the 'highly observable' F-15s and F-16s strike aircraft penetrate the Russian-designed, modern and long-range surface-to-air missile systems of Syria.[6]

Furthermore, certain NATO nations have already recognized at a national level the convergence between cyberspace and EW activities[7] and employed them under the concept of Cyber-Electromagnetic Activities (CEMA).[8] This synergy was also effectively employed during Operation Atlantic Resolve.[9,10] Similarly, the symbiotic relationship between EW and Cyberspace operations has also been noted by near-peer competitors of NATO such as Russia, China and Iran.

In fact, Cyberspace is a part of the EMS, and it is the only domain which has been physically and virtually created by humans employing applications of the EME such as copper wires, fibre optic cables, microwave, and satellite relays. The common ground of Cyberspace operations, EW, and SIGINT activities is apparent, and it has been previously highlighted by United States (US) Army Doctrine.[11] Cyberspace operations overlap with more than 50 percent of both EW and SIGINT activities; necessitating the great need for operational consolidation allowing EMS disciplines to share the same staff, processes, and technologies in order to avoid duplication of effort and to prevent working at cross-purposes.[12]

The High Value of the Electromagnetic Spectrum

The differences in the Libyan and Syrian conflicts could be omens which foreshadow a future in which NATO will only achieve dominance in the Land, Maritime, Air, and Space domains, while superiority is achieved in the whole EME including Cyberspace. Dominance in the EME may not be achieved unless all the EME stakeholders[13] operate in a synchronized, harmonized and coherent manner with all domain owners towards the campaign's desired end state. To put it simply, all EM disciplines and functions including Cyberspace operations need to be integrated and synchronized in order for NATO forces to be dominant in the ambiguous, increasingly complex, and contested future conflict environments.

Similarly, the Russo-Georgian conflicts' lessons learned allowed Russia to develop tremendous and modern EW capabilities, which have been effectively employed in the Eastern Ukrainian and Syrian battlefields. In particular, the recent Russian–Ukrainian clash highlighted that employing EW and Cyberspace operations synergistically, could be a high-value and highly effective tool of operations during 'gray zone'[14] conflicts. Upon Russia's invasion of the Crimean Peninsula, an extended array of multipurpose electromagnetic assets was established along all the territories of interest, allowing Russia to implement its strategy on creating, not only a contested, but also a congested and denial environment against adversaries' operations. It is apparent that Electromagnetic Operations (EMO) has probably become a key element of Russia's modern warfare doctrine, allowing it to employ deliberate actions, by proxy, in support of fulfilling its ambitions and goals against opposing nations' pursuits during the outbreak of a 'gray zone' conflict.

Unifying EME stakeholders and challenging those to operate as a single task force under one policy, such as the EMO concept, may let NATO achieve its goals and desired end state during an intervention. The EMS might be a significant factor of operations when the threshold line between military and non-military actions is opaque, and intervention events could not be clearly attributed to any of the opposing forces.

Not only could EMS capabilities provide a great advantage to NATO forces against adversaries during a 'gray zone' conflict, but the EMS could also be rendered as a high value domain of operations that NATO political leaders and planners may employ as a tool of deterrence. Employing EMO may prevent NATO from being engaged in a lethal intervention, and shield its forces and infrastructure, while at the same time NATO forces may have the opportunity to occupy the EMS and dominate a potential adversary.

Conclusion

Apart from Russia's resurgence, for the first time, the NATO Secretary General addressed that the rise of China also poses challenges for Alliance security and he stressed that 'as the world changes, NATO will continue to change.'[15] While the world is changing and new security challenges are arising, EMO might be a cornerstone in any future conflict, in particular, among near-peer NATO competitors. NATO adversaries have identified that EMS disciplines can be unified into a single domain of operations, rendering it as a cost effective and highly valued solution in support of their goals and strategies, as well as, their 'gray zone'[16] operations.

While NATO planners are still pursuing the utopia of Multi-Domain Operations, presently no one can be the only occupant of the EME to achieve electromagnetic dominance. However, the apparent common ground of Cyberspace, EW, and SIGINT operations necessitates that NATO should unify all of the EMS dimensions including Cyberspace, so that allies may acquire the ability to use more of the EMS, to share the EMS more efficiently, to protect our own forces' use of the EMS, deny our opponents' use, and achieve electromagnetic dominance in the future.

Lieutenant Colonel Panagiotis Stathopoulos is an experienced F-16 instructor pilot and a graduate of the Tactical Weapons Fighter School. He has served as Director of Operations and as Squadron Commander of 341 Fighter Squadron, He also served as the EW including SEAD Operations SME at the JAPCC.

Endnotes

1. NATO officially defines the Cyberspace as the global domain consisting of all interconnected communication, information technology and other electronic systems, networks and their data, including those which are separated or independent, which process, store or transmit data.
2. One article proposes, 'blizzard' is employed to convey the concept that EMS is like a unlimited invisible space where large or overwhelming number of things or effects arising or generating suddenly with the speed of light and sharp blow, and cannot be sensed by the human information processing system. 'Blizzard' is also used figuratively to refer to future EMS activities and effects that come suddenly in large quantities and must be dealt with appropriate technology in order decision-makers to acquire the required information, facts, and data in support of military operations.
3. NATO Topics, 'Electronic Warfare'. In NATO, 2014. (Accessed 15 Apr. 2020) Available at: https://www.nato.int/cps/en/natohq/topics_80906.htm?
4. NATO Topics, 'Cyber Defence.' In NATO, 2020. (Accessed 15 Apr. 2020). Available at: https://www.nato.int/cps/en/natohq/topics_78170.htm.
5. McDermott, R. 'Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum', A report of the International Centre for Defence and Security (RKK/ICDS), Estonia, 2017. Online at: https://icds.ee/wp-content/uploads/2018/ICDS_Report_Russias_Electronic_Warfare_to_2025.pdf (accessed Oct. 2019).
6. Clarke, Richard A. and Robert K. Knake, 'Cyber War: The next threat to National Security and What to do About it'. New York: Harper Collins Press, 2010.
7. Porche, Isaac R. III, et.el., 'Redefining Information Warfare Boundaries for an Army in a Wireless World'. In RAND study prepared for the US Army. Santa Monica: RAND, 2013.
8. CEMA is an US Army initiative designed to provide tactical commanders with integrated cyberspace operations, Department of Defence Information Network operations, Electronic Attack, Electronic Protection, Electronic Warfare Support, Spectrum Management Operations, Intelligence, and Information Operations support/effects.
9. Sjheiffer, Matthew J., Lt Col, 'US Army information Operations and Cyber-Electromagnetic Activities, Lessons from Atlantic Resolve'. In: The Military Review Online Exclusive Journal of US Army, Mar. 2018. Fort Leavenworth, Kansas: Army University Press, 2018. Online at: https://www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2018-OLE/Mar/Army-Info-Ops/ (accessed Oct. 2019).
10. Atlantic Resolve is a demonstration of continued U.S. commitment to collective security through a series of actions designed to reassure NATO allies and partners of America's dedication to enduring peace and stability in the region in light of the Russian intervention in Ukraine. (Available at: https://www.eur.army.mil/Newsroom/Fact-Sheets-Infographics/Fact-Sheet-Article-View/Article/1451471/%20atlantic-resolve-fact-sheet/).
11. FM 3-12, 'Cyberspace and Electronic Warfare Operations', US Army, 2017. (Accessed 15 Apr. 2020) Available at: https://fas.org/irp/doddir/army/fm3-12.pdf.
12. Ibid. 7.
13. Ibid. 8.
14. On article purposes, the RAND corporation definition has been captured by the study 'Gaining Competitive Advantage in the Gray Zone', available at: https://www.rand.org/pubs/research_reports/RR2942.html According to this study, gray 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 action, often by blurring the line between military and non-military actions and the attribution for events.
15. Stoltenberg, Jens, Secretary, General, 'NATO Secretary General's Press Conference following the meeting of the NAC at the level of HoS/G, London, 3-4 Dec. 2019'. In NATO newsroom, 4 Dec. 2019 (Accessed 4 Dec. 2019). Available at: https://www.nato.int/cps/en/natohq/opinions_171554.htm.
16. Ibid. 13.

© Allied Air Command/OR-8 Sebastien Raffin

Denial of Spectrum Denial: NATO's EW Worry

XIII

By Mr Steve 'Tango' Tourangeau and Mr Dirk Smith

In the world of electronic warfare (EW), the North Atlantic Treaty Organization (NATO) seems to be doing a good job of preparing to meet our adversaries on the battlefield tomorrow. The problem is that we are not prepared to fight them today. Indeed, there are many ongoing efforts to develop new technologies that will protect our ability to operate in a denied spectrum environment; a conflict in which our access to the spectrum is limited or blocked, thus interfering with our spectrum-dependent capabilities including position, navigation, targeting and communications.

Spectrum and Electronic Warfare Defined

The *spectrum*, or the *electromagnetic spectrum*, is the medium through which all radio, radar, cellular, wireless data, laser, and visual signals pass, therefore, it is where Electronic Warfare (EW) operates. The spectrum is categorized by frequencies and wavelengths used by each device to transmit and/or receive signals in the form of radiated energy. It is what enables radar acquisition and tracking, communications for command and control, navigation and precision timing, targeting and precision strike, and supports critical cyber activities.

The issue is that those new technologies will not be available for years to come. Compounding the problem is that many people are reluctant to accept that we do not own the spectrum in today's battles like we owned the air as we hit Normandy on D-Day. To better protect our forces, our missions, and our interests, we must understand and accept what risks we have; only then can we determine how to operate today so that we can survive until our new technologies are deployed tomorrow.

Today's Risks

The extent to which our military capabilities are networked is impressive, from high tech command centres to systems embedded in soldiers' clothing. However, since these systems are 100 % dependent upon the spectrum to send and receive data, they will fail in a denied spectrum environment from three major causes: adversary actions, environmental interference, and human error, as described briefly below.

Adversary Actions

In 2008, Russian forces conducted a full-spectrum offensive that denied the use of radio waves and the Internet within the country of Georgia. As a result, the Georgian military was effectively blinded, drastically reducing their command and control capacity.[1] Similar approaches were used by Russian forces in Eastern Ukraine, where, according to a BBC article, 'electronic jamming by specialized Russian units has been highly effective. Indeed, Russia has won the battle in the electromagnetic spectrum hands down.'[2]

In 2018 China has shot down one of their own satellites. This was the second such action following the initial shot down in 2010 when they likely used a DN-3 missile that reached 62 miles above the earth's surface. These demonstrations did more than raise the eyebrows of many in the west.[3] Though the satellites were their own and were apparently defunct, the message was clear: we can take down yours too.

Then consider the Islamic Revolutionary Guard Corp's apparent ability to intercept control of a US, $6 million RQ-170 stealth drone and land it safely 140 miles inside Iran.[4] This was the same drone system that enabled the US to watch the raid on Osama Bin Laden without detection.

Environmental Interference

Everyday, natural climactic conditions can interfere with EW operations. A common example was explained by a former USAF C-141 Starlifter navigator, who said that 'the atmosphere is not constant; it changes its altitudes and even its shape. During our many Atlantic crossings, these atmospheric changes would increase or decrease the range of our HF signals, at times completely eliminating our ability to communicate with base.' Adding to this is the effect solar flares have on the Earth's ionosphere, causing it to become super-ionized which can also interfere with radio transmissions[5] Then again, even a simple snowstorm can interrupt signal reception; just ask anyone who has dish instead of cable TV and lives where it is cold enough.

On the man-made side, the World Meteorological Organization (WMO) warned that 'The race to release 5G technology threatens to squeeze out other radio-frequency dependent technologies.' The concern is that its transmissions are expected to bleed over to bands used by the world's critical national severe weather early warning systems.[6] Another human-caused environmental event occurred last year when Global Positioning System (GPS) signals were interrupted around Ben Gurion International Airport in Tel Aviv, Israel. The cause appears to have been Russia's attempts to protect operations at Hmeimim Airbase in Syria through the use of their EW systems. The effect, though not apparently directed at Israel, spread far enough to reach Ben Gurion some 200 miles to the south.[7,8]

Human Error

From 2001 to the end of 2014, we lost 1,401 NATO/ISAF coalition personnel to Improvised Explosive Detonations (IED) in Afghanistan.[9] To counter the new threat, the Counter Radio-Controlled Improvised Explosive Device (RCIED) electronic warfare system or 'CREW' was devised. It worked. However, in the rush to protect our soldiers, we ended up fielding a system that emitted jamming signals that included our communications frequencies. Therefore, when CREW was on, comms were out. In some cases, when needing to use the radio, soldiers would turn the system off... and we lost more soldiers. In another case, a 2,000 pound bomb was tragically directed by our own GPS systems to land on three US Special Forces north of Kandahar. The cause? During the bombing run, the ground controller who called for the air strike changed the battery in his GPS device, not realizing that rebooting it caused the aim point being transmitted to the B-52 bomber to be his.[10]

Denial of Spectrum Denial

In spite of the facts presented above, some people still deny that our forces are likely to be denied unfettered access to the spectrum in the field of battle. In other words, denial of spectrum denial or DoSD; they just won't believe it will happen. A 2016 article in The Diplomat exemplified this point when it stated that 'The United States has been criticized for ignoring the rapid development of Russia's SIGINT and EW capability, which was put on full display at the onset of the Russian invasion into Crimea and east Ukraine, as Ukrainian cell-phones and communications equipment fell silent to Russian jammers.'[11] If we now accept that we are likely to find ourselves in a spectrum-denied environment, what alternative solutions can we turn to? What follows is only a portion of many options, both old and new.

Tactics, Techniques and Procedures in a Spectrum-Denied Environment

Celestial Navigation

When the Apollo 12 rocket was struck by lightning after launch in 1969, the astronauts turned to celestial navigation; using the stars to get to the moon. This ancient system of navigation was shelved two decades ago but, as of 2015, the Naval Academy dusted off their sextants and have returned to teaching the skill.[12] Let's face it, you can't hack a sextant but, then again, there are often clouds or fog '…'.

Wide Area Augmentation System

The Wide Area Augmentation System, or WAAS, provides augmentation information to GPS/WAAS receivers, resulting in increased navigational accuracy. However, when, GPS signals are interrupted, WAAS can provide information to GPS/WAAS receivers. The service is only available for use in North America today, but compatible systems are planned internationally.[13]

Omni-Directional Range/Distance Measurements Equipment

Very High Frequency (VHF) Omni-Directional Range (VOR) navigation systems are a commonly used navigation system based on fixed ground radio beacons. Through the use of radial and distance measurements to each beacon, the VOR/DME system enables a pilot to fly straight course between almost any two points.[14] Granted, many are being phased out, but military use continues.

Radio Direction Finder

The radio direction finder has been around for a long time. By using two signals, such as two commercial radio stations, a vessel at sea can triangulate to pinpoint its own location. With search and rescue, a simple RDF device can pinpoint the location of a distress signal triggered by a man overboard, a wounded soldier on land, or a downed aircraft.

Star Tracker

Draper Laboratories has developed another approach to the GPS-denied solution; the 'Cross Polarizing Star Tracker'. The system uses polarized sensors (rather than imaging optics) in a solution that does not require 'power-hungry pixelated imaging sensors' and can be fabricated on a 'thin substrate, enabling vertical profiles of less than a millimeter,' eliminating the need for bulky, mechanically complex optics.[15]

Inertial Navigation

Inertial Navigation Systems (INS) are not dependent upon any external information and do not radiate any energy externally. Instead, INS bases its capabilities on some initial reference point and the use of several gyros and accelerometers to derive subsequent positions. However, without external input, INS is subject to drift over time.

Dead Reckoning

Dead reckoning, the traditional method of navigation using a known starting point, a compass course, travel speed and time elapsed, is too oft ignored. However, the US Coast Guard included it in their 2020 Manual which teaches to leverage such '… traditional forms of navigation if, and when, electronic means of navigation are not available.'[16]

Atomic Clocks

The Defense Advanced Research Projects Agency (DARPA) is developing a chip-sized atomic clock that will enable navigation and targeting without GPS satellite access.[17] Though chip-sized atomic clocks are commercially available, DARPA is working to refine their accuracy.[18]

Look Out the Window

Of all things, too few people look out the window. A pilot highlighted its value in his memoir about flying B-26 bombers in World War II when he stated that his instructor said 'Don't be afraid to look out the window. It might just let you know that you are over Dallas instead of Waco, as you thought from your star shots.'[19]

Ham Radio Cybernetwork

A resourceful hobbyist developed a way to transmit and receive Internet traffic through a ham radio. To accomplish this, he developed a new protocol called 'New Packet Radio' or 'NPR' and used $ 80 worth of easy-to-assemble hardware. The result is an apparent ability to 'send data via IPV4 up to 300 kilometers.'[20]

Software Defined Radio

Software-Defined Radio (SDR) enables transmitter and receiver modulation/demodulation through software instead of spinning a dial. This ability enables a single radio to constantly hop from one frequency to another to avoid congestion or, more importantly, to avoid enemy jamming. As a result, most updates are simple software downloads, negating the need for costly hardware changes.[21]

Morse Code

Morse Code, communication-based on dots and dashes of electrical pulses or flashing lights, still exists. While forgotten by most people, Morse Code remains in use in Aviation and Aeronautical fields since radio navigational aids such as VOR's and NDB's still identify in Morse Code. The US Navy and Coast Guard still use signal lamps to communicate via Morse Code.[22]

Hand Signals

For the first time in 30 years, the US Army has updated its Visual Signals manual for use when 'electrical and/or digital means of communication are inadequate or not available'.[23] Fighter pilots also use hand signals to communicate with wingmen when radios fail. For example, a hand moving horizontally above the glare shield, palm down, means level off while a hand moving forward means add power.[24]

Free Space Optics and Laser Communications

Free space optics, or FPS, uses high frequency modulated light pulses to transmit data through the spectrum. FPS can transfer data at the rate of tens of gigabits per second over a distance of 'several kilometers near the sea level or even over 100 km at high altitude.' Also important is its high immunity to both interception and jamming and it won't interfere with other transmissions.[25]

Conclusion

The risks to NATO and our member nations when operating in a denied spectrum battle environment is clear. Whether at the command level or the grunt on the ground, when spectrum is denied, the effectiveness of NATO forces is reduced or eliminated. The good news is there are myriad alternatives to turn to, only some of which are mentioned here. What we need to do next is establish a list of spectrum-denied scenarios then train with tactics, techniques, and procedures that provide back-up solutions to meet each scenario. Indeed, by exploiting the tools and skills that we have today, we truly can survive until the promised future capabilities are deployed tomorrow.

Steve 'Tango' Tourangeau is the Vice President and Chief Operating Officer of Warrior Support Solutions, LLC, providing expertise to the DoD, industry and academia to advance Electromagnetic Spectrum capabilities. Tango is a retired Air Force officer with over 1,500 hours as Flight Test Navigator and Electronic Warfare Officer.

Dirk A. D. Smith is an international award-winning technical writer and freelance journalist. He specializes in the research, analysis, writing and presentation/publishing of complex technical knowledge. This work often includes interviewing Subject Matter Experts (SME) for internal and external corporate, military, and intelligence communications.

Endnotes

1. Tyagi, R. K., Col., ‘Understanding Cyber Warfare and its Implications for Indian Armed Forces’, United Service Institution of India, New Delhi, 2013, chapter 3.
2. Marcus, Jonathan, ‘Are Russia’s military advances a problem for NATO?’, BBC News, 11 Aug. 2016.
3. Lin, Jeffrey and Singer, P.W., ‘China shot down another missile in space’, Popular Science, 3 Feb. 2018.
4. Peterson, Scott and Faramarzi, Payam, ‘Iran hijacked US drone, says Iranian engineer’, The Christian Science Monitor, 5 Dec. 2011.
5. Papiewski, John, ‘How Solar Flares Affect Communication’, Popular Science, 24 Apr. 2017.
6. ‘WMO expresses concern about radio frequency decision’, World Meteorological Organization, 27 Nov. 2019.
7. ‘Loss of GPS Signal at Ben Gurian Airport’, IFALPA, 25 Jun. 2019.
8. ‘Russia denies role in Israeli airport GPS jamming’, BBC, 27 Jun. 2019.
9. ‘Afghanistan IED Deaths’, areppim AG, 2008–2020.
10. Thompson, Mark, ‘The Curse of ’Friendly Fire”, TIME, 11 Jun. 2014.
11. Patterson, Caitlin, ‘Russia’s Surging Electronic Warfare Capabilities’, The Diplomat, 19 Apr. 2016.
12. Prudente, Tim, ‘Naval Academy reinstates celestial navigation’, MilitaryTimes, 1 Nov. 2015.
13. ‘Satellite Navigation – WAAS – How It Works’, Federal Aviation Administration, 4 Nov. 2019.
14. ‘Ground-Based Navigation (Part Four) – VOR/DME RNAV’, Flight Literacy.
15. ‘Draper Awarded Patent for Cross Polarizing Star Tracker’, Charles Stark Draper Laboratory, Inc., 25 Apr. 2018.
16. Coast Guard Navigation Standards Manual, COMDTINST M3530.2F, p. 2, Jan. 2020.
17. Strout, Nathan, ‘Could chip-sized atomic clocks replace GPS?’, C4ISRNET, 28 Aug. 2019.
18. ‘Reducing Tics in the Tocks of Atomic Clocks’, DARPA, 23 Dec. 2015.
19. Moore, Carl H., ‘Flying the B-26 Marauder Over Europe: Memoir of a World War II Navigator’, 2nd. Edition, p. 22, Google Books.
20. F4HDK, ‘Build a Long-Distance Data Network Using Ham Radio’, IEEE Spectrum, 25 Oct. 2019.
21. Harper, Jon, ‘Military, Industry Gung-Ho on Software Defined Radios’, National Defense, 15 Feb. 2019.
22. Novel Treasure, ‘Is Morse Code Used Today? The Brief History and Importance of Morse Code’, Owlcation, 18 Feb. 2020.
23. Kravets, David, ‘US Army “Visual Signals” manual gets first update in 30 years’, ars Technica, 1 Apr. 2017.
24. Chesire, John, ‘Do fighter pilots use hand signals to communicate with their wingmen in cases where radios fail or radio silence must be maintained’, Quora, 15 Jun. 2019.
25. Mikolajczyk, Janusz, et al, ‘Analysis of Free-Space Optics Development’, Metrology and Measurements, Polska Akademia Nauk.

© US Air Force

Winning the Invisible War

XIV

Gaining an Enduring Advantage in the EMS

By Ms Whitney McNamara, Mr Bryan Clark and Mr Timothy Walton
Center for Strategic and Budgetary Assessment

Note: This article has been amended for use for this Read Ahead publication. The complete study can be accessed through https://csbaonline.org/uploads/documents/Winning_the_Invisible_War_WEB.pdf.

The explosion of mobile communications and, most recently, the emerging Internet of Things are turning the Electromagnetic Spectrum (EMS) into an increasingly crowded place. The advent of 5G, with its need for wide swaths of spectrum in multiple frequency ranges to enable higher data rates, will only intensify this trend and create more conflicts between commercial and government users. The challenge of spectrum management and control will be even more acute for militaries, which depend almost entirely on the EMS for sensing and communications.

The American military is particularly affected by a congested EMS. US forces deploy the most advanced networks of sensors and precision-guided munitions, relying on them for almost all operations. Adversaries like China and Russia, however, have exploited this vulnerability by developing and fielding during the last decade a comprehensive array of Electronic Warfare (EW) systems to contest the spectrum.

The US military, however, did not address the challenge posed by its competitors and numerous assessments argue the US military is now unprepared for competition or conflict in the EMS.[1] This situation is particularly frustrating as budgets for EMS operations grew since 2015. Those dollars, unfortunately, flowed predominantly to upgrading legacy systems and attempting to fill the most urgent capability gaps as they arose. Regaining EMS superiority against Chinese and Russian forces at the current pace will take one or two decades – assuming US competitors do not increase their efforts.

DoD should accelerate its efforts to regain an advantage in the spectrum, but likely budget constraints will preclude simply throwing more money at the problem. Instead of perpetuating the current move-countermove competition by attempting to fill every EMS capability gap, the DoD should adopt a new approach to EMS operations focused on asymmetries between US and opposing militaries. An EMS strategy designed to undermine enemy strengths and exploit adversary vulnerabilities may leave some capability gaps intact but could be the only way for the US military to regain EMS superiority in time to forestall opportunistic aggression by one of America's military competitors.

Exploiting Asymmetries

The most important asymmetry between US and opposing militaries is the adversary's 'home team' advantage and how it impacts EMS operations. For example, Chinese and Russian forces can exploit their proximity to likely conflicts by employing sensor techniques that rely on multiple stationary arrays such as passive Radio Frequency (RF) detection or geolocation and long-range high-frequency radars. As an expeditionary force, the US military is less able to employ these techniques and often relies on active, monostatic radars for situational awareness and defence, exposing US units to enemy detection and geolocation.

The US has a robust EW and EMSO relationship with North Atlantic Treaty Organization (NATO) allies through the NATO Electronic Warfare Advisory Committee (NEWAC) and Conference of National Armaments Directors (CNAD). The NEWAC is responsible for development of requirements and oversees NATO's EW policy, doctrine, and C2 concepts, and it oversees EW support to NATO operations and exercises. The CNAD oversees acquisition policy and interoperability. However, interoperability with NATO is becoming more difficult, however, with the introduction of new cognitive and networked US EW and EMSO capabilities, which are not being introduced in other NATO militaries. A renewed focus on emerging spectrum technologies from NATO would help improve integrating capabilities and operations, making U.S and its NATO allies a more formidable and coherent force vis a vis Russia in the EMS competition.

Their home team advantage also allows China's People's Liberation Army (PLA) and the Russian Armed Forces to place EW and sensor systems on their own territory, where they can rely on wired communications, or place them in nearby sea or airspace, where line-of-sight RF communications will be reliable and difficult to jam. The relatively uncluttered spectrum near their territory permits Chinese and Russian militaries to pre-plan their spectrum use. As an expeditionary force, the US military must manage spectrum dynamically.

The proximity of US competitors to likely areas of conflict creates additional asymmetries in force design and command and control (C2) between US and competing militaries. Because the PLA understands where conflict is likely to occur, the Chinese forces to be employed, and the likely variety of enemy dispositions and tactics, the PLA can employ an integrated collection of systems designed to paralyze opposing forces' C2, communications and sensors, rather than annihilating the enemy through attrition.

The PLA's operational approach, which Chinese military strategists call System Destruction Warfare, would be implemented through tactics analyzed and agreed to in advance and implemented through pre-architected systems of systems.[2] Although it also uses pre-architected systems to defeat an opponent's C2, the Russian military's operational approach delegates subordinates more authority to improvise tactics. Similar to PLA leaders, however, Russian commanders are expected to use modeling and cybernetics to scientifically lead forces and anticipate combat outcomes.[3]

The worldwide commitments of the US military require a much more flexible force design than those pursued by the Chinese or Russian governments. Today this design centres onmonolithic multimission platforms, such as an F-35 or aircraft carrier, and troop formations, which are efficient but reduce the force's flexibility. Although new DoD concepts such as Distributed Maritime Operations (DMO), Multidomain Operations (MDO), and Expeditionary Advanced Base Operations (EABO) emphasize more distributed formations, DoD's investments still prioritize relatively small numbers of multimission platforms and troop formations that lack the numbers or decision support tools to enable distributed operations The flexibility and complexity the US poses to its adversaries that is possible with traditional forces is constrained by the cost of monolithic multimission units, which limits their number. Furthermore, the co-location of all the kill chain elements in a single platform or formation constrains the number of independent paths and nodes possible in a force package. The high value of multi-mission units also requires they be protected, which limits the flexibility possible in the configuration of associated forces.

US forces also need a more adaptable C2 process than competing militaries to accommodate more contested communications, changing force packages, and local conditions. The US military employs 'mission command', a concept that relies on the judgement and ability of junior leaders of tactical elements to follow the commander's intent if communications are lost.[4] A lack of planning and management tools available at the tactical level currently hinders their ability to innovate, however, making their actions more predictable to an adversary.

A Return to Manoeuvre Warfare

To regain EMS superiority, DoD should focus on exploiting asymmetries in ways that could undermine adversary strengths or exploit enemy vulnerabilities. Most prominently, the home team advantage of US adversaries could be turned into a weakness if DoD adopts new warfighting approaches that emphasize manoeuvre and complexity over attrition. For example, the PLA's reliance on relatively static systems of systems and tactics results from its proximity and understanding of likely conflicts, but more dynamic and unpredictable US force postures and capabilities would partially obviate the PLA's planning and degrade its ability to fight in its near abroad. More dynamic and unpredictable US EMS operations could be especially damaging to Chinese and Russian operational concepts that centre on defeating US C2, communications, and sensors.

To fully exploit the potential of manoeuvre warfare, the US military should replace some of its self-contained multimission platforms that result in highly predictable force packages and tactics with cheaper and less multifunctional units to create a disaggregated and recomposable force. Multimission platforms and multifunctional units are designed to individually address a wider range of threats but because of their sophistication, the difficulty of quickly changing hardware or software components reduces the pace of US military innovation.[5] Replacing a small portion of today's multimission ships, aircraft, or troop formations with smaller, cheaper and less multifunctional units would be enough to enable greater adaptability in US forces packages while imposing considerable complexity on adversaries.

This would enable greater adaptability in US force packages while imposing considerable complexity on adversaries. A more disaggregated force would better enable the US military to conduct EMS operations that would be more challenging for an enemy to detect and counter, including passive and multistatic sensing, distributed EW, and decoy operations.

A more disaggregated force will be difficult to manage, however, in a contested communications environment. Instead of DoD's current trend toward centralized staffs and resilient wide-area communications for distributed operations, the US military should adopt context-centric C2 and Communications (C3). In this approach, C2 relationships are based on communications availability, rather than trying to build a communications architecture to support a pre-determined C2 hierarchy. An essential element of context-centric C3 is planning tools to enable junior leaders at to creatively plan, adapt and recompose their forces and operations. These tools are already being developed and fielded by DoD labs and industry.

The US military's over-reliance on active monostatic radars will prevent it from creating complexity and uncertainty for an adversary, because these sensors can be detected, classified, and geolocated relatively easily. To more fully support manoeuvre and adaptability, US forces should increasingly use more passive or multistatic sensing, complemented by Low Probability of Intercept/Low Probably of Detection (LPI/LPD) communications and electronic countermeasures.

To support passive and multistatic sensing, every US EMS system should also incorporate Electronic Support (ES) capabilities. US forces will increasingly need to reduce or eliminate their active emissions and find enemy targets using passive geolocation, passive radar, or other covert techniques provided through ES. ES capabilities would also help achieve LPI/LPD characteristics, improve the effectiveness of EW actions, and coordinate EMSO operations with minimal communications. Having an organic ES capability would also enable each system to sense the environment and coordinate friendly force actions in the EMS using onboard Electromagnetic Battle Management (EMBM) programs. Introducing multifunction systems to US forces would increase the variety of locations from which sensing or effects can be provided and would also provide greater adaptability to US forces and create complexity for the adversary, in line with manoeuvre warfare.

Fully exploiting networked and multifunction capabilities to operate at machine speed will require operators to yield some decision-making to the EMSO system. Today, adaptive algorithms that can react to adversary actions are reaching EW systems in operating forces. These programs should be accelerated, along with efforts to establish testing processes and data governance procedures for future cognitive EMSO systems. The most significant impediments to networked EMSO and EMBM are creating interoperable data transmission standards and the varied security levels at which different EMSO systems operate.

EMS manoeuvre and superiority only have meaning if DoD treats the EMS as an operational domain. Today's approach to EMS operations treats the EMS as a utility, in which actions such as ES, Electronic Attack (EA), and Electronic Protection (EP), communications, and sensing are distinct operations. In a domain construct, these actions would be considered as interrelated operations that can be employed in concert to accomplish the commander's intent and tasking through manoeuvre in the EMS.

Implementing a New Electromagnetic Spectrum

Moving toward(s) a force that is more disaggregated and recomposable would have significant implications for how DoD identifies and develops new capabilities. To that end, DoD should adopt a more opportunity-based rather than a requirements-based innovation process, which would improve DoD's ability to incorporate commercial technologies and accelerate the fielding of new EMSO systems. Whereas a requirements-driven development process identifies needs for new capabilities, a systems development process would identify opportunities to improve the force's performance in important missions.

Finally, the DoD will need to restore its EMSO range facilities for US forces to regain their operational proficiency, develop new operational concepts and tactics, and evaluate the impact of new capability opportunities. Ongoing efforts to upgrade live open-air ranges to modern threats is an ineffective approach due to operational security concerns. DoD should shift its emphasis for EMSO practical training to virtual and constructive facilities, which would enable EW and EMSO concept development, tactics innovation, and proficiency training against the most challenging threats at all security levels. Live EMSO training would still be needed to practice mechanics of EMS operations; however, these operations could focus on less-modern threats or could employ closed-loop radar, communication, and EW systems.

Instead of reacting to adversary moves with its own countermoves, DoD should move in a new direction to gain the ability to achieve EMS superiority and take back the initiative in EMSO. If the DoD does not mount a new, more strategic and proactive approach to fighting in the EMS and developing the requisite capabilities, adversaries could be emboldened to continue their ongoing efforts to gain territory and influence on their peripheries at the expense of US allies and partners.

Whitney Morgan McNamara is a Senior Analyst at the Center for Strategic and Budgetary Assessments. She received her M.A. in Strategic Studies and International Economics from the Johns Hopkins School of Advanced International Studies where she was a Bradley Fellow and a Presidential Management Fellowship Finalist.

Bryan Clark is a Senior Fellow at the Center for Strategic and Budgetary Assessments. At CSBA he has led studies in naval warfare, electromagnetic warfare, precision strike, and air defence. Mr Clark was an enlisted and officer submariner, serving in afloat and ashore submarine operational and training assignments.

Timothy A. Walton is a Research Fellow at the Center for Strategic and Budgetary Assessments. Mr Walton focuses his research and analysis on the development of new operational concepts, trends in future warfare, and Asia-Pacific security dynamics. He has a Master's degree in Security Studies from Georgetown University.

Endnotes

1. The most significant recent authoritative EW studies include the following: Defense Science Board (DSB), 21st Century Military Operations in a Complex Electromagnetic Environment (Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, 2015), available at https://apps.dtic.mil/dtic/tr/fulltext/u2/1001629.pdf; Government Accountability Office, Electronic Warfare: DOD Actions Needed to Strengthen Management and Oversight (Washington, DC: US Library of Congress, 2012), available at https://www.gao.gov/assets/600/592211.pdf; Madison Creery, 'The Russian Edge in Electronic Warfare,' Georgetown Security Review, 26 Jun. 2019, available at https://georgetownsecuritystudiesreview.org/2019/06/26/the-russian-edge-in-electronic-warfare/; and Robert O. Work and Greg Grant, Beating the Americans at their Own Game: An Offset Strategy with Chinese Characteristics (Washington, DC: Center for a New American Security, 2019), especially p. 7, available at https://s3.amazonaws.com/files.cnas.org/documents/CNAS-Report-Work-Offset-final-B.pdf?mtime=20190531090041.
2. Engstrom, Jeff, Systems Confrontation and System Destruction Warfare (Santa Monica, CA: RAND Corporation, 2018), p. 27.
3. McDermott, Roger N., Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum (Tallinn, Estonia: International Centre for Defence and Security, Sep. 2017), p. 8.
4. US Army Training and Doctrine Command (TRADOC), The Army in Multi-Domain Operations 2028 (Ft. Eustis, VA: TRADOC, 6 Dec. 2018), pp. 32–44, available at https://www.tradoc.army.mil/Portals/14/Documents/MDO/TP525-3-1_30Nov2018.pdf.
5. Clark, Bryan, Daniel Patt, Harrison Schramm, 'Mosaic Warfare: Exploring Artificial Intelligence and Autonomous Systems to Implement Decision Centric Operations.' Center for Strategic and Budgetary Assessments. Washington, D.C. Feb 2010., p.14.

© posteriori/shutterstock

Gaining Competitive Advantage in the Gray Zone

XV

Courtesy of the RAND Corporation

Note: This is an excerpt from the main paper that can be accessed through www.rand.org/pubs/research_reports/RR2942.html.

Response Options for Coercive Aggression Below the Threshold of Major War

The 2017 US National Security Strategy and the publicly released summary of the 2018 National Defense Strategy agree on one fundamental theme: The United States is entering a period of intensifying strategic competition with several rivals, most notably Russia and China. Numerous statements from senior US defense officials make clear that they expect this competition to be played out primarily below the threshold of major war – in the spectrum of competition that has become known as the gray zone.

Although such tactics as psychological warfare, subversion of political systems, and covert paramilitary and information operations are not new phenomena in international conflict and competition, our analysis shows that some of the tactics employed by Russia and China are comparatively new in form and effect. Moreover, the methods of gray zone coercion vary significantly between Russia and China and require differentiation of scope of threat posed to the United States, as well as types of potential responses. Both problems represent a strategic threat to US and allied interests, especially as techniques and technologies evolve over time. The United States and its allies, we find, have yet to come to terms with the challenge of the threat, let alone fashion a strategy to neutralize it or roll it back.

In this project, therefore, we aimed to provide a framework for conceptualizing the gray zone challenge and offer new policy options for the United States and its allies to consider in response. Despite the challenges involved, one finding of this research is that the United States can treat the ongoing gray zone competition more as an opportunity than a risk: By seeking to coerce, acquire influence within, or destabilize key countries and regions, Russia and China are opening the space for a vigorous US campaign to rally allies and partners in both regions in the direction of an effective response. This report uses insights from our extensive field research in affected countries, as well as general research into the literature on the gray zone phenomenon, to sketch out the elements of a strategic response to this challenge.

To inform such a response, we sought to (1) identify a potential strategic concept to govern a US strategy in the gray zone and (2) identify and evaluate a menu of specific response options. It is important to emphasize that the scope of this study is to offer a menu of options that could be of utility to US policymakers in both establishing a general strategy and choosing specific actions in response to gray zone tactics.

We do not seek to offer a judgment of the relative efficacy of specific courses of action for discrete gray zone events or an assessment of how the adversary may respond; this should be the objective of follow-on research. The study focused on Russian and Chinese gray zone activities and potential US and partner responses to them; we did not consider the gray zone tactics of other challengers.

Our primary source of information to support this analysis was an extensive program of field research in spring 2018. We traveled to Australia, the Czech Republic, France, Germany, Indonesia, Japan, the Philippines, Poland, Singapore, the United Kingdom, and Vietnam to gather perspectives on the ongoing gray zone challenge. We also interviewed officials and scholars in Washington, D.C., including several from the Republic of Georgia, and we met with current and former national security officials, scholars, and researchers.

In addition, we reviewed the existing literature on gray zone challenges for possible response options, as well as the literature on deterrence for its possible lessons for the gray zone context. We relied on all of these sources of information to construct a potential strategic concept for gray zone competition and to inform our evaluation of specific response options.

The set of response options offered in this report is designed to offer an initial draft of a living document. The menu of options ought to be fleshed out and refined over time based on experience and further consultations. We do not pretend that the options offered here are comprehensive or optimal even now. And new ideas will emerge as the United States and its allies and partners gain more experience in this realm.

A Concept for Gaining Strategic Advantage in the Gray Zone

Not all gray zone activities are alike. Responses to more-aggressive gray zone activities will not necessarily mirror those of more-gradual, persistent initiatives. Any strategic concept for the gray zone therefore must distinguish among the various levels and design its responses accordingly.

Admittedly, the dividing lines between levels of gray zone tactics will not be precise or well defined in all cases. Rather, they are designed to convey three general conceptual ideas rather than three clearly defined baskets. The three general levels of gray zone activities are (1) aggressive actions, at one end of the spectrum, that the United States should seek to deter; (2) persistent actions, at the opposite end of the spectrum, that it must live with but can compete against; and (3) moderate actions in the middle that the United States should actively seek to discourage over time. As part of this study, we offer a specific framework for distinguishing levels of gray zone actions, and these distinctions then become the basis for the response concept.

Any division of gray zone activities points to one especially critical implication and a theme that our research suggests is essential to any US response strategy. The United States and its allies, partners, and friends must decide what actions they will resolutely not tolerate in the gray zone environment. Because of the difficulty in stopping gradual, sometimes unattributable actions involving secondary interests, identifying the actions that the United

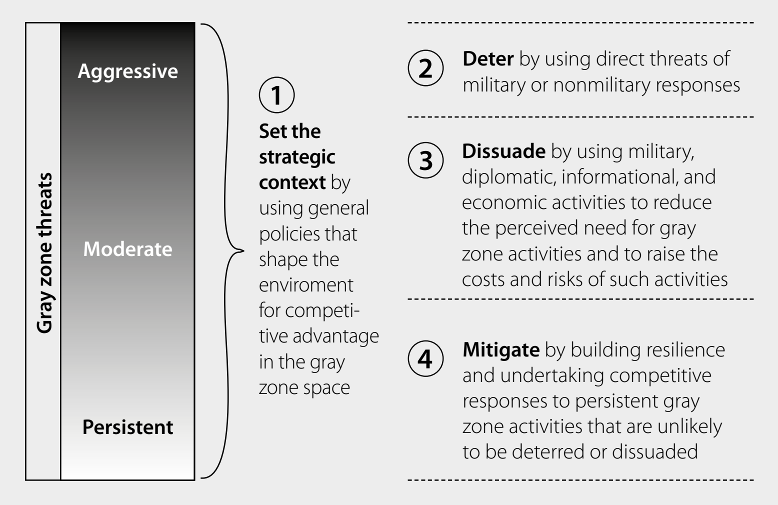

Gray zone threats
Aggressive
Moderate
Persistent
1
Set the strategic context by using general policies that shape the enviroment for competitive advantage in the gray zone space
2
Deter by using direct threats of military or nonmilitary responses
3
Dissuade by using military, diplomatic, informational, and economic activities to reduce the perceived need for gray zone activities and to raise the costs and risks of such activities
4
Mitigate by building resilience and undertaking competitive responses to persistent gray zone activities that are unlikely to be deterred or dissuaded

***Figure S.1:** Overarching Strategic Concept for Responding to Gray Zone Threats*

States will seek to deter is the one reliable way to draw a boundary around the possible effects of gray zone encroachment. With this conception of a spectrum of gray zone activity levels, we outline a four-part framework for responding to gray zone threats, shown in Figure S.1.

The proposed strategic concept for the gray zone has four major components. It first calls for a whole-of-government approach utilizing geopolitical, military, and economic actions to shape the strategic context. Second, it proposes that the United States should identify a small number of aggressive gray zone tactics to deter with explicit, credible threats of military or nonmilitary responses. Third, it seeks to dissuade a wider range of moderate gray zone activities over time. Finally, it calls for mitigating persistent threats by building a capability for resilience and competitive response to threats that cannot be deterred or dissuaded.

The remaining task for US strategists is then to draw on a rich menu of specific tools, techniques, and capabilities to formulate both ongoing and event-specific responses to gray zone provocations. As part of this study, we laid out a roster of such options. In the process, we did not attempt to build a scripted playbook that specified responses to every plausible Russian or Chinese action. The reality of gray zone competition is too fluid for that, and specific contexts will demand different responses to the same action. Instead, we aimed to assemble a menu from which US officials can choose in such situations, evaluating each potential response option according to three criteria: its potential advantages and benefits, its potential risks and costs, and other considerations derived from our research. In no case do we make a final evaluation of the advisability of any given option in a given situation; that will depend on the specific circumstances when each response takes place.

A multicomponent strategy like the one outlined here will be of limited utility if the US government continues to lack a clear coordinating function with the responsibility for overseeing a renewed effort to gain strategy advantage in the gray zone. An important part of any gray zone response strategy, therefore, is undertaking institutional reform. A major difficulty given the current organization of key US national security departments and agencies is that there is no single ideal home for a gray zone management function. The National Security Council is not an operational body, and it has a small staff devoted to coordinating policy rather than running multicomponent campaigns. The State Department has personnel and funding shortfalls and lacks interagency coordination authorities. It also often lacks an institutional mindset needed for aggressive countermeasures. Finally, placing a gray zone coordinating function solely at the Defense Department risks encouraging a dominant focus on military tools, which would not reflect the character of the challenge.

In considering alternatives for a fresh approach, we assessed two basic options. One can be described as the thin option and would use a presidentially directed strategy, perhaps issued in the form of a National Security Presidential Directive or other White House order, as the foundation of the approach. The order would outline the elements of a gray zone response concept and direct the actions of specific departments and agencies in support. It would then be coordinated by the National Security Council, under a senior director office devoted to the purpose.

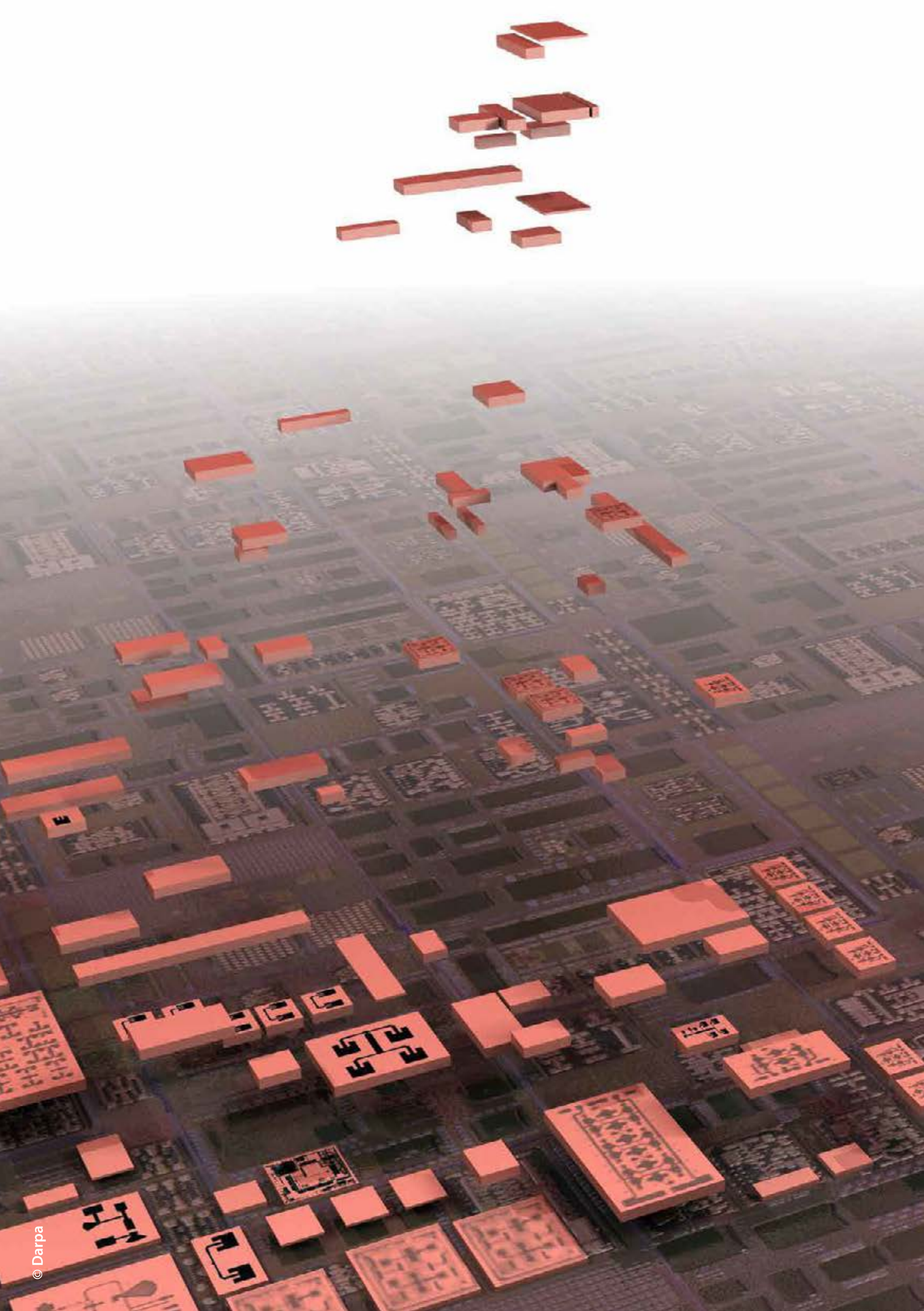
Another alternative could be described as the thick option. This would assemble a more purpose-built office in the US government, with a significant devoted staff, to run counter–gray zone campaigns. It could be headed by a presidential special representative with the highest subcabinet rank and a direct reporting line to the president.

We looked at the National Counterterrorism Center for insights into launching a new, focused organization, although that model is designed to promote information-sharing and strategic operational planning more than the operational control of the strategy. This more elaborate option for institutional change could even include the development of regional implementation offices – the equivalent of military combatant commands – to run the gray zone campaigns in those areas (at a minimum, in Europe and Asia).

Whatever option is chosen, the US government can take several accompanying steps to give the gray zone strategy the necessary profile in national security planning. These steps include the following:

- Make the issue a special focus in state and Defense Department regional offices, ensuring the necessary staff support to track evolving gray zone activities on their own terms.
- Require that responses to gray zone activities be included as a prominent theme in relevant embassy country strategies.
- Require military service initiatives to emphasize gray zone issues in, for example, career development; training and education; and the funding and support for technologies, capabilities, and experimental force design and concepts tailored to the gray zone.

The **RAND Corporation** is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest.



© Darpa

DARPA Tiles Together a Vision of Mosaic Warfare

XVI

Banking on Cost-effective Complexity to Overwhelm Adversaries

Courtesy of Defense Advanced Research Projects Agency

Online Article at: https://www.darpa.mil/work-with-us/darpa-tiles-together-a-vision-of-mosiac-warfare.

The concept is called 'Mosaic Warfare'. Like the ceramic tiles in mosaics, these individual warfighting platforms are put together to make a larger picture, or in this case, a force package.

The idea will be to send so many weapon and sensor platforms at the enemy that its forces are overwhelmed. The goal is to take complexity and to turn that into an asymmetric advantage, said Burns, who retired this past May (2018) as director of DARPA's Strategic Technology Office (STO), handing the leadership baton off to Timothy Grayson.

'When you attack in parallel across a wide front and you have distributed your sense-decide-and-act systems across a wide number of platforms, you can mass your firepower without having to mass your forces,' said

Burns, who is credited with getting talk about the Mosaic Warfare concept going in Department of Defense circles.

The DARPA hard problem is that today's weapon systems are not built to function this way, Burns said. 'They are more like pieces of a puzzle than tiles for a mosaic. They are exquisitely engineered to fit into a certain part of the picture and one part only. You can't pull it out and put in a different puzzle piece. It won't fit,' he said.

One way Mosaic Warfare might work in a ground battle would be to send an unmanned aerial vehicle or ground robot ahead of the main ground battle force. It might spot an enemy tank. The unmanned system passes the coordinates back, which are then relayed to a non-line-of-sight strike system in the rear, which in turn launches its munitions and takes out the target.

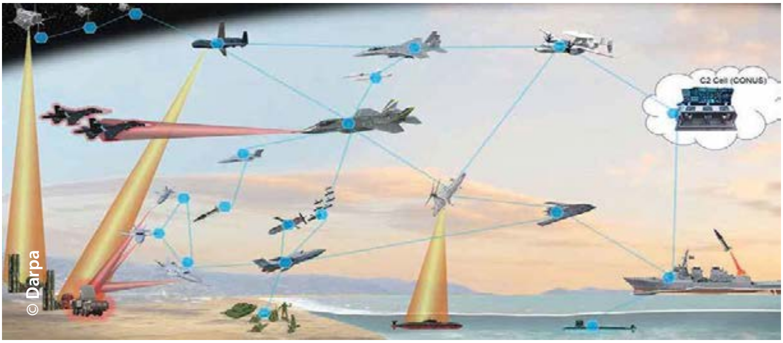
'It sounds like it should be something very doable, but it's not right now,' said Burns. 'The interfaces are not made to communicate that kind of information and the Army doesn't have air and ground vehicles that it can send forward,' he added.

In the air domain, four F-16s might be going head-to-head with four rival jet fighters. However, in a Mosaic Warfare context, the US Air Force might also deploy four relatively inexpensive, somewhat expendable unmanned aerial systems ahead, each with different weapons or sensor systems. The combatant commander can treat these assets like a football coach who chooses team members and then positions them on the field to run plays. The added aircraft make the situation much more complex and can overwhelm the opponent's decision-making.

'It makes us more lethal and a lot more survivable,' Burns said. But like a football play, things don't always unfold as planned. The autonomous systems and pilots must be able to adapt, especially as the mission changes or unexpected events occur. And commanders in a Mosaic Warfare context would have the option of substituting new components and systems as parts of the initial mosaic composition are lost or they want to deploy a new tactic that requires different capabilities. John Waterston, a Program Manager in the STO and a Navy Reserve officer, said Mosaic Warfare may impose even more complexity on the adversary in the maritime domain, because it encompasses a diversity of environments: air, land, sea, and undersea. His charge now is to figure out how ships, submarines, aircraft, and unmanned systems all can work together to achieve a mission.

The organization and war-planning task almost surely would cross services as well, as combatant commanders mix and match assets. This fits into recent joint multi-domain battlefield concepts that Pentagon leaders have been talking about. These decision-makers acknowledge that going up against peer and near-peer competitors means having to protect forces from threats that could be coming at them from any domain – ground, air, space, sea, and/or cyberspace.

'You want to leverage the best characteristics of different platforms,' Waterston said. 'It all gets down to where do you have access and capacity, and distributing them properly so all your eggs aren't in one basket.'



© Darpa

Joint-Multi-Domain Concept

'We keep making awesome stealth fighters, or better submarines, and better and better unmanned systems,' Waterston elaborated. 'The thinking is: Why don't we take simpler systems and then network them together, have them share, collaborate – sense their world in their own unique way – and put them together?'

Expendability (attritability in military speak) is key, Burns said. Conventional wisdom says U.S. forces shouldn't fight in the open. 'You'll be killed. But if you have large numbers of expendable platforms, you can fight in the open,' he said.

Again, the problem is that to create these systems of systems, they need to be linked together, Waterston said, highlighting the challenges here by pointing to recent reports that the new F-35A and the F-22, the Air Force's two most sophisticated fighters, cannot stealthily share data.

Burns said the Strategic Technology Office's goal is to create the interfaces, communications links, and the precision navigation and timing software – the technology backbone – to allow these exquisite systems to work together. On PowerPoint illustrations of battlefields, these communication links are often portrayed with lightning bolts. 'One of our mottos is to make lightning bolts real,' Burns said.

For a concept that welled up from DARPA, rather than from the services, think tanks, or war colleges, Burns said that Mosaic Warfare – a term coined by Burns and his former deputy director Dan Patt has been relatively well received during briefs to military leaders.

For Patt, Mosaic Warfare is 'about an effective warfighting whole made up of many diverse and fluid pieces. How can you get all these little pieces all aligned toward a common objective without perfect communications and without planning everything in advance? It's really hard. And that's the idea of Mosaic Warfare.'

There is a direct line in thinking from the Chinese military strategist Sun Tzu and his treatise, The Art of War, to the Mosaic Warfare concept, said Patt, who is now CEO of Vecna Robotics and a non-resident Senior Fellow at the Center for Strategic and Budgetary Analysis, a Washington, D.C. –based think tank.

© Dynetics

Asymmetric Advantage

'All ideas are present in Sun Tzu. But when these ideas are applied for the first time, it can give an asymmetric advantage,' he said, citing Germany's blitzkrieg tactics in World War II as an example, where an overwhelming force of armor, motorized infantry, artillery, and air power combined to force a local breakthrough that could then be exploited to continue the advance.

The so-called 'Second Offset' strategy following the Vietnam War, which matured into the air-land battle concept, called for airborne sensors and missiles that could work together to overpower a large Soviet army without having to escalate to nuclear warfare. Also known as Assault Breaker, the strategy is centered on the deployment of a system of systems, Patt said.

The problem with that approach was that it was 'very brittle,' he said. It took years of engineering to ensure one system could link with another system.

© PHC D. W. HOLMES II, US Navy

Second Offset Strategy

'They brought together a couple pieces and it did offset Soviet capability,' Patt said. 'But it wasn't a particularly easy or scalable approach. There were a lot of challenges to make that work fluidly. Today, it is still difficult for systems to share information with each other.'

'There has to be a better way. And the technologies DARPA is developing are about that better way,' Patt said.

Another benefit of Mosaic Warfare is that it makes the kill chain more resilient, Patt said. The sense-decide-act decision loop has also been around since the days of Sun Tzu, or longer, he said. More recently, the U.S. military refined the idea to the observe-orient-decide-act decision cycle, or OODA loop.

If a commander could unbundle those functions, everything that has a sensor could be connected to everything that can make a decision, and then to anything that can take an action. 'That is really powerful, because mathematically, you expose all the possible combinations and create thousands upon thousands of connections,' Patt said. Those thousands upon thousands of connections force an enemy to contend with many possible combinations of attacks as well.

'That gives resilience. It doesn't matter what the enemy does, the [blue force] still has options for completing a kill chain.'

Many of the platforms that could be used for Mosaic Warfare already exist. Nevertheless, work continues on developing unmanned platforms that could be applied to the concept.

Waterston said the next step for Mosaic Warfare, and an all-important one, will be demonstrating how it all works.

'Operational commanders aren't going to use these systems if they haven't been tested and demonstrated,' Waterston said. 'They have to trust them.'

For sixty years, **DARPA** has held to a singular and enduring mission: to make pivotal investments in breakthrough technologies for national security. DARPA comprises approximately 220 government employees in six technical offices, including nearly 100 program managers, who together oversee about 250 research and development programs.

NATO INFORMATION AND COMMUNICATORS' CONFERENCE
WARSAW
NATO
OTAN
POLAND - SEPTEMBER 2019

© ACT. NATO

SACT's Address NICC Warsaw

XVII

SACT's Address to The NATO Information and Communicators' Conference (NICC), Warsaw, 23–27 September 2019

Gen André Lanata, Supreme Allied Commander Transformation

Online Article at: https://www.act.nato.int/application/files/1415/7290/8629/190925_nicc.pdf.

Ladies and gentlemen, Welcome to the 2019 NATO Information and Communicators' Conference. This year, Allied Command Transformation is organizing this important event, and I want to thank our friends from Poland for hosting us in Warsaw.

In particular, I thank the Minister of Defence, Mr Mariusz Błaszczak for opening the conference.

I would also like to extend my personal thanks to those from NATO HQ for their strong involvement and support, especially Assistant Secretary General for Public Diplomacy, Ambassador Tacan Ildem and, NATO Spokesperson Ms Oana Lungescu.

Most importantly, I thank you all for participating. And, I urge you to take the discussions from your working groups, workshops and plenary discussions back to your commands, centres and institutions, to your commanders and leaders, and continue improving our military culture and NATO's effectiveness in the information environment.

While I cannot be with you in person, I want to share my thoughts on the importance of the continuous development of different communications disciplines: Strategic Communications, Military Public Affairs, Information Operations and Psychological Operations.

The conference is taking place in the middle of the adaptation of NATO's command structure and increasing competition in the information environment. It is also taking place in a year in which we celebrate NATO's 70th anniversary. The anniversary of an open and transparent alliance, built on freedom, democracy, individual liberty and the rule of law.

Our cohesion, based on mutual trust and solidarity is the key of our success and longevity.

In our increasingly interconnected and networked world, our potential adversaries recognize the information domain and seek to exploit perceived weaknesses. And, certainly, in democratic nations there will surely be fissures that can be exploited. And, information, or better say – disinformation, is, among other asymmetric means, an important instrument that our adversaries use in their approaches.

We count on you, NATO's team of networked communicators, to help us understand the information environment and to prepare us to rapidly identify and counter malicious actions in the future like we do it today. And, we also have to build our resilience against possible strategic shocks in the information domain, as much as possible.

Make no mistake: Information may be weaponized.

Technologies such as Artificial Intelligence may be used as a 'weapon of the weaker'. A weaker in terms of conventional military capabilities, but capable of harnessing new technologies in non-kinetic, information domain. These new technologies may be applied to use personal data to build better microtargeting capabilities in an effort to control public opinion. This is why we not only need to understand the dynamics of media, social networking and our common need to relate and share deeply personal information. But, we also need to understand and use the potentials of new, disruptive technologies relevant to this domain.

I will illustrate it with one of ACT's particular line of efforts, which is development of the Information Environment Assessment (IEA) capability. It aims at assessing the perception of our populations and potential adversaries of NATO strategic message, even with the weak signals.

This capability aims at allowing us to assess the effectiveness of NATO deterrence, especially in hybrid threat environments. We experimented it during the last year's Trident Juncture exercise and this effort received a valuable support and recognition from Assistant Secretary General for Public Diplomacy.

You are the front-line warfighters in this increasingly contested information environment. It is of paramount value for the Alliance to ensure you are resourced, trained, operating and succeeding like never before.

Again, thank you for your participation. I assure you, I will follow the outcomes of your discussions with a great interest. I wish you a very successful conference and many fruitful discussions.

Battlespace Management

Battlespace Management Panel Introduction

XVIII

Future NATO Battlespace Management Requirements

By Lt Col Zenon Kot, POL Air Force

Joint Air Power Competence Centre

> ***'We have to put aside the comfortable ways of thinking and planning, take risks and try new things so that we can prepare our forces to deter and defeat adversaries that have not yet emerged to challenge us.'[1]***
>
> ***Donald Rumsfeld, US Secretary of Defense, Feb 2002***

Introduction

According to Alliance Joint Doctrine, which describes how operations should be conducted, 'Battlespace Management (BM) is necessary adaptive means, measures and procedures that enable the dynamic synchronization of activities in the modern battlespace.'[2] Traditionally, the battlespace was seen as a geographically defined area with clear boundaries that designated the 'Area of Operations' (AOO). In modern warfare, with Space, Cyberspace, EMS and the information domain included, the battlespace will extend well beyond these traditional boundaries. However, the fundamental functions and objectives of BM are unchanged. BM is a process that facilitates and seeks to maximize operational effectiveness, minimize constraints, and contributes to reducing the risk of fratricide. It should coordinate and synchronize activities of all force elements, including non-NATO actors, which makes the task more difficult. Also, BM should produce a high level of Situational Awareness (SA)[3] by mitigating friction caused by the existence of boundaries and seams between all force elements.

NATO's Focus

Due to constantly changing BM conditions and new requirements, NATO should focus more attention on a change of mindset and a different approach to future modern warfare. The Alliance needs to embrace and employ new emerging technologies and processes to exploit/gain additional advantages through information sharing. Figuring out how to stay a step ahead and be ready for any adversary's unexpected activity in a modern congested and ever-growing battlespace is critically important. Particularly when information flow needs to be managed in real-time to allow commanders to make the most appropriate decisions to achieve coalition goals. NATO needs to change its thinking from the orthodox to the decidedly unorthodox.

There is also a strong need to become more agile. Decision-making processes will increase in tempo and necessitate real-time decisions. All entities involved in a conflict need to use emerging technologies to support BM in order to make it as effective as possible.

The Joint All-Domain Fight

For the foreseeable future operations will most likely employ more than one force element and take place in more than one operational domain (land, sea, air, space, and cyberspace). At the same time, while remaining invisible to the naked eye, the whole range of the Electromagnetic Spectrum (EMS) needs to be constantly explored and monitored to detect adversary activity to allow swift and timely reactions, in some cases even preemptive actions. Additionally, more than two nations will more than likely be involved in any future conflicts, which is especially true for collective NATO defence which brings with it several important aspects that need to be carefully examined. What is more, the battlespace will not be exclusive to only military actors and activities. Recent conflicts and current trends have shown that adversaries will use high-end equipment to create havoc anywhere which can be favourable for achieving their goals.

The question then becomes how to react in this type of situation, how do we maintain positive control of the situation? Command & Control (C2) processes need to be reviewed and adopted to confront the new reality and meet new challenges. Due to the high density of information flow, different players, and multiple environments, effective BM is essential. Proper BM provides to all allied forces synchronized Situation Awareness (SA) which is critical, and required, to avoid any mistakes which can have a negative impact on allied forces. But how to manage the excessive amount of information in a manner accessible for all allied users? The answer may lay in Artificial Intelligence (AI), which can significantly support human interactions, without the need to limit their leading role.

New Approaches

How then to use the **capability of a machine to imitate intelligent human behaviour?** It is commonly known that there is a big difference between theory and practice. Instead of meeting standardization requirements, there will inevitably be a situation when during an operation some forces will use outdated equipment, which has not been upgraded to meet NATO standards. But it might be not enough to merely meet agreed-upon BM requirements, as the amount of data needed to be received and processed is ever increasing. This situation forces all BM elements to think about new approaches to the data management and force users to implement emerging technologies to support commanders' processes, as well as seek ways gain the ability to exploit AI for C2.

Additional Articles

This section presents five related articles which will introduce various ideas and issues related to the Battlespace Management, and the different challenges NATO faces therein. The ideas expressed in this article are meant to prepare those attending the 2020 Joint Air & Space Power Conference for the panel discussion on Battlespace Management:

- Lt Col Asger Pilgaard's (DNK Air Force) article, Exploiting AI in Command and Control of the Air Battlespace, refers to a current study that intends to exploit AI in the Air Command and Control planning cycle (AirC2) in a Joint Force Air Component (JFAC). A decisive deliverable of the study will be a demonstrator linked to an 'AI agent'[4] that can create options to assist air planners and diminish their workload as well as recommend options for the JFAC Commander. Implications, opportunities and risks associated with AI will require continued ethical and judicial discussions.

- Artificial Intelligence promises to enhance speed and accuracy of military decision-making, i.e. in particular shortening the operational C2-cycle. Mr Daniele Frisoni therefore analyses the *Potential Impact of AI on Command and Control Systems*[5]. He shows how AI relates to Machine Learning (ML) and Deep Learning (DL), underlines that the use of new technologies like AI require a cost-benefit analysis of all relevant aspects, makes us aware that a learning systems can be only as good as the data it learns from and emphasizes the importance of verification and validation for AI-based algorithms. The main part of his article provides an overview of some C2 functions that may particularly profit from AI technologies and identifies track classification as currently one of the most promising areas of application which is further explained and analysed. Machine Learning classifiers will not yet replace the legacy classifier bit operate in parallel. In mission critical applications, the human operator will not be removed from the decision loop.

- Ms Gentry Lane, in *Harnessing AI and Deep Learning*[6], makes us aware how our Informational Technology (IT) and Operational Technology (OT) networks are attacked with 'fileless malware' or through 'data integrity attacks' and what we can do to quickly detect them. Moreover, she ('explores' or 'advocates') an approach that shifts the 'tactical advantage to the defender'. Analysis supported by Artificial Intelligence and Machine Learning should enable discovery of 'fileless malware' and 'low-observable characteristic' attacks in near real time. A comprehensive analysis of all IT and OT systems across all branches, i.e. a 'big-picture analysis' will provide a clearer view of breach behaviour over time and enable accurate predictions. An essential requirement to support this approach will be a sharing of both real time and predictive data over secure channels because the privacy of forensics and anomaly detection is crucial for military operations.

- From Christophe Fontaine's article, *New Medium Altitude Long Endurance (MALE) capabilities including AI will power NATO's cross-domain Joint ISR*[7], we see predictions that AI will play an important role. It argues these new technologies have moved beyond the drawing board. The first generation of Remotely Piloted Aircraft (RAP) MQ-9A 'Reaper' is an example that flight duration is not a limitation now like it is for currently still used AWACS system fleet, where crew working time limitations impose significant limitations on mission lengths. It looks like the new RPA will be able monitor (occupy) airspace by staying on station more than 40 hours to provide information from over a target area. Beyond the horizon transmission will no longer be a problem thanks to satellite links and laser transmission availability. C2 systems will be supported relevant to operational information without any interruption or security degradation.

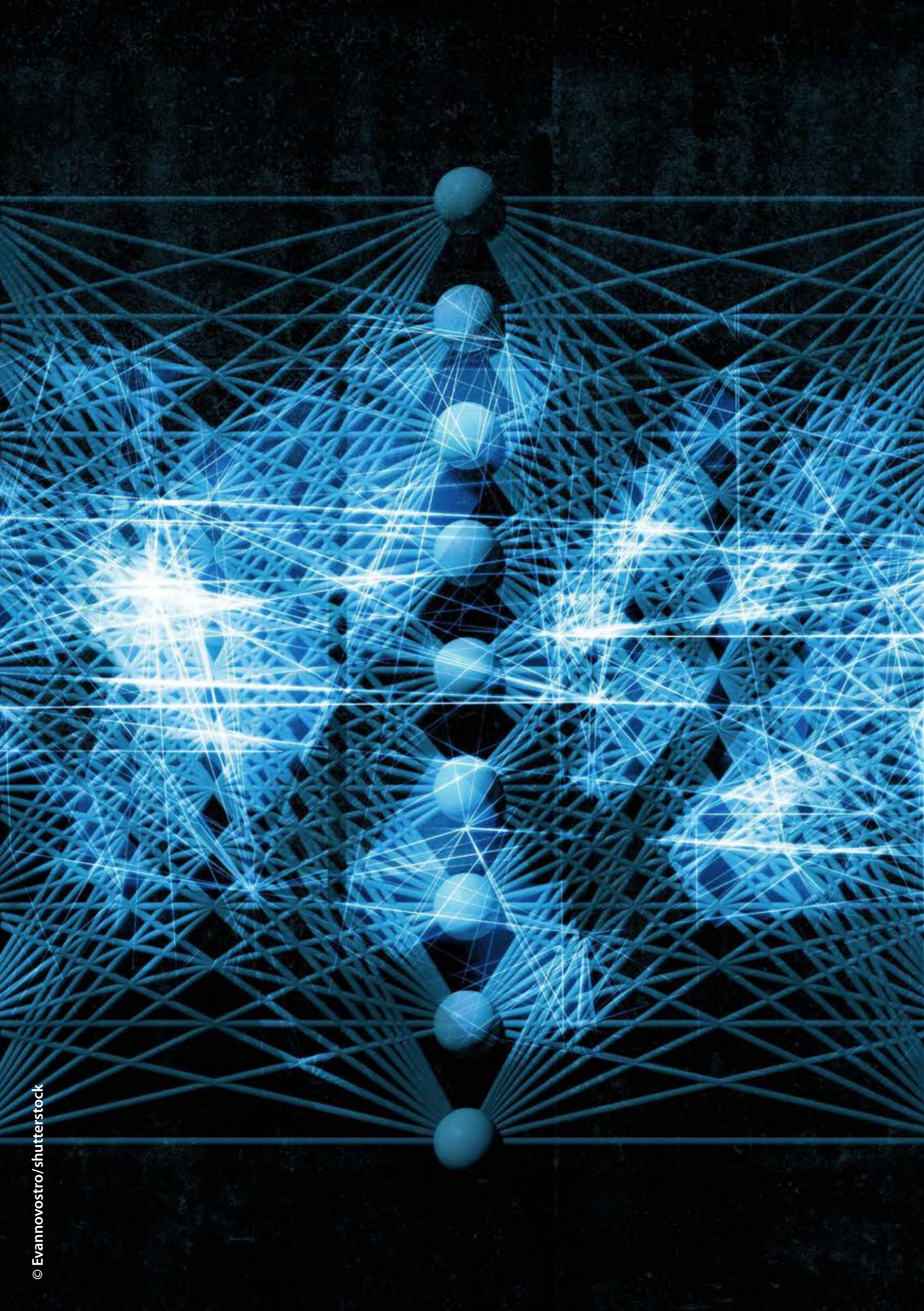
- The final article, *Building the Command and Control of the Future from the Bottom Up* by Col Paul Birch, Maj Brad DeWees, and Capt Ray Reeves (US Air Force), comes with permission from *War on the Rocks*. In this article the author presents the case for developing a vision for future decision-making with a bottom-up approach. The paper discusses specific advantages to be gained from this approach style, related to decision speed, integration, problem-solving, as well as resiliency and survivability.

Technology is very much at the forefront of BM development and the implications of emerging technology for BM vary from one functional area to another. Information Management (IM) was and still is a key enabler for SA and depends on the effective use of IT. Of course, technology can never replace the human element but it can significantly support humans and be as useful as necessary to meet future requirements. The cognitive ability to operate effectively within a rapidly changing battlespace can be developed and reinforced first through training and then with experience gathered during upcoming operations to allow NATO to face new BM challenges. That is why constant training is required for those who will play a significant role in decision-making process.

Lieutenant Colonel Zenon Kot is the Polish SNR assigned to the JAPCC working in the Plans, Concept Development & Vision division, ACE Branch. He has 28 years' experience in Air Traffic Control (National, and Command & Reporting Centre) and was a Duty Controller in the National Air Operation Centre. His last assignment was as Branch Chief Analyst, for the NATO AWACS missions.

Endnotes

1. Speech given at the National Defense University, Washingtion D.C 31 Jan. 2002,<http://defenselink.mil/speeches/2002/s20020131-secdef.html>.
2. NATO AJP-3, Allied Joint Doctrine for the conduct of operations, 2019. p. 3-5.
3. Battlespace management market overview. Defence IQ Mar. 2014.
4. Ability to exploit AI to C2 the Battlespace, Lt Col Asger Pilgaard, DNK AF, JAPCC.
5. Derived from the presentation „Potenziali impatti dell'applicazione dell'Intelligenza Artificiale nel Combat Management System' held at Tiberio workshop, organized by Italy MoD, Jun. 2019, Rome.
6. Harnessing AI and Deep Learning for Real-Time automated advanced persistent threat detection and multi-domain situation awareness. Ms Gentry Lane.
7. New MALE capabilities including AI will power NATO's cross-domain Joint ISR, Christophe Fontaine.



© Evannovostro/shutterstock

Exploiting AI in Command and Control of the Air Battlespace

XIX

By Lt Col Asger Pilgaard, DNK Air Force
Joint Air Power Competence Centre

Based on the Study, 'AI in Air Command and Control'.

Introduction

Leveraging existing and emerging technologies is one of the Allied Command Transformation challenges, along the Innovation and Technology path of Warfare Development in NATO. 'Experimentation and Demonstration' is one of the work strands that accentuates the need to invest time and resources toward the capability development process.[1]

The German Air Force took the enterprising approach of leveraging Artificial Intelligence (AI) technologies and commissioned a study undertaken by Subject Matter Experts (SMEs) from the German and French Air Forces, NATO ACT, and the JAPCC. Initiated in late 2017, the study formed with the ambition of investigating the development and use of AI in the Air Command and Control (AirC2) planning cycle in a Joint Force Air Component (JFAC).

Between the two main stakeholders, Germany and France, the combined expectation was that AI would free-up human resources during JFAC training and/or exercises, as well as create options during planning, thus speeding up the process.

The study was expanded on 1 November 2018 when a contract was awarded to CAE[2] to provide deliverables such as analysis, a demonstrator, and progress reports.

The working title of the study is 'AI in AirC2 Planning & Education, Training, Exercise and Evaluation (ETEE)'. The study explores the human-centred approach to overcome the challenges in the planning and execution phases of the JFAC planning cycle.

The Planner

The human participants in this study, planners assigned to the JFAC, needed to be observed in their working environment to understand the challenges they face, and how those challenges could be reduced to their simplest form most effectively.

The SMEs conducting the study observed and questioned the staff in the different JFAC divisions and branches during a high-intensity exercise in 2019, and collected information on the challenges of the different planners throughout the process. The information was collected using a combination of empirical data and performance-interviews conducted in all branches. Several planning branches were identified as potential candidates for further study. Some of them, such as Electronic Warfare and Defensive Fighter Operations planning, were identified to be very challenging, but the most stressful[3] workload for planners was recognised to be the offensive Composite Air Operations (COMAO) planning. The scarcity of COMAO planners, the time constraints during planning and the considerable amount of data necessary for the process, this consequently became the primary focus of the study.

Why is the COMAO planning a suitable target for study? COMAO planning normally requires a lot of different resources[4] in a short period of time, which makes it the most time- and capability-constrained activity for the JFAC, and it is as complex as it is demanding. It is challenging for the human planners, so the ambition, therefore, is to provide an AI agent. It may be described as a software that gathers information about an environment and takes action based on that information[5]. The AI agent must be taught the necessary knowledge and models to create a variety of COMAOs, thereby increasing options and improving the recommendation to the commander. The agent is defined by the type of application available and best suited for purpose, which, in this case, is Reinforced Learning.[6] The way an AI agent learns, can be supervised or unsupervised. In this case, the supervised learning will place a human in the loop. The supervised learning portion will consist of professional COMAO operators/planners regularly testing and checking the agents learning method.

Reinforced Learning, simply explained, is a method of learning that includes sensation, action and goal. The agent interacts with its environment (sensation), explores and exploits it (acts), and is rewarded for solving the given task (goal). The agent will search for the optimal outcome (many times) to get as much reward as possible. The agent in this study will be fed well defined COMAO parameters in an environment (in this case the ICC system[7]: COMMAND) which it will use to try to exploit and win the air battle over an opponent. It will execute this process recognising why it is winning while indicating the choices made for its actions.

The goal of creating the best plans begin with understanding the performance of the best planners. In that sense, the best planner is a persona[8] that performs, or behaves, in a certain way in order to further the plan. In the planning process, the persona's (the agent) task must consist of either 'Create Options', calculate 'Risk and Benefits' or build 'Situational

Awareness'. 'Create Options' is respecting the study's collective ambition and is, therefore, the selected persona.

During the study, the SMEs utilised the lens of the 'Design Thinking process[9]' to develop the persona of a 'perfect planner' (as in the best knowledgeable and experienced). This provided the framework idea of the best planning behaviour that an artificial agent would need. Behaviour, as a theme, is not (yet) easily produced in the AI world and cannot as such be demonstrated. However, this study will bridge the gap between the two planner types – the AI and the human planner.

To sum up, the focus of the study is to build a demonstrator, consisting of an agent that can create options in an Offensive COMAO scenario in order to assist planners and recommend options for the commander while showing the preferred actions/options.

When the human-centred approach is the most effective, it focuses on deep integration of humans into the data annotation process and into the real-world operation (optimizing both)[10]. The data annotation process involves the human selecting and prioritizing data from which the agent learns and optimizes the models. Before the agent is taught anything of the COMAO planning, the scope of the agent has to be defined by data (environment, program and network), policy (planes and flying/offensive parameters) and by setting the scenario – in this case a COMAO scenario.

The Commander's Decision

The best outcome of any COMAO planning includes having several options, of which a chosen few are ultimately briefed to the commander. The commander then decides on his preferred option.

By the year 2021/2022, during the exercise Kalkar Sky[11], the AI agent will have run and learned from thousands of COMAO-based scenarios in the given environment. The JFAC commander at Kalkar Sky will be presented with the agent's recommendation and reasoning of actions of the COMAO plan based on the same available data, which the human planners will have at their disposal. It will be up to the commander to choose the recommendation to follow, the AI agent's or the human planners'.

Will it be the perfect plan? Probably not. On the short term, the study will identify whether or not an agent will be able to develop a COMAO plan with the given data, meaning both the constraints and the restraints of the warring entities. What must the blue and the red forces do, and not do?

Should the German Air Force consider the agent to be of operational use, the technological future will look promising. It may expand to include another planning process (Defensive Fighter Ops or others), and when incorporating more than one component's organic assets, the joint aspect might look promising as well. It may also be possible to fine-tune the planning to include denial and diversion and not only destruction operations.

The agent will need training in all characteristics of the air domain, and will always have the oversight of a human in the loop while doing so. This check ensures adherence to the legal aspects of the operations and, equally, validates the operational efficiency of the agent.

Future Outlook

The perfect planner, the skills of the persona, the rules of the planning, and a working knowledge of what comprises a COMAO all combine to provide an expert-level planner[12]. The AI agent's strength is in adapting the skills and rules provided for a goal-oriented plan, not one that is process-oriented. In this case, you may say that the agent's recommendation is provided with certainty, since it will be based on a lot of optimal outcome-planning. Expertise in a human is the combined behaviour of the previously recognized strengths fostering of fast decisions in complex situations and environments where there is a high degree of uncertainty. The human expert uses knowledge for reasoning in situations, which do not match previous experience. The AI agent at the current technological stage is not easily adaptable to that kind of reasoning to new situations (meaning new environments and different scenarios). Therefore, the agent will require extensive human assistance during its learning process, as well as validation during the final recommendation to be in line with current Rules of Engagements and Special Instructions. The ambition of this study in leveraging the AI technology in this JFAC planning situation might free up resources, add options, and possibly bring the German and French Air Force to the forefront of AI experimentation in military affairs.

Once it gets going, AI may be like a train that does not stop, and for that reason it will need to be recognized as an area that requires a regulatory framework and some kind of Standardisation Agreement(s) in NATO. Research and development are important as the forefront of the technology but should not be leading the principles of warfare and the development of doctrines adhering to that specific technology. The implications as well as opportunities and risks associated with the near AI future in warfare require more discussion, not only at the judicial level but also the ethical level. Others, not NATO, are leading the development of Artificial Intelligence strategy, according to the NATO Secretary-General Jens Stoltenberg[13]. This difference will most likely cause a significant capability gap if not appropriately dealt with.

Lieutenant Colonel Asger Skov Pilgaard is an Air Operations Planner expert, with both GBAD and Air Defence operational experience during the last 27 years. His attention towards the connection between AI and AirC2 brings value to the JAPCC portfolio, hence NATO.

Endnotes

1. Allied Command Transformation invitation letter of 22 Mar. 2018, NATO UNCLASSIFIED. Internal ref.: 7730/TSC TPX 0220/TT 180372/Ser:NU0207.
2. CAE, previously known as Canadian Aviation Electronics, is a global company with training expertise in civil aviation, defence, security, and healthcare.
3. Stressful in the sense of being time consuming with little information available.
4. Resources meaning different categories of specialised versions of aircraft, link systems and communication systems (also known as capabilities), working in a timely and controlled, synchronized effort together with the appropriate amount of ground resources.
5. Massachusetts Institute of Technology, Education, AI, '6.825-lecture-01.', 2019.
6. Sutton, Richard S. and Andrew G. Barto, 'Reinforcement Learning: An Introduction', Cambridge, Massachusetts, 2014/15.
7. NATO Communications and Information Agency, 'The NATO-wide Integrated Command and Control Software for Air Operations (ICC) is an integrated Command, Control, Communications and Intelligence/Information (C3I2) environment that provides information management and decision support to NATO air operation activities during peacetime, exercise and war.'
8. Persona, 'the aspect of a person's character that is presented to or perceived by others.', Oxford English Dictionary.
9. Design Thinking, the creative process used by business and education in which divergent and convergent thinking, ideation and analysis may provide the persona (the perfect planner).
10. Fridman, Lex, 'Introduction to Human-Centered Artificial Intelligence', MIT 6.S093, Feb. 2019.
11. Although the script and purpose has not yet been fully approved for the next Kalkar Sky, the expected outcome will be an exercise which will demonstrate NATO's air power capability to project stability to NATO borders and beyond. Certification as a NATO Response Force (NRF) component is expected and will prove its (the German Air Ops Command) capability to exercise effective command and control over assigned forces in executing NRF missions and tasks in a high-threat environment.
12. Cummings, M. L. , 'Artificial Intelligence and the Future of Warfare', International Security Department and US and the Americas Programme, Jan. 2017.
13. NATO Secretary-General Jens Stoltenberg, Speech given at Maritime Academy, Odesa, Ukraine, Oct. 2019.

© i3d/shutterstock

Potential Impact of Artificial Intelligence to C2 Systems

XX

By Mr Daniele Frisoni
Naval And Air Defence System LoB

Note: This paper is derived from the presentation 'Potenziali impatti dell'applicazione dell'Intelligenza Artificiale nel Combat Management System' held at Tiberio workshop, organized by Italian MoD, June 2019, Rome.

Introduction

In the frame of combat systems, the Command and Control System (C2) allows the Commander and their team to manage in near real-time: (i) system electronics, (ii) sensors, (iii) electronic warfare and (iv) effectors, in order to generate Situational Awareness (SA) and ensure the tactical control of the area-of-operations.

Artificial Intelligence (AI) is not new, yet recent advances in Deep Learning have spurred great excitement in the field. The research objective is to develop novel approaches based on AI and candidate solutions which can reduce information overload, improve situational awareness and support the decision-making process. In order to achieve this, it is important to identify constraints and goals in the use of AI, identify roles and problems for which AI is better suited, define the process and develop the tools needed for experimentation, define metrics for performance evaluation, and delineate applicable verification and validation procedures.

It is therefore essential to start a process of analysis and experimentation to verify that all relevant issues from an operational, technical and industrial standpoint are properly addressed. Some of these analyses / experiments will necessarily need the support of the end user, because any solution is doomed to fail if it does not adhere to concepts and expectations of the user. Moreover these innovative approaches strongly depend on the availability of real data, which is crucial for the appropriate training of AI algorithms.

Problem Definition

There are many reasons to investigate the potential benefits of AI application to defence systems, but the most relevant is that AI promises to improve the speed and accuracy of just about everything from logistics to battlefield planning and speed in this case is not about the velocity of an airplane or a munition. Speed is about decision-making, making the right decisions first and shortening the C2 cycle[1].

Future scenarios will probably exceed current scenarios in terms of speed, number, and density of threats by including hypersonic and cruise missiles, unmanned platforms, stealthy aircrafts of the latest generation, and swarms of drones in multiple forms and sizes operating in teams. In such complex saturating scenarios, where everything from detection to coordination and synchronization is more difficult, the human cognitive capacity is overwhelmed and the human response time is not fast enough. AI, from a military perspective, can represent a significant force multiplier.

Brief Remarks on AI

AI is a broad umbrella which encompasses Machine Learning (ML) and Deep Learning (DL)[2]. Figure 1 presents a simplified view of the relation among AI, ML and DL.

ML extracts knowledge from training data and applies this knowledge on new data: ML behaviour therefore depends on the quality of the training data and on how the new data relates to the training data.

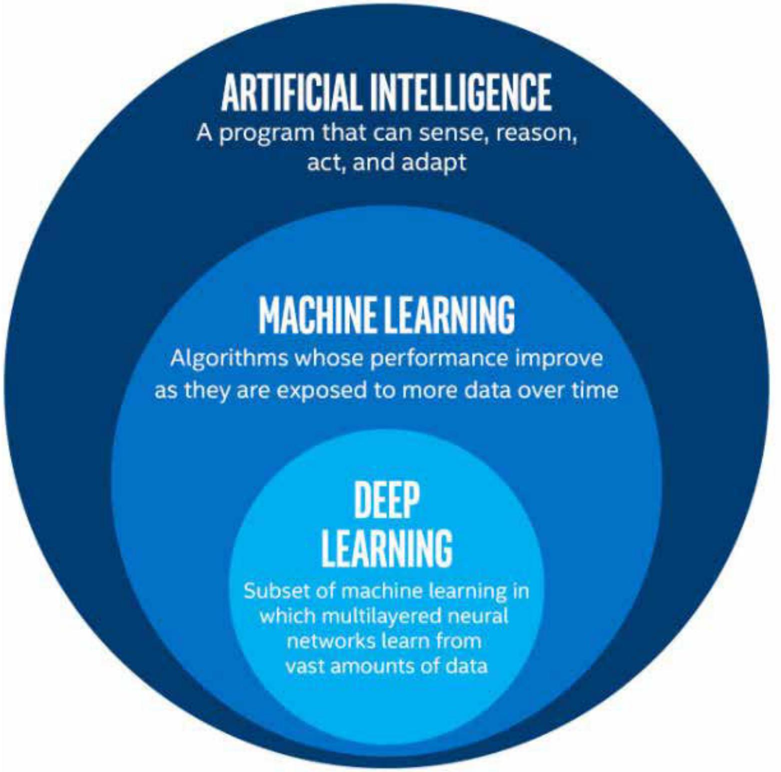

ARTIFICIAL INTELLIGENCE
A program that can sense, reason, act, and adapt
MACHINE LEARNING
Algorithms whose performance improve as they are exposed to more data over time
DEEP LEARNING
Subset of machine learning in which multilayered neural networks learn from vast amounts of data

Figure 1: *Relation among AI, ML and DL[2].*

DL is the subset of ML-based on multilayered neural networks which has triggered this latest revival in AI. DL is the best realization so far of a computational model which can address visual pattern recognition and natural language processing via hierarchical spatio-temporal machines inspired by biological models.

DL has surpassed human performance in specific tasks, yet 'Machine learning-based systems can fall not only under 'unanticipated situations' or 'when it encounters data radically different from its training set' but also under normal situations, even on data that is extremely similar to its training set'[3].

Flaws and fragility in ML algorithms keep popping out, e.g failures to classify an image when one or few pixels are modified[4], failures to detect large obstacles in autonomous driving, or vulnerability to deception[5].

ML behaviour is therefore not fully predictable and this is something which needs to be considered in military applications.

Problem Analysis

The adoption of a new technology, from an industrial point of view, is generally a burdensome activity. It is necessary to evaluate the impacts deriving from the inclusion of the new technology and carry out a cost-benefit analysis on all relevant aspects:

- Operational (e.g. change of paradigm, ease of use, training, etc.);
- Technical (e.g. complexity, performance, computational load, safety, etc.);
- Support (e.g. associated logistics, industrial maintenance, etc..).

Furthermore a new technology, for the end user, should exhibit features such as:

- Ensure better performance;
- Be predictable / understandable;
- Fail in a controllable manner.

Avoid behaviour which is unexpected / illogical / incomprehensible / irrecoverable.

Another issue to consider is that ML is only as good as the data it learns from; the data should be representative of the problem to be solved. It is expected that to make the AI algorithms work properly a large set of training data, and related correct 'responses', have to be set up and run; this is a huge activity that requires experience in conception of scenarios and the use of specialized software tools and computational machines for building and training the AI architecture.

A solution based on AI may be more or less comprehensible to the end user, e.g. if DL techniques are used the solution is a kind of Black Box and user understanding is pretty low; in fact internal processing is no longer available for inspection, analysis, modification or correction, under penalty of altering the behaviour of the algorithm and the need arises for new testing techniques (especially during formal acceptance tests).

Verification and Validation (V&V) is therefore a critical related issue for AI-based algorithms. In fact with respect to a conventional software code, the following issues must be considered for the application of V&V to an AI-based approach:

- Greater complexity;
- Lack of 'transparency';
- Totally different implementation techniques;
- Code Inspection not completely effective;
- Need for adaptive behaviour introduces additional level of complexity;

- Difficulty to rule out unwanted behaviour;
- Criticality of application of existing regulations and procedures.

To overcome the V&V issues reported above, a number of applicable strategies can be adopted such as:

- Expand testing cases and procedures;
- Adversarial Testing;
- Verification and validation of training data after the event;
- Preparation of behavioural maps;
- Improve Human Machine Interface ('explainability of AI');
- Constrained use and integration of the new technology.

In a nutshell it can be said that an AI approach has to consider the:

- Type of application and to what extent it can be entrusted to AI;
- Amount, quality and completeness of training data which is required;
- How to approach V&V;
- Level of human-machine teaming.

AI for Command and Control Systems

The study of the potential impact of AI for the C2 product has identified as one of the first steps the areas that appear suitable for AI introduction. Figure 2 presents a list of C2 functions potentially upgradable by the AI technologies with an indication of the temporal timeframe.

Tracks classification is currently one of the most promising areas of application since it shares one essential aspect of big data, i.e. there is a large number of tracks flowing in the system which must be assessed in near real-time and whose filtering is of paramount importance in order not to saturate the Operator and system resources. This topic is expanded in the next section.

Function	Description	Time-frame	Notes
Classification	Determination of the type / class of the target	Near term	Conventional solutions have shown their limits, AI based solutions may provide better performance
Threat Assessment	Determination of the threat level of a target	Near term	Need to manage different situations based on context (e.g. peacetime, crisis). Importance of real data for various situations.
Generation of 'Smart' Red Forces	Training and Wargaming	Near term	Creation of novel situations.
Analysis / understanding of the situation and determination of the action	Situational Awareness and Decision Support / Making to support the Human Operator	Medium term	Very broad class, to be implemented and verified on increasingly complex scenarios.
Management / use of resources	Support to mission planning	Medium term	Problems with many variables and constraints, generally solved with heuristic techniques.
Damage/Kill Assessment	Evaluation of damage inflicted to the enemy	Near term	Not much real data is available, more work should be dedicated towards reliable automatic solutions.

Figure 2: *Potential impacts of AI for C2.*

Another area of potential interest is the generation of smart red forces to develop penetration testing of defences. An AI-powered red force can provide advantages such as adaptive threats which can better train the skills of the trainee and uncover gaps in the defence system.

A potentially interesting application is also the Kill Assessment (KA) of a threat engaged by on board effectors. Today KA is often entrusted to the Operator and this is a time consuming process; as a consequence this either limits the possibility of re-engagement in the case of fast threats or forces to the waste of precious ammunition if the assessment is not rapid enough. Saving ammunitions using an AI process is just one of the tangible benefits in addition to increasing a high-value target's probability of survival through identification and closure of vulnerabilities.

ML for Classification

The determination of the type / class of the target is an important and critical issue in homeland and military defence since it is one of the main drivers in deciding the type of reaction. State-of-the-art fielded solutions generally encode Human Knowledge in the form of heuristics and they can be used as reference to measure the potential upgrade due to AI in terms of:

- Improvement of accuracy in response;
- Minimizing the number of false alarms;
- Minimizing response time.

Relevant factors in a classification problem are the separability of the classes and sensor limitations: three different cases may arise:

- Classes are not be separable in the observed dimensions;
- Classes are separable in principle but noise and limited resolution of the sensors may obfuscate such separation;

- Classes are separable even if noise and resolution of the sensors are taken into account.

Classification performance must of course be appreciated differently in each case.

Current results confirm that ML techniques are powerful at extracting knowledge from data and can improve the classification performance and reduce the response time with respect to conventional solutions; in fact the ML classifier provides excellent performance with very high precision and recall, yet this performance may still not be enough for stringent military requirements according to the case.

The ML classifier does not replace the legacy classifier but it operates in parallel to it. The legacy classifier enforces deterministic and probabilistic rules which codify human derived knowledge; the ML classifier brings in knowledge extracted from the training data. An intrinsic or extrinsic confidence is associated to the class determined by each classifier. The experiments on classification modules that use both hard-coded algorithms and ML methods combine the classifiers (ML, Legacy and external sources) in order to exploit the strength of each classifier and take into account the respective areas of consistent operation. Current results once again confirm that the combination of the classifiers achieves superior performance with respect to individual classifiers.

According to the classification problem at hand, the classifier may provide a fully automatic solution or provide data filtering and reduction capability which ease the Operator workload. Several parameters are available for fine-tuning the overall classifier performance.

As a final remark it is not foreseen to remove the Human Operator from the decision loop in mission-critical application.

Conclusions

AI has been around for decades and the field continues to show continuous progress even though there have been dark periods of reduced funding and skepticism. Recent advances in machine learning, notably DL, are now showing impressive results in consumer applications and have spurred a lot of enthusiasm and activity in the field. On the back of these advances the relevance of AI is being re-examined and experimented with in military C2.

The application of ML in the military is not straightforward due to the critical nature of military operations and also due to noise susceptibility and vulnerability to adversarial attacks of the technology. The ability to understand and explain the decision-making process in mission-critical applications is of paramount importance; ML solutions should be properly studied, trained, constructed, and managed so that they can earn the trust of designers and end users. The specificities of AI require that the integration of these technologies takes place only after all the necessary verifications are made and successfully passed.

DL techniques are basically still recognizing patterns in data, there is no understanding and no intelligence in a true human sense.

True AI is still ahead, yet AI is here to stay. The approach to AI and the expected impact on C2 today are mostly evolutionary. In the long run they may gradually become more and more revolutionary, and change the way things are done, information is approached, and operations are performed and also the way in which systems are designed. For these reasons it is important to continue to monitor, investigate, and experiment with advances in the field of AI and learn how to most effectively deploy AI.

Daniele Frisoni obtained his degree in Aerospace Engineering at University 'La Sapienza' di Roma, and since 2004 is employed at Leonardo as a Project Engineer for Naval and Air Defence Systems. Since 2014, he is responsible for the 'Defence Systems Analysis' Unit at the Naval and Air Defence Business Unit.

A special thanks to Mr Antonio Graziano, Mr Andrea Sacchet, Mr Luca Timmoneri, Mr Domenico Vigilante, and Mr Mario Ravanelli for their assistance and contributions to this article.

Endnotes

1. Albert, D. S., &al, 'Network Centric Warfare: developing and leveraging information superiority', 2nd edition, DOD CCRP, 2000.
2. https://towardsdatascience.com/cousins-of-artificial-intelligence-dda4edc27b55.
3. A case against mission-critical applications of machine learning', Communications of the ACM, Aug. 2019.
4. Su, J., D. Vargas, K. Sakurai, 'One Pixel Attack for Fooling Deep Neural Networks' – arXiv https://arxiv.org/pdf/1710.08864', 2017.
5. Thys, S., W. Van Ranst, T. Goedemé, 'Fooling automated surveillance cameras: adversarial patches to attack person detection', 2019.
   Mclemore, C. S., and Hans Lauzen, 'The dawn of artificial intelligence in naval warfare', https://warontherocks.com/2018/06/the-dawn-of-artificial-intelligence-in-naval-warfare/ 15 Mar. 2019.
   Horowitz, M. C., The promise and peril of military applications of artificial intelligence.

© metamorworks/shutterstock

Harnessing AI and Deep Learning

XXI

Real-Time Automated Advance Persistent Threat Detection and Multi-Domain Situational Awareness

By Ms Gentry Lane

ANOVA Intelligence

Cyberattacks (with the objective of disrupt and degrade critical communications) on military and intelligence targets are long, incremental operations that precede kinetic military strikes by months or years. Detecting and defending this 'cyber strike before the kinetic strike' at scale requires a fundamentally different approach and coordinated response. This paper proposes an asymmetric engagement strategy framework which shifts tactical advantage to the defender using the latest in Artificial Intelligence (AI) automation and Machine Learning (ML)[1] powered analysis to detect the fileless type of malware (favoured by adversary cyber-armies) over disparate networks.

No Informational Technology (IT) or Operational Technology (OT)[2] network is impervious to a focused cyberattack from one of the well-organized cyber-armies of the major threat actors, let alone all of them simultaneously. Each system presents its own threat surface, and within that system are innumerable subsets of exploitable vulnerabilities. The aggregate of IT and OT networks – which comprise nearly every aspect of modern warfare – presents an exponential increase in breach opportunities for adversarial cyber-armies possessing the resources for persistent engagement. In order to escape the defensive posture in this persistent asymmetric conflict, the vulnerability imbalance requires rectification by shifting the tactical advantage to the defender.

Achieving the defender's advantage in the cyberspace domain requires a unified attack response across all military branches, adequate and unilaterally distributed defensive resources, full and accessible situational awareness, discretion, and sustainable engagement.

Adequate defensive resources, for the purpose of this paper, means an evenly distributed Advanced Persistent Threat (APT) defence and detection capability combined with real-time raw and synthesized intelligence sharing across secure channels. All of which must respect and preserve the privacy required when sharing sensitive intelligence across branches, agencies, operations, and assets.

The Problem with Current Commercial Approaches to Advanced Persistent Threat Detection

The most obvious challenge presented by commercially available cybersecurity solutions is their accessibility. Defending critical systems with off-the-shelf solutions will assure cyberspace domain inferiority. It is not difficult for adversaries to discover some, if not all the cybersecurity solutions in play from open source announcements made when private companies win government contracts, from industry whitepapers, use cases presented at industry conferences, or direct inspection of outward-facing code. Adversarial cyber-armies design and test their payloads against commercially available solutions. This had led to the rise of and preference for sophisticated 'fileless' malware as the cyber-weapon of choice for both IT & OT networks. Fileless malware and other Low-Observable Characteristic (LOC) attacks are undetectable at the time of breach by all commercially available endpoint security solutions. The best outcome produced by a commercial Intrusion Detection System (IDS) is the ability to catch anomalous beacons, or detecting evidence of fileless malware during data transmission back to its home base. This occurs weeks or months after the initial breach and after malware has already probed and surveilled part or the entirety of an IT/OT system.

It is prudent to remember that commercial cybersecurity companies are beholden to their shareholders, and not to any national security mandate. It is not in their interest to solve for a definitive fileless malware solution when selling suites of single-problem solutions is more profitable.

Rather than developing another malware detection tool that would soon be discovered, reverse engineered, and used to design more undetectable malware, US and allied forces will be better served by democratizing two forensic processes specifically adroit at discovering fileless malware and other LOC attacks at the moment of breach.

Automated, Endpoint Memory Forensics at Scale

Endpoints (computers and servers) have different types of memory. Random Access Memory (RAM) is where files are stored. Volatile RAM (vRAM) is where data is processed. vRAM forensic analysis is the deepest memory scan available, hence the industry standard. Because vRAM forensics shows what data is being processed, where, how and when, it's a record of behaviour and interactions, thus examination will always show evidence of any malware, including fileless malware executions. At present, vRAM forensics are only executed post-breach. It is time consuming and requires experienced tier 1-level analyst expertise. It takes one expert, one day, to analyze one host, with a variable accuracy rate dependent on the analyst's expertise and familiarity with fileless malware and adversarial nation-state tactics and techniques.

But by leveraging AI to automate vRAM ingestion and analysis, and employing deep learning to classify, analyze and resolve APT behaviour, the forensic process can be run at enterprise scale and requires only one junior analyst to oversee thousands of endpoints. Computational pattern recognition is more accurate than human pattern recognition, so algorithmic systems are much more accurate at discrete anomaly detection. On binary battlefields, math is the weapon with the highest lethality.

Automating the vRAM forensic process allows users to run forensic scans proactively and discover fileless and LOC breaches in near real-time. The defender can now detect adversarial interference at breach, which affords the option of surveillance or immediate expulsion.

Computational Mechanism for Data Integrity Attacks

Most cyber-physical systems, especially OT or Industrial Control Systems (ICS), do not have volatile RAM. Sensor data processing is comparatively simple in cyber-physical systems and does not require significant processing power. ICS sensors, such as those in any land, air, sea, or space vehicle, are typically binary (yes/no, go/stop) and are all closed-loop systems. By relying on the immutable properties of physics in a closed-loop system (demonstrated in Kirchhoff's Voltage Law which states that voltage in must equal voltage out), and by leveraging AI to automate voltage monitoring and machine learning to classify and analyze these voltage readings, anomalies caused by data reply attacks[3], sensor corruption or other data integrity attacks can be discovered in real-time. The algorithmic system that powers this OT solution calculates all the possible corroborations between sensors. Depending on the size of the cyber-physical system there are typically hundreds of thousands, and often hundreds of millions, of different corroborations that would indicate no sensor compromise. Because the algorithmic system is doing the heavy lifting, periodic, persistent readings and differential data comparisons require very little computing resources and can be easily integrated into any closed-loop system from manned and unmanned aerial vehicles, to satellite communication systems to base electric grids.

Quantified Situational Awareness and the Need for Discretion

The APT breach data gleaned from IT networks can be combined with that generated by OT networks for full server to host to sensor situational awareness over disparate, distributed IT and OT systems[4]. But the situational awareness is useless without context. While it is useful for system administrators and intelligence officers to detect APT breaches in near real-time in the systems under their charge, the aggregate and analysis of all IT and OT systems across all branches produces the most useful insights. Big-picture analysis affords unprecedented views into adversarial cyber operation behaviour patterns. Analysis of breach behaviour over time will yield accurate predictions[5]. Therefore, in order to understand APT breach behaviour patterns in their full context, it is essential to garner the participation of as many fielded forces, military installations, and defence agencies as possible and to share both real-time and predictive data freely over secure channels.

The advantages to these computational approaches to anomaly detection are numerous (resource-efficient, highly accurate, low size, weight, processing power, no required hardware testing, architecture and OS independent), but most crucial to sensitive military operations is the privacy afforded by vRAM forensics and sensor corroboration anomaly detection. In both cases, analysis is performed on binary code and does not require access to data or storage files that may contain sensitive documents or passwords. Therefore, this computational analysis approach is an ideal solution not only for US military branches, defence and intelligence agencies, but also a viable solution among allied forces.

Conclusion

History proves that the ideal solution is not always the one adopted. Commercial and bespoke cybersecurity solutions at play in critical military IT and OT networks are inward-facing and disparate. They take a whack-a-mole approach to catching and extinguishing adversarial breaches. While Security Event and Information Management systems (SEIMs) provide an aggregated view of breach activity behind the firewall, this view offers limited insight into adversarial cyberspace campaign behaviour patterns. Without big-picture situational awareness and without the ability to predict adversarial cyber-strikes, we are fighting blind and forced into a persistent defensive posture.

Access to behaviour-based cyber-conflict prediction has been an adequate incentive for mass adoption within the American private sector. Combined with the privacy afforded by this method of analysis and anonymized data shared over secured channels, context provided by big-picture situational awareness has proved crucial to readiness and the definition of relevant readiness metrics. The projected outcome of mass adoption of these capabilities and framework is deterrence by denial: Rendering nation-state fileless malware ineffective and eventually obsolete.

However, there is risk of an undesirable secondary effect of this strategy. Adversaries are likely to respond by turning their forces to other vulnerable targets, and perhaps disproportionately subjecting NATO allies to increased focused aggression. It would be most advantageous for all NATO members to adopt the same tools and strategy.

Independently, proactive memory forensics are certainly useful and work in a part of the security stack not addressed by other commercially available solutions. However, the insights gleaned from daily behaviour-based, persistent analysis affords unparalleled insight into adversarial cyberspace campaigns. These powerful defensive tools which allow for real-time incident response, the timely sharing of relevant intelligence both laterally and vertically, and access to cyber-conflict trends and predictions form the base of a unified attack response across multi-domain operations. The likely outcome from mass adoption of these tools and this framework is a shift in tactical advantage in favour of the defender.

Gentry Lane is a visiting fellow at the National Security Institute at George Mason University's Antonin Scalia Law School, and the CEO and founder of ANOVA Intelligence, an American cyber defence and threat intelligence software company. ANOVA's groundbreaking computational approach to anomaly detection is revolutionizing cyberwarfare engagement for US companies and allies globally.

Endnotes

1. AI & ML are often used interchangeably, but they are separate processes with separate aims. In this paper, AI serves to automate a complicated process with little-to-no human supervision. ML is the process of updating and adjusting analysis parameters without human intervention.
2. OT networks are cyber networks that have physical component. Example: Industrial control systems (like an energy grid or HVAC system), drone command systems, SATCOM systems.
3. Data integrity attacks trick a sensor into constantly reporting that everything is fine. Stuxnet is malware that compromised data integrity and caused sensors to report no problems when centrifuges were indeed spinning out of control.
4. Commercial software solutions and disparate operating systems do not play well together.
5. Weather prediction is another example of complex behaviour-based analysis over time.

© General Atomics

New MALE Drone Capabilities with AI

XXII

The Power Behind NATO's Cross-Domain Joint Intelligence, Surveillance, and Reconnaissance?

By Col (ret.) Christophe Fontaine
General Atomics Aeronautical Systems Incorporated

With the current security challenges that Europe and NATO are facing, Intelligence, Surveillance, and Reconnaissance (ISR) requirements have now grown well beyond traditional military needs. The resurgence of the Russian threat at NATO borders and the maritime domain demand the reestablishment of a persistent Joint ISR capability to give NATO the ability to collect strategic and operational multi-intelligence (Imagery, Radar, Accoustic, Signals) to complement that produced by US European Command and members nations. In a period where NATO nations have dramatically reduced their Maritime Patrol Aircraft (MPA) capabilities, Medium-Altitude, Long-Endurance Remotely Piloted Aircraft (MALE RPA) are the perfect cost-effective supplement to the remaining manned ISR aircraft. However in the future, these platforms developed for armed ISR loitering in permissive airspace will probably no longer be capable of operating in more and more contested airspaces. This warrants a new family of RPA with a certain level of automation and Artificial Intelligence (AI). In fact, as 'there is nothing more manned than an unmanned system' automation and AI will have to be introduced to sort the collected data, enable continued flight in electromagnetic spectrum jammed conditions, and fuse collected data with other intelligence collectors to present the most comprehensive common relevant operational picture (CROP) for the decision-makers.

New Context

NATO is at a crossroads in its history. After a period of peace dividend that included a drastic reduction of Command and Control (C2) structure and defence spending by most member nations, the security situation has fundamentally degraded on almost all borders of the alliance. Threats have not only multiplied, but have regained a peer to peer nature. With the investment in the Allied Ground Surveillance (AGS) program, for the first time NATO possesses an organic capability to establish its own Situational Awareness (SA) on the ground in addition to its legacy air recognized picture, thanks to its AWACS fleet. But these capabilities are limited in number, lack multi-intelligence sensors and, most importantly for AGS, lack Positive Identification (PID) capabilities. Other challenges include the Process Exploitation and Dissemination (PED) of cross domain Joint ISR data in a multinational environment for collective defence, reassurance measures, coalition-based missions (Unified Protector for example) or alert forces (i.e. NATO Response Force (NRF)). But today, and even more so tomorrow, the challenge is to fuse the collected data available in cyberspace (open sources and social medias). This challenge of big data and multi-intelligence collection will only be mastered with automation and AI aided PED. Without this revolution in the analysis part of the Joint ISR process, the continuous collection by platforms equipped with near or real-time sensors will not produce intelligence to match the expectations of decision-makers and the requirements of the fielded forces. Next-generation assets and sensors require next-generation C2, called Joint All Domain C2 (JADC2) and a next generation PED process is necessary to establish the CROP and speed up the Observe, Orient, Decide, Act (OODA) loops at all levels.

Next-generation Surveillance MALE

The 'Dronic Revolution' is in fact inexorably underway. The first generation MQ-9A Reaper has an endurance of 24 hours while the new MQ-9B Sky Guardian to be delivered to the UK and Belgium has more than 40 hours. It foreshadows ongoing and future RPA concepts of operation will evolve thanks to technologies and how they will affect the OODA loop as well as NATO's Joint ISR enterprise. Technology continues to eliminate most current operational constraints by helping collection of data and intelligence to satisfy the requirements of persistence, precision and time contraction across the full spectrum of NATO Multi-domain operations. The significant increase in endurance will offer 'occupation of the airspace' over a target and its environment, as time on station would then be counted in days. For that to become routine, the next few years will see the advent of RPAs built to civilian aircraft standards. In fact, these RPAs systems will be certifiable according to the standards established by civil aviation and NATO standards (STANAG 4671 Unmanned Aircraft System Airworthness Requirements – USAR). Initially conceived to fill surveillance and combat roles, the use of large RPAs remained limited to the Dirty, Dull and Dangerous missions. Their production logic followed performance and low-cost objectives, because of their supposed 'expendable' character, more than the respect of airworthiness standards. The demands of European customers in particular have forced Israeli and US RPA manufacturers to take this mandatory requirement into account. In order to perform these deployments all over NATO members' airspace and areas of responsibility, modern RPA will also be equipped with a full 'Sense and Avoid' suite. It comprises an air to air radar coupled with Traffic Collision Avoidance System (TCAS) offering a credible alternative to the see and avoid rule. The RPAs will therefore be able to perform, like any modern aircraft, automatic trajectory avoidance with other aircraft whether they are cooperative, (i.e. equipped with similar devices), or not. Coupled with protections against icing and lightning, the flights of these large RPAs will be conducted without having to physically separate the manned aircraft with those flown remotely.

SATCOM Autoland & Redundancy of the Main Satellite Link

The MQ-9B demonstrates that it is now possible to deploy a multi-sensor ISR capability thousands of kilometres from its home base. Based on a three GPS point-based automated SATCOM landing technology, the aircraft can now deploy to any airfield. The only requirement is a small team of technicians at the deployment site to perform pre- and post-flight checks and refuelling. It is no longer necessary to dismantle the aircraft and deploy the entire system (to include the launch and recovery element). This facilitates the availability of an initial ISR capability in emergency missions outside country or for homeland operations. With this capability, every existing airfield in the area of operations becomes a potential diversion site in case of weather or technical problems. In addition, the redundancy of the main Beyond Line-of-Sight (BLOS) link with a secondary satellite link operating on another frequency band ensures the continuation of the mission, thus enables maintaining permanently piloting capabilities even in the event of communication interference, jamming or technical problems. Satellite data links are used to fly, operate sensors, and disseminate the ISR data collected from the aircraft to the cockpit and the C2 system. Beyond the impact on the ISR mission itself, these link losses, though fortunately rare, reveal a true weakness, especially when RPAs operate in an unsegregated environment or in bad weather. Equipped with a second satellite link, the aircraft remains pilotable and continue its mission safely. In addition to the Sense and Avoid Equipment mentioned above, this double security undeniably make aircraft more resistant to jamming operations and makes them perfectly suitable for flights in civilian airspace. The continuous adaptation of their sensors to address military as well as domestic mission imply a certain level of plug-and-play capabilities.

National Platforms that Could Operate NATO-Owned Plug-and-play Sensors

Modern RPAs will allow more sensors to be integrated according to customers needs. The ISR omni-role platform will be plug-and-play and 'sensors agnostic'. As RPAs will allow constant monitoring of a target and its environment, it is necessary to capitalize on that through a modularity of sensors ideally without hampering endurance. Sensor variety ranges from traditional real-time Full Motion Video (FMV) high-definition cameras to multi-mode radars and a wide range of guided weapons and multi-intelligence sensors (communication intelligence, electronic intelligence, wide-area motion imagery (WAMI), hyperspectral, LIDAR, Electronic Warfare for offensive and defensive self-protection, anti-submarine warfare, etc.). For obvious reasons of sovereignty, the idea is to offer the possibility, or coalition data sharing requirements, to quickly perform integration of specific weapons and sets of sensors without losing the airworthiness certificate of the flight system. This flexible plug-and-play capacity for sovereign and/or coalition missions will be a considerable step forward, especially if completed with multi-mission command computer at CAOC or on board of ship in order to take control of the sensors, if not the aircraft for a specific part of the mission. Additionally it may be a solution to solve the data-sharing issue within NATO. Nationally owned platforms could operate NATO owned plug-and-play sensor suites on a routine basis, for NRF missions or specific operations. In addition, integrating a self-protection suite on traditional MALE aircraft is becoming more and more necessary in the light of recent events in Libya and Yemen where MALE aircraft were shot down. It would also be a first step and low-cost option allowing operations in more contested airspace and continued operations of armed ISR missions outside traditional counterinsurgency (COIN) operations. The limitations of these systems will require augmenting their level of automation with AI aided pilot and navigation systems as well as the development of newer, more combat capable platforms.

AI Aided for PED and New Gen RPAs

Timely acquisition of quality data and preserving the integrity of such data for targeting cycles are paramount in the digitalised world. Even more, in a contested environment, the OODA loop will have to be fed continuously with real-time data. Therefore, more automation and a certain level of on-board AI will be necessary. It will apply not only to control certain parts of the flight system when the BLOS link is either disrupted and/or jammed, but also to on-board data processing sending only the relevant information to the cockpit and the C2 system. These evolutions are likely to be the next step in RPA development along with more agile and stealthy RPA platforms. In order to strengthen transmission capabilities of these new platforms, laser transmission is probably a next step forward as a back-up if not the main tool to preserve real-time flow of information. In fact, it is probably the only way to increase necessary fusion capabilities of cross-domain operations for these platforms to not only collect, but also to process their own data on board and fuse them with other collected data. The first step of AI employment will likely be the PED on the ground. Autonomous or AI-aided combat RPAs are still posing a certain number of ethical and legal questions. The ideal situation should not only feed Collection Shares Databases (CSD) with raw data available to multiple customers, but also perform automated cross cueing of sources to augment the CROP. For example, AGS ground moving target indicator data should be processed automatically into a geospatial intelligence product consisting of fused multi-layers and multi-sensors (open-source intelligence, FMV, image intelligence and signals intelligence) for Joint ISR and targeting purposes.

Conclusion

Technology will no doubt continue to facilitate the use of MALE RPAs in the same manner as manned aircraft as automation and AI facilitate processing and fusing of multi-intelligence including open sources. The emergence of more capable RPAs will be in line with new-generation aircraft to satisfy the requirements of persistence, precision and time contraction across the full spectrum of defence and homeland missions including operations in more and more contested airspaces. These new-generation RPAs will have to be able to continue to occupy the airspace in order to perform continued ISR collection while performing other ones like early warning, air-to-air refuelling, ballistic missile defence and SIGINT. They will have to address new missions like Suppression/destruction of Enemy Defence and electronic warfare, as well as air to air missions autonomously and/or in conjunction with an AWACS or traditional fighter aircraft as loyal or slave wingman. The open software architecture offered by the MQ-9B family of aircraft could enable NATO nation owned platforms to operate NATO owned plug-and-play sensor suites on a routine basis, for NRF missions or specific operations and, therefore, solve the challenge of exchanging intelligence. Only automation and AI are likely to provide future Joint All Domain C2 the necessary level of information and intelligence requested to perform cross-domain operations. The introduction of AI-based automation will first affect data analysis, then assist in flying multiple aircraftw, and undoubtedly in executing more kinetic operations. It's the next iteration of the on-going revolution. Paradoxically, it may be remotely AI-augmented piloted aircraft that lend strength to the prophetic quotation of Clement Ader, 'He who will master the air will master the world'.

Colonel (ret.) Christophe 'Taraz' Fontaine is the director of strategic development for Europe at General Atomics Aeronautical Systems, Inc. Former colonel, he served 30 years in the French Air Force and deployed 28 times worldwide as an ISR, CSAR, EW, SOF, targeting, RPA and Air C2 expert; was NATO doctrine JISR document custodian, French air staff ISR division chief and the first French MQ-9 Reaper squadron commander.

© US Air Force / R. Nial Bradshaw

Building the Command and Control of the Future from the Bottom Up

XXIII

By Col Paul Birch, Capt Ray Reeves and Maj Brad DeWees

Courtesy of War on the Rocks, Web Edition, 16 January 2020

Note: This article was published in War on the Rocks. https://warontherocks.com/2020/01/building-the-command-and-control-of-the-future-from-the-bottom-up/.

We have seen the future of effective military command and control and it is only made possible by speed. In the future, adversaries will increasingly rely on machines rather than people for basic functions like surveying the battlespace, distinguishing friend from foe, and formulating options for strikes. To keep pace, the US military is developing a new mechanism for command and control, *calling it* the 'Joint All-Domain Command and Control system.' This new system will have two organizing principles aimed specifically at increasing decision speed: pre-decisional functions (i.e., surveying, identifying, and formulating) will be automated through AI-enabled technology, and decision-making itself will occur at the lowest level possible (because of ethical and pragmatic limitations, today's *AI is nowhere near the point of being able to make decisions*). Since people – not machines – will remain responsible for real-time choices about the use of force, the only way for a military to decide quickly in a complex battlespace is to diffuse decision authority throughout the organization, rather than concentrate it in the hands of a few.

Despite this vision of future decision-making occurring at low levels, *preparation* for the command and control of the future has *concentrated* on the *operational* or *higher* levels of warfare. The Air Force, for example, has created a new career field devoted specifically to the operational level – the '*13 Oscar*' multidomain command-and-control officer. Separately, after unveiling its multidomain operations concept, the Army *began exploring* the formation of two new 'field army' headquarters occupying an echelon above Army divisions and corps. These efforts indicate that, in building the command and control of the future, the military is working from the top down, prioritizing the operational and strategic levels above the tactical level.

But this isn't the only way. Senior leaders would be wise to consider a bottom-up approach, which would offer four distinct advantages: improved decision speed, superior inter-service integration, a greater likelihood of solving the most difficult command-and-control problems, and the best chances for the survivability and resiliency of the holistic command-and-control system.

Four Reasons to Build Bottom-Up

Let's start with decision speed. A core principle of military theory holds that more rapid decisions – provided they are not so hasty as to be rash – have inherently more value than slower decisions. Deciding faster puts the adversary in a reactive position. With people responsible for choices about the use of force, decision speed requires diffused decision authority. The trouble with working top-down is that it risks transferring the more cumbersome decision-making practices of traditional command

and control – higher levels hold decision authority while tactical levels act – onto the command and control of the future. Of course, some traditional command and control already embraces the idea of tactical level decision-making, called 'mission command' in the Army or 'centralized control, decentralized execution' in the Air Force. Despite the intentions of such directives, however, *reality is often different*, especially at the intersection of domains. Today, for example, what sounds like a simple matter of deciding what air assets will support which ground-combat unit is the result of a tedious back-and-forth between the overall commander of a given region and the commander of the air units in that region. In the future, the military would do well to have this apportionment decision an outcome of many decisions at the lowest level possible, made fast and frequently over the course of a conflict, rather than the result of one decision at the flag-officer level. The same will be true for decisions at the intersections of other domains, many of which the military is only beginning to imagine, and for which it has neither defined mechanisms nor practiced in exercises.

Second, the bottom-up approach increases the likelihood that the resulting command-and-control structure will be joint in practice and not just in name. Our previous *research* demonstrates that the further one gets from the battlefield, the less likely it is that genuine inter-service cooperation will occur. It is a simple matter of the structural impediments to joint acquisition that have accumulated under the Department of Defense's zero-sum budget game and Washington politics. At the tactical level – with its imperatives of surviving and defeating the enemy overshadowing bureaucratic politics – cooperation happens quickly and fluidly. But because they originate under the control of D.C. politics, systems designed for use at the operational level or higher are more likely to be 'service-parochial' and incompatible with other services' systems than those designed for tactical use, or cobbled together in the heat of battle. The implications for investing in command-and-control systems are clear: Jointness requires bottom-up experimentation and development.

Third, the technological problem of conducting all-domain control is most troublesome at the tactical level. The future environment will be *one in which* every sensor is connected to every shooter in every domain. In this environment all echelons of war will go from being *complicated* arenas to truly *complex* by a rigorous complexity-theory definition of the latter term. Navigating this complexity will be a big challenge regardless of the level of war, but will grow especially daunting in a tactical setting where any all-domain control system would have to be mobile at the level of small teams and would have to function in close proximity to adversaries. Moreover, the tactical level may be best suited for solving this problem: tactical-echelon units get the most practice in combat-realistic simulations of what the new style of warfare will look like, and are therefore much more likely to rapidly innovate systems that are interoperable and practical, provided the services allow this innovation to take place. Candidly, as members of an Air Force warfighting specialty best suited to serve in this capacity, we admit some cultural preparation will be required. Eagerness to prioritize the command-and-control portion of the tactical air-control party mission on equal footing with the maneuver-centric portion of the mission has not been a popular endeavor. But here again tactical development is a boon, because it could serve to overcome this institutional inertia.

Last, emphasizing the tactical level now is the best way to maximize the survivability of systems. While centralized control has proven effective in the past, in a major conflict with a peer adversary, centralized nodes will be vulnerable. Building architecture dispersed among tactical nodes is one means of buying insurance at the operational and strategic levels. Current thought is already pointing in this direction – the Air Force's great-power conflict concept, for example, envisions tactical nodes as a means of making an entire network survivable against a peer adversary.

The (Tactical) Way Forward

Moving forward, the military – led by what the military calls in typical unwieldy jargon the 'Joint Cross-Functional Team for Joint All-Domain Command and Control' – can better prepare for the future with initiatives emphasizing tactical development. It should start by educating and equipping tactical elements across the joint force for all-domain control. Operators should receive familiarization training in domains with which they do not currently interact, and subject-matter experts from each domain should be assigned to tactical command-and-control units. The military should also create direct links between tactical operators and the industry partners who will develop the AI-enabled technology of the future. When it sanctions experiments with future systems, the military should require involvement and feedback from tactical elements. This type of bottom-up development is anathema to the structural and political limitations that shape most military acquisition, and will require committed senior leaders from at least two separate services who are willing to make concessions. This approach, however, is feasible – in the 93rd Air Ground Operations Wing, our current unit and the one responsible for the preponderance of conventional tactical air-control party airmen, we have participated in joint experiments with the express intent of gathering feedback from tactical operators. We have found that industry partners are eager for this kind of feedback, that tactical operators are happy to give it, and that the confluence promises to build more pragmatic and survivable networks in the end.

Overall, the arguments here speak to a more general debate ongoing within the military: As it reforms itself, whether in command-and-control structure or something else, is it better to drive change from *the bottom up* or *the top down*? Of course, all levels of war are important and proficiency at each level can determine effectiveness in the others. Tactics can drive strategy and, at the same time, no level of tactical proficiency can make up for poor strategic decision-making. Tactical innovation ought to link with operational aims, top-echelon commanders' priorities, and knowledge of how the higher echelon needs to receive and process data. Otherwise, tactical innovation becomes a trivial novelty with no meaningful warfighting application.

Our argument evokes the building of the transcontinental railroad. The railroad could have been built from the East, where capital and labor were concentrated at the time, or from both the East and the West. Building from both sides required adjustment to meet in the middle, but that approach forced the builders to deal with Western-specific problems like mountain passes sooner, and ultimately resulted in a faster timeline. Likewise, our argument is not that the tactical level is more important than the operational and strategic levels, simply that the tactical level offers some of the best ways to solve the litany of problems facing the military as it transitions to the command and control of the future. At this stage of development, we believe that emphasizing the tactical level will build more 'railroad' faster. Working bottom-up is the best way to increase decision speed, maximize joint cooperation, develop all-domain command and control, and increase the survivability of future command and control, all of which are critical requirements for higher echelons.

With such a big set of problems ahead, it is reasonable for the military to start with what it knows. In a world of scarce resources, however, each sensible step the military takes is also a step it doesn't take. Ingrained habit and organizational power suggest the first step will be from the top. Prudence suggests the weight of effort should be on the bottom.

Paul Birch is a colonel in the US Air Force. He is the commander of the 93rd Air Ground Operations Wing, which contains the preponderance of forces responsible for providing the Army and Air Force with tactical-level command and control. He holds a PhD in Military Strategy from Air University.

Ray Reeves is a captain in the US Air Force. He is a tactical air control party officer and joint terminal attack controller at the 13th Air Support Operations Squadron on Fort Carson, Colorado. He is a doctoral student in organizational leadership at Indiana Wesleyan University.

Brad DeWees is a major in the US Air Force. He is a tactical air control party officer and joint terminal attack controller at the 13th Air Support Operations Squadron at Fort Carson, Colorado. He holds a PhD in decision science from Harvard University.

Future Developments

Future Developments Panel Introduction

XXIV

With an Eye Towards the Horizon

By Lt Col Henry Heren, USA Air Force
Joint Air Power Competence Centre

Introduction

Many of today's military conflicts are still largely contested with predominately Industrial Age forces and mind-set … both of which are increasingly changing. The exponential growth in technology, coupled with increasing applications, and understanding, of those technologies is rapidly changing the tools we use in our daily lives and in the conduct of military operations. As NATO transitions more firmly into the Information Age, the tools it utilizes to address security issues and ensure the safety of the Alliance have the potential to increasingly alter the way in which NATO goes about its business. Artificial Intelligence (AI), of the Narrow variety, has for years provided protection for NATO aircraft and tanks in the form of radar warning receivers and reactive armour. While the applications of Narrow AI will continue to grow, the possibility of General AI (AI that can perform a wide variety of functions) will present new opportunities as well as new challenges. NATO has already begun to ponder how it will both utilize and react to weapons systems exploiting hypersonic technologies, and those concerns are certain to increase with time. As capabilities continue to provide increased speed and reach, the ability to test and train with those capabilities will force the need to develop synergies between live, virtual, and constructive ranges which allow for simulations to provide realistic scenarios involving the full spectrum of capabilities … as they emerge. With continued advancement of technologies and capabilities, the need to establish an appropriate balance of human control over AI will drive the Observe, Orient, Decide, Act (OODA) loops to meet requirements, maintain a competitive advantage, and ensure human responsibility and safety.

Artificial Intelligence

The term AI is commonplace today, so common that many are not aware of the different types of AI or even that there are different types of AI. The type of AI most of us interact with daily is referred to a Narrow, or Weak, AI. This type of AI is focused on specific, or narrow, tasks and is exclusively good at them. For example, in December 2017, computer programmers working for Google, on a program titled AlphaZero, reached a programming milestone. 'Starting from random play, and given no domain knowledge except the rules, AlphaZero achieved within 24 hours a superhuman level of play in the games of chess and shogi (Japanese chess) as well as Go, and convincingly defeated a world-champion program in each case'[1]. Still, AlphaZero, world-champion of chess, shogi and Go, is incapable of vacuuming your living room as it is simply not programmed to deal with that task. Conversely, General, or Strong, AI is programmed to accomplish a wide variety of tasks. This type of AI is the type portrayed in science fiction movies with anthropomorphic androids (robots) threatening human existence; or at least that of the protagonist. More importantly, this type of AI does not yet exist in any meaningful way outside of a laboratory. Even self-driving cars being tested on roads around the world are incapable of making toast and are therefore categorized as Narrow AI.

Militarily speaking, it is important to note these differences. Often when AI is being discussed in military conversations focused on new and emerging technologies, any concerns expressed are usually in relation to General (Strong) AI. The concerns surrounding the development of General AI have been sounded for decades by the likes of Ray Kurzweil, such as in his 2006 The Singularity is Near: When Humans Transcend Biology, Nick Bostrom's 2014 Superintelligence: Paths, Dangers, Strategies, and most recently P.W. Singer and August Cole's 2020 book Burn-In: A Novel of the Real Robotic Revolution. As AI continues to develop and evolve, military leaders and planners will need to remain cognizant of, and able to articulate, the differences between the capabilities currently available and those still on the proverbial drawing board.

Hypersonic Capabilities

Hypersonic research programs have existed in the US and Russia (Soviet Union) going back as far as at least the 1980s but have recently seen renewed interest and public speculation. At present there are two types of hypersonic weapons: hypersonic cruise missiles and hypersonic glide vehicles. With hypersonic cruise missiles the missile is self-propelled at extremely high speeds (five times the speed of sound or more), while hypersonic glide vehicles are launched from a rocket, then detach at altitude and glide to their intended target.

Whereas hypersonic technology was sought after by relatively few during the Cold War, today many countries are pursuing the technology for both offensive and defensive means, including the US, Russia, China, France, Germany, Australia, and India. It is also important to note that speed is not the only reason this technology is being pursued. Hypersonic weapons are also distinctly manoeuvrable, with the ability to 'use aerodynamic forces to manoeuvre laterally to targets hundreds of kilometres away from the location indicated by the bearing of their initial launch.'[2]

Live, Virtual, & Constructive Training Ranges

As new military technologies emerge, many with the operational reach measured in hundreds if not thousands of miles, they have to be tested and trained with on ranges capable of accommodating their operational capabilities. Coupled with the need for operational and technical security, it is neither feasible nor practicable to test and train these emerging systems on legacy ranges. Hence the integration of Live, Virtual and Constructive (LVC) test and training opportunities. The live element is the traditional open-air ranges where systems have the freedom to manoeuvre and operate in simulated scenarios, i.e., two fighter aircraft engaging in an in-flight simulated air-to-air combat. The virtual element involves systems which simulate not just scenario, but also the capabilities being tested or trained, i.e., two pilots utilizing flight simulators to engage one another in simulated air-to-air combat. The third element of LVC, constructive, involves computer-generated entities to represent various systems or platforms, i.e., one pilot utilizing a flight simulator to engage a computer-generated pilot in simulated air-to-air combat.

In the future, AI will be used to assist with battlespace management across multiple operational domains. These operations will witness hypersonic weapons engaging targets from thousands of miles supported, or supporting, attacks by a host of different AI's through cyberspace. Sensors in orbit will communicate directly with operators on the ground and sea, as well as unmanned systems operating in the air and under the water. And all of this will require coordination and synchronization that can only be produced through testing and exercises … which will require ranges capable of supporting any and all compositions of existing and emerging technologies.

Additional Articles

This section presents four related articles which will introduce various ideas and issues related to future technological developments, and the various issues NATO may face while incorporating or facing these capabilities. The ideas expressed in these articles are meant to prepare those attending the 2020 Joint Air & Space Power Conference for the panel discussion on Future Developments:

Kill the Enemy and Don't Forget to Buy Milk on the Way Home is written by Group Captain Jo Brick (AUS Air Force). This paper focuses on technologies which enable military operators to execute their missions from the homefront, thus blurring the lines between war and peace.

Dr. Cathy Moloney's Hypersonics: Changing the NATO Deterrence Game appears next in the booklet. The paper examines NATO's approach to deterrence with respects to potential adversaries, and the Alliance's approach might shift with the fielding of hypersonic capabilities.

Implications of 5G to Air Power: A Cybersecurity Perspective is a work by Major Fotios Kanellos (GRC Air Force). This paper discusses the potential impacts to air power in the age of 5G networks, particularly as this new technology pertains to cybersecurity of air forces.

The final Future Developments Panel paper is, Forecasting Change in Military Technology, 2020–2040. This is an abridged executive summary of Michael E. O'Hanlon's comprehensive study looking at changes in military technology during the next two decades. The excerpt touches the highlights of a well-research study intended to inform military planners and operators preparing for future conflicts.

Lieutenant Colonel Henry Heren is a NATO Space & Cyberspace Strategist assigned to the JAPCC. He is a Master Space Operator with more than 27 years' active duty experience in the US Air Force. He is a Graduate of the US Air Force Weapons School.

Endnotes

1. Silver, D., Hubert, T., Schrittwieser, J., Antonoglou, I., Lai, M., Guez, A., Lanctot, M., Sifre, L., Kumaran, D., Graepel, T., Lillicrap, T., Simonyan, K. and Hassabis, D. (2017) Mastering Chess and Shogi by Self-Play with a General Reinforcement Learning Algorithm. London. Available from https://arxiv.org/pdf/1712.01815.pdf [accessed 6 November 2018], p. 1.
2. Hypersonic Weapons and Strategic Stability, IISS, Mar. 2020, https://www.iiss.org/publications/strategic-comments/2020/hypersonic-weapons-and-strategic-stability, accessed on 29 Apr. 2020.

© Iaremenko Sergii/shutterstock

Implications of 5G to Air Power – A Cyber-security Perspective

XXV

By Maj Fotios Kanellos, GRC Air Force
Joint Air Power Competence Centre

Introduction

The next generation of wireless and mobile network, called 5G[1], is expected to become the most important network of the 21st century and is predicted to have a decade-long impact. 5G's deployment started in 2019, and since then a 'race' has been ongoing between governments, industries, and investors to be the first to build a functional network. 2020 is expected to be the year that 5G will be globally launched and by 2025, 15% of global mobile connections will be based on it[2]. The worldwide 5G revenues in 2025 are anticipated to reach € 225 billion[3].

5G is gradually replacing the 4G/LTE[4] network which was released in March 2009[5] and introduced ground-breaking, for that period, fast connection speeds and mobile hotspots. 5G technology, based on the 802.11ac IEEE wireless standard[6], is expected to boost data transmission and communication by over three times while simultaneously guaranteeing ultra-high reliable and resilient connections. In the 3G and 4G world, speed and throughput were the most important characteristics to differentiate a network. The amount of data that a network could relay and the upload and download speed were the main features for users or services. But in a future 5G world this is not enough; 5G technology is not simply a faster version of 4G, but rather, an entirely new network architecture[7].

Technical Characteristics

The three main technical characteristics of 5G networks are:

- Data rates of between 1 – 20 Gbit/s per mobile base station, at least 10 times faster than before, allowing users on the same cell to quickly download a large volume of data.
- Latency speed less than 1 ms, virtually eliminating any delays or lags when requesting data from the network.
- Increased capacity to connect not only a high number of individual users but also more objects per specific geographical area.

The three characteristics above, together with mobility (staying connected while travelling at high speeds), energy efficiency (switching inactive radio interfaces into low-energy mode), service deployment and reliability, synthesize the key features of 5G networks that make them unique and, indeed, revolutionary as they promise to expand our ways of communication and completely transform our way of living.

5G's network infrastructure will no longer be based on the combination of specialised hardware and software elements. Instead, customization and functionality will take place only in the software. A new core network will support 'network slicing' features which will provide different service layers on the same physical network[8]. 5G, unlike previous technology, operates on three different spectrum bands (high, medium and low – see figure on next page) with each band having specific characteristics suitable for certain deployment scenarios. Finally, a more decentralized architecture than the traditional one in 4G will allow the network to steer traffic at the 'edge of the network' while still ensuring low response times.

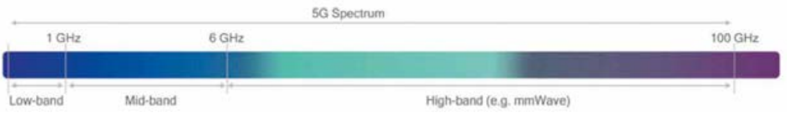


Figure: *5G Spectrum Strategies for Low-, Mid- and High-Band Ranges.*

5G technology enhanced by Artificial Intelligence (AI) is accelerating the development and implementation of technologies such as Connected Autonomous Vehicles (CAVs), 'smart cities', Virtual Reality (VR) and Augmented Reality (AR). Moreover, 5G networks contribute to a huge rise in the number of components in the Internet of Things (IoT), massively increasing the number and diversity of interconnected devices. It is predicted that around 75,44 billion devices worldwide will be 'online' by 2025[9], virtually connecting 'everything to everything' (X2X). Subsequently, 5G has the potential to transform the employment of military air operations and enhance its capabilities with components and functions that never existed before.

Cyber Threats

However, from a cyber-space perspective, 5G technology also increases drastically the attack surface (in some ways previously non-existent) and the number of potential entry points for attackers. The increased speed of the connected devices could make them more vulnerable to Distributed Denial-of-Service (DDoS) attacks. In today's era of 4G/LTE mobile Internet, a large botnet[10] formed simply by hacking a user's home devices could be used to launch large-scale DDoS attacks against websites; in tomorrow's 5G network era, a similar botnet could disrupt an entire network of autonomous cars in a city[11]. As a result, the wide range of services and applications, as well as the novel features in the architecture, will introduce a plethora of new security challenges.

It was in September 2016 when hackers succeeded in scanning and exploiting hundreds of thousands of low-cost and low-powered IoT devices such as IP cameras, home routers, and digital video recorders, and turned them into remotely controlled bots by using 'Mirai' malware to launch large scale DDoS attacks. Not only 5G technology itself but also the communication between devices connected to the internet can be the weakest link in 5G's security. If the manufactures of those low-cost interconnected devices do not embed cybersecurity standards in their products, the security risks will remain high.

5G networks and smart devices must adopt reliable and long-term security requirements beginning in the early stages of the design and manufacturing processes in order to fulfil their technological promises. By embracing a structured 'cyber hygiene policy', 5G technology can eventually be effectively implemented in Air Operations to improve communications and situational awareness.

Enhancing Air Power

NATO Allied Forces can gain great advantages by leveraging the novel features of 5G cellular technology. Communications and network operations in the air battlespace will be able to handle far more data at much faster speeds supporting real-time video streaming and VR applications. The wide employment of Unmanned Aerial Vehicles (UAVs) for purposes ranging from Intelligence, Surveillance & Reconnaissance (ISR) to airstrikes is expected to evolve even further in terms of geographic coverage and efficiency. Even logistic and maintenance activities, such as tracking maintenance stocks and conducting technical inspections, could benefit from a reliable and secure mobile connectivity.

Modern logistics systems such as the Autonomic Logistics Information System (ALIS) for the Joint Strike Fighter, are integrated with maintenance and operations procedures from across the world identifying problems with the aircraft, installing software updates, and providing preventive actions. 5G technology can clearly enhance productivity and safety of such complex, large-scale and interconnected military logistics operations transforming them to 'sophisticated weapon systems' ready to use even on the battlefield.

5G networks have the ability to expand the range of cloud-based applications and exponentially increase the amount of data transmitted and exchanged during air combat operations. The challenge of infobesity (information overload) can still be encountered using digital technologies that take advantage of the super-fast, high-bandwidth and low-latency communication environment that 5G provides. Consolidating the extracted information from internet-connected sensors and platforms, and immediately distributing the acquired knowledge to the Command and Control structure is essential to facilitate 'smart' decision-making[12]. Therefore, securing (allied) military networks and maintaining their high level of interoperability will become even more critical.

According to an 'EU coordinated risk assessment report'[13], published on 9 October 2019, among the main threats and vulnerabilities of 5G networks are the high dependencies on individual suppliers. The lack of diversity in equipment and infrastructure can lead to increased exposure to attacks by State-sponsored actors who interfere with the suppliers. Thus, the individual risk profile of suppliers will become particularly important, especially for those with significant presence within networks.

In order to develop a secure 5G mobile network strategy, the US Department of Defence (DoD) decided, about a year ago, to strengthen the requirements for the supply chain of innovative technology products, including subcontractors, by introducing higher cybersecurity standards that would ensure resiliency to cyber-attacks. The established public-private partnership, known as 'Trusted Capital Marketplace', connects defence technology start-ups with trusted sources of capital in order to secure the delivery of such critical emerging technologies[14].

Future Challenges

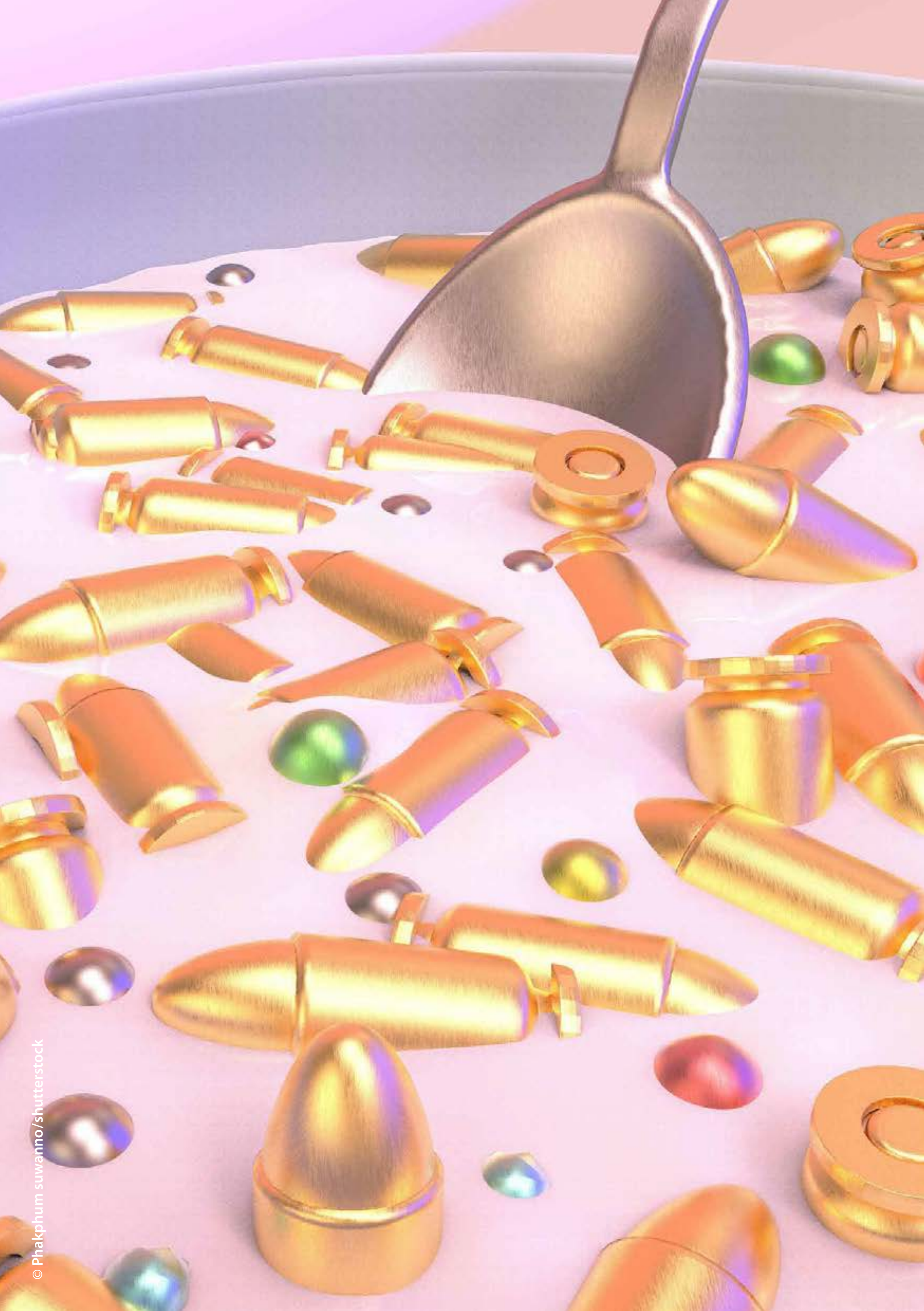
With the future stand-alone 5G ecosystem, as described above, all network functionalities will be virtualised based on software rather than hardware, and take place within a single cloud environment. 5G networks are going to be deployed in a complex global cybersecurity threat landscape. To ensure confidentiality (authorised access), integrity (accurate information) and availability (any time access) with such a revolutionary technology and confront the challenges derived from it, NATO member and partner countries will have to follow a new security paradigm. Current cybersecurity models and policies must be reassessed and new security frameworks applied in order to mitigate risks and threats.

Are Alliance members determined to invest the resources necessary for establishing a resilient and secure infrastructure for 5G technology? Are we willing to adapt to this emerging technology at the speed of change and not lagging behind other competing nations? Those questions have to be answered as clearly and decisively as possible in the very near future.

Major Fotios Kanellos (GRC AF) is currently the NATO Cyberspace SME at JAPCC. His academic background is in Electrical Engineering with a specialization in Telecommunication and Computer Science. His previous appointment was at the Hellenic Air Force Support Command (HAFSC) managing IT and Cybersecurity projects.

Endnotes

1. A relatively recent definition of 5G networks provided by the EU Commission Recommendation 2019/534 (26 Mar. 2019) is 'all relevant network infrastructure elements for mobile and wireless communications technology used for connectivity and value-added services with advanced performance characteristics such as very high data rates and capacity, low latency communications, ultra-high reliability, or supporting a high number of connected devices. These may include legacy networks elements based on previous generations of mobile and wireless communications technology such as 4G or 3G. 5G networks should be understood to include all relevant parts of the network.'
2. Fragouli, N., '5G brings $2.2Tn to the economy over the next 15 years', Hellenic Association of IT & Communications, 2019 http://www.sepe.gr/gr/research-studies/article/13004311/axia-22-tris-fernei-to-5g-stin-oikonomia-ta-epomena-15-hronia/, accessed 21 Feb. 2020.
3. NIS Cooperation Group, 'Cybersecurity of 5G networks: EU Toolbox of risk mitigating measures',CG Publication, 29 Jan. 2020.
4. 4G LTE stands for the 4th Generation of Cellular Network Long Term Evolution. LTE is considered an improvement of the 4G.
5. The first commercial use of 4G was in Norway and Sweden.
6. Techopedia, 'Fifth Generation Wireless (5G)', https://www.techopedia.com/definition/28325/fifth-generation-wireless-5g, accessed 21 Feb. 2020.
7. CPO Magazine, '5G and the Future of Cybersecurity', https://www.cpomagazine.com/cyber-security/5g-and-the-future-of-cybersecurity/, accessed 21 Feb. 2020.
8. Each 'layer' will perform in parallel varying functions across the network, processing different volumes of information and transporting data packets to and from other layers within it.
9. Statista Research Department, 'Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025', https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/, accessed 21 Feb. 2020.
10. 'A botnet is a set of computers infected by bots. A bot is a piece of malicious software that gets orders from a master. (…). A computer becomes infected either when a worm or virus installs the bot, or when the user visits a malicious web site that exploits a vulnerability in the browser'. ENISA, https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/botnets, accessed 21 Feb. 2020.
11. Ibid. 7.
12. Pappalardo, D., 'The Role of the Human in Systems of Systems: Example of the French Future Combat Air System', OTH Journal, 2020, https://othjournal.com/2020/01/27/the-role-of-the-human-in-systems-of-systems-example-of-the-french-future-combat-air-system/amp/, accessed 21 Feb. 2020.
13. European Commission, 'Member States publish a report on EU coordinated risk assessment of 5G networks security', Press Release, Oct. 2019, https://ec.europa.eu/commission/presscorner/detail/en/ip_19_6049, accessed 21 Feb. 2020.
14. Mitchell, B., 'DoD to launch Trusted Capital Marketplace of startups, investors', FedScoop, 2019, https://www.fedscoop.com/dod-trusted-capital-marketplace-ellen-lord/, accessed 21 Feb. 2020.



© Phakphum suwanno/shutterstock

Remote Warfare and the Erosion of the Military Profession

XXVI

'Kill the enemy and don't forget to buy milk on the way home.'

'… all our fine new technologies and fine new legal theories were blurring the boundaries of 'war', causing it to spread and ooze into everyday life.'

Rosa Brooks[1]

'I'd literally just walked out on dropping bombs on the enemy, and 20 minutes later I'd get a text – can you pick up some milk on your way home?'

Jeff Bright (retired pilot)[2]

By Gp Capt Jo Brick, AUS Air Force
Courtesy of The Forge, the website of the Australian Defence College

As Brooks and Bright highlight, the emergence of technology that enables the conduct of armed conflict from 'home' has led to the disappearance of a clear dividing line between war and peace. Contemporary and future combatants using remote warfare technologies in support of the NATO mission are essentially caught in a state of permanent liminality – of being caught 'betwixt and between' war and peace.

Such technology affords us the major advantage of removing our own forces from areas of danger, yet the conduct of strike missions from afar creates a dangerous context that may likely result in the erosion of ethical paradigms held by the profession of arms. This is exacerbated by the unending conflicts in Iraq and Afghanistan, which have been in progress for almost two decades and currently show little sign of abating. These wars largely occur out of sight – in the cloisters of Defence headquarters, in air operations centres, and ground control stations – whether in operational areas or at home. Even in this context, the combatant 'privilege' of killing in armed conflict must retain its extraordinary place in the legal and ethical canon of nations with professional standing military forces. This demands the construction of clear ritualised transitions between war and peace that are established and enforced by national leaders and military commanders. The ritual can be something as simple as changing clothes into a particular uniform worn only on duty at that place, coupled with detailed pre and post mission briefs that mark a handover of shifts. The challenge in secular and multicultural military forces is to find a ritual that addresses the psychological or spiritual aspects required by a workforce from diverse backgrounds. It is easy to be transfixed only on the capabilities offered by emerging technologies such as next generation aircraft, artificial intelligence, and remote weapons platforms. However, for war to have meaning within society – as a means for human societies to achieve strategic objectives – then we must examine and acknowledge the price of emerging technologies on the humans who use or 'team' with these new capabilities.

The Danger of Permanent Liminality

The persistence of contemporary conflict has split Clausewitz's aphorism. The politics of war are no longer clear or transparent and war continues indefinitely.[3] The blurring of this distinction is further exacerbated by the persistent presence and reach offered by airpower – particularly Remotely

Piloted Aircraft (RPA). Those who bear the burden of fighting these wars remain caught in a state of 'permanent liminality', which is an anthropological concept that is defined as meaning 'betwixt and between'.[4] This concept originated from the 1909 publication Rites de Passage by French anthropologist, Arnold Van Gennep, who undertook a taxonomy of existing rites within different social groups that marked the passage of individuals from one status to another.[5] Van Gennep identified 'rites of passage' as a particular type of ritual that consisted of three sub-categories of rites: rites of separation, transition rites ('liminal rites'), and rites of incorporation.[6] Van Gennep's work was re-discovered in the 1960s by Victor Turner, who advanced the concept of liminality by examining the importance of these transitory periods, the human reaction to such experiences, and how they are shaped by liminality.[7] The key point is the place that transitional rites or liminal rites hold as a transformative experience from one status to another. Thomassen's paper considers 'permanent liminality', which occurs when the rites of incorporation do not occur and the transformative experience is not complete. In the context of extant conflicts, when the framework of liminality is applied to the experience of RPA operators, it may be possible to obtain some insight into what these dangers may be in that particular context.

In the context of today's persistent wars, the concept of liminality can be used to describe the state of being caught between war and peace. The state of liminality exists because the reach of modern military capability has provided a bridge between two planes of existence that overlap: a physical state of 'peace' and a psychological state of 'war'. When coupled with the mental intimacy that the sensors of RPAs provide, there is a significant jarring effect for the operators as they move quickly between these states. What is needed to mitigate these effects are overt 'rituals of war' that traditionally marked a rite of passage between war and peace. This is necessary to counter the erosion of the special status of 'war' and the dilution of the privileges and obligations that accompany it. The erosion of these traditional rituals of war, which is the gateway between war and peace, may be accompanied by a significant risk of ethical or professional degradation caused by war becoming routine and 'normal'. Strong, principled, and ethically conscious leadership is necessary to maintain a warfighting ethos, accompanied by an ethical framework for coherence in which these operators can mentally place their wartime experiences. Many NATO countries have had RPAs in service for some time, and the issue of remote warfare has been discussed for almost a decade.[8] The time to address these issues related to preparing and building resilience in the personnel caught in a state of permanent liminality is long overdue.

Former RAF chaplain, Dr Peter Lee, conducted research into the experience of RPA operators by spending periods of time with operators from the 39 Squadron (Royal Air Force) at Creech Air Force Base, Nevada, United States; and XIII Squadron at RAF Waddington in Lincolnshire, United Kingdom. He recounts his experience in his book, Reaper Force – Inside Britain's Drone Wars, which provides vivid accounts of the firsthand experiences of RPA operators of the MQ-9 Reaper RPA.[9] A significant point that arises throughout Lee's work is the disjointedness of their experience. The practical effect of the operators' state of permanent liminality is that diametrically opposed ideas attempt to occupy the same psychological space at the same time. The operators can concurrently exist in a state of war and peace. Lee relates one particularly poignant example. A Mission Intelligence Coordinator (MIC) named 'Jamie' relates an incident from 2011 where a strike in Helmand Province, Afghanistan, resulted in civilian casualties ('civcas') including children.[10] Jamie's account of his thoughts as he drove home after this incident demonstrates the liminal nature of his existence:

How did I find myself in this situation? … How did my first weapon event turn into a nightmare, an awful nightmare? What have I got myself into? Then a reality check: What time do I need to pick up Jane and the kids from the barbecue? (emphasis in original).[11]

Although the operators physically exist in a location far from the operations area in which the physical consequences of their actions manifest, their psychological existence occupies both war and peace. One minute they are at war; the next they are at church or picking up their kids from school.'[12] Existing within a state of permanent liminality probably has significant jarring effects on the mental state of these operators, as Lee attests: 'The normality of events immediately after they exited the GCS seemed abnormal.'[13]

Warfighting Ethos and Ethical Frameworks Essential

The acquisition of RPAs have provided states with the ability to project force into the relevant operational area, well beyond their geographic boundaries. However, the human cost of the capability must be brought to the forefront of the minds of military and civilian leaders. From a purely capability perspective, preserving the force that operates the Reaper is just as important as routine maintenance on the RPA system itself. Most importantly, however, the state is under a moral obligation to look after the very citizens in the military forces that are the means for protecting itself or advancing its strategic interests. As Phil Klay commented, '(j)oining the military is an act of faith in one's country – an act of faith that the country will use your life well.'[14] To discharge this obligation to the operators, commanders take action in two ways: (1) use overt rituals to mitigate the effects of permanent liminality and establish a strong military ethos in the unit; and (2) create an ethical framework that can form the foundation on which the operators can situate their experience, and form an anchor for military professionalism and ethical decision-making.

Codes of behaviour have been a significant part of any profession, including the profession of arms. These codes are generally the foundation for ethical conduct of the fighting classes throughout history and form the starting point for guiding ethical conduct.[15] However, more is needed for those caught in a state of permanent liminality and who have a psychologically intimate connection with the individuals they see and kill via RPA capabilities. When these operators are on duty, they require strong anchors to the world of war as a means to preserve it as an extraordinary space that sits outside the ordinary world that awaits the operator at the end of shift, beyond the GCS door. Operators require ongoing, focused, education in the fundamental philosophies, values and ethical frameworks of the profession of arms that are for a number of important reasons: to gain a comprehensive understanding and appreciation of their privileged status as combatants, that they are imbued with this privilege for the purposes of their duty to the nation and not for their personal reasons; and the reasons why they must kill others as part of their duty.

Conclusion

RPAs offer an effective capability to a nation's military force that allows for these prolonged wars to be waged from home. Such systems place the people who operate them in a state of permanent liminality as they move across insufficient boundaries between war and peace on a daily basis. The blurring of the distinction between 'war' and 'peace' places an obligation on military leaders to ensure that warfare is not normalised, and to preserve the status of warfare as 'special' or 'sacred'. This can be achieved by the creation of rituals that form rites of passage to ease the transition of operators between war and peace as they conduct their daily duties. Rituals have been a central part of warfare for centuries.[16] These rituals may include enhancing current practice such as mandating operators to change into and out of uniform form civilian clothes at the beginning or end of shift. Further the delivery of more detailed pre-and post mission briefs that include discussion of significant personal ethical challenges faced by crew members during that shift. This enables the crew members to metaphorically 'leave behind' their concerns at the end of the shift. The challenge is in finding rituals that address individual psychological and spiritual needs within a diverse and multicultural workforce. The inculcation of a practical understanding of the philosophical foundations of warfare via professional military education programs and mission specific training can be a means for preserving the status of war as being 'extraordinary'.

Group Captain Jo Brick is a Legal Officer in the Royal Australian Air Force and is currently the Chief of Staff, Australian Defence College. Previous appointments include Legal Advisor to the Chief of the Defence Force, and Legal Advisor to the Chief of Air Force.

Endnotes

1. Brooks, Rosa. How Everything Became War and the Military Became Everything – Tales from the Pentagon (New York: Simon & Schuster, 2016): p. 4.
2. Eyal Press, 'The Wounds of the Drone Warrior,' New York Times, 13 Jun. 2018 (accessed 21 May 2019). Available at https://www.nytimes.com/2018/06/13/magazine/veterans-ptsd-drone-warrior-wounds.html.
3. von Clausewitz, Carl, statement: 'war is not entirely an act of policy but a true political instrument, a continuation of political intercourse, carried out by other means.' Carl von Clausewitz. On War. Translated by Michael Howard and Peter Paret (Princeton: Princeton University Press, 1984): p. 87.
4. Beech, Nic, 'Liminality and the practices of identity construction,' Human Relations 64, no.2 (2011): p. 286.
5. Thomassen, Bjorn, 'The Uses and Meanings of Liminality', International Political Anthropology 2, no. 1 (2009): p. 6.
6. Thomassen, 'The Uses and Meanings of Liminality', p. 6.
7. Ibid., p. 14.
8. See National Public Radio, 'War by Remote Control: Drones Make it Easy', 26 Nov. 2011 (accessed 26 Feb. 2020). Available from https://www.npr.org/2011/11/26/142781012/war-by-remote-control-drones-make-it-easy.
9. Lee, Peter. Reaper Force – Inside Britain's Drone Wars (London: John Blake, 2018).
10. Ibid., p. 93-113.
11. Ibid., p. 107.
12. Press, 'The Wounds of the Drone Warrior'.
13. Ibid. 9., p. 106.
14. Klay, Phil. 'The Citizen-Soldier. Moral Risk and the Modern Military', The Brookings Essay, 24 May 2016 http://csweb.brookings.edu/content/research/essays/2016/the-citizen-soldier.html (accessed 28 May 2019).
15. See Shannon E. French. The Code of the Warrior. Exploring Warrior Values Past and Present (London: Rowman & Littlefield, 2017); and Nathan K Finney and Tyrell O. Mayfield (eds). Redefining the Modern Military. The Intersection of Profession and Ethics (Annapolis: Naval Institute Press, 2018).
16. See brief discussion by Ruddy Canno, '5 Rituals Warriors Used to Prepare for Battle', We Are The Mighty online, posted 14 Dec. 2018: https://www.wearethemighty.com/history/the-rituals-of-battle (accessed 4 Apr. 2020).

© U.S. Air Force graphic

Hypersonics: Changing the NATO Deterrence Game

XXVII

By Dr Cathy Moloney
Australian Defence College, Department of Defence

As NATO 'increases investment into innovation to harness the benefits and mitigate the risks of emerging technologies, such as hypersonic systems,' will the current 'balanced and defensive package of measures that ensure the credibility and effectiveness of our deterrence'[1] defend against this new capability? The emergence of hypersonic weapons provides a new challenge to strategy and the way we think about deterrence. Russia's new hypersonic capability demands NATO reconsider its approach to its deterrence and defence posture. This paper argues that hypersonic weapons will change the nature of NATO's strategic posture. The threat of hypersonic weapons increases the likelihood of compellence or coercion by risk as defined by Pape and Schelling.[2] The integration of the offensive use of hypersonic weapons capability into Russian operational doctrine, in tandem with the use of nuclear weapons, creates serious escalatory dynamics for NATO. The purpose of this piece however is not to detail the engineering feats of hypersonic missiles, rather it is to highlight how these technologies can be used for deterrent and coercive purposes. Beginning with an examination of the current state of NATO Air and Space power, the paper will outline traditional understandings of deterrence and how emerging hypersonic technology could change this. Thus, the development of hypersonic technology will have a large and possibly irreversible impact for NATO, and globally will have far-reaching consequences for the international system, state behaviour, escalatory dynamics and the distribution of state power. The paper then concludes that a theoretical (not just scientific or operational) understanding of hypersonic weapons and the strategic impact of such systems is imperative.

Current State of NATO Deterrence

In the twentieth century, NATO existed to perform a specific function: keep the people and territory of the NATO member states safe from Soviet attack. In order to achieve this, NATO members unified militarily and politically to prevent possible threats from the Soviet Bloc through a doctrine of deterrence. In the twenty-first century, however, this doctrine of deterrence needs reinvigorating due to the rising tensions reappearing among great powers; the continuing threat of terrorism; and the changing character of war to include hybrid, asymmetrical, cyber and information warfare. In the area of air and space disruptive technology, the Russian testing of hypersonic weapons is chief among the threats to NATO deterrence doctrine. In the 2017 JAPCC Conference Read Ahead, which focused on NATO Deterrence, Henrik Breitenbauch argued that after the Ukraine conflict in 2014, NATO shifted its attention to conventional deterrence and defence. He reasoned that while Russia was unlikely to 'commit the bulk of armed forces in an incursion in a Baltic state, Russia's conventional advantage in the region is still decisive'.[3] He was correct in observing that Russian conventional advantage is powerful and therefore NATO neighbours are at risk of military intervention. If Russia is willing to escalate its use of conventional weapons, as we saw in Syria with the surprise use of cruise missiles, is NATO's deterrence and defence doctrine ready for the possible use of the hypersonic weapons?

Traditional Understandings of Deterrence

Deterrence is a relatively simple idea; convince your opponent that the costs of attacking you will outweigh any potential gains. During the Cold War deterrence generally worked due to three factors. First, the West had the political will to act as one against the adversary. Second, the West had the military power to back up its own threats. And third, there was a clear and consistent message that the West would – without doubt – be ready, willing and able to defend the alliance. But, as Shelling observed, deterrence and international relations are often characterised by the competition of risk-taking – not so much by a test of force but a test of nerve. The test is not who can bring force but who is willing to bring the most force to bear or at least make it appear so.[4]

In the case of nuclear deterrence, which was key for NATO in the last half of the twentieth century, Brodie argued that it was nuclear weapons themselves that were the existential deterrent, not the nuclear deterrence strategies. In the Cuban Missile Crisis 'neither side needed to believe the other side would deliberately and knowingly take the step [to use the weapons] that would raise the possibility [of war] to a certainty … it a was a contest of risk taking.'[5] Having a nuclear deterrent threat is generally considered more credible because of the magnitude of the weapon. Sir Michael Quinlan argued that 'weapons deter by the possibility of their use'[6], or in other words, no matter how distant the possibility of their use it is necessary to understand the doctrines and plans for their employment. However, in the game of deterrence and coercion, which are in effect complementary, deterrent threats 'can shift the burden of the first hostile move to the target of the threat'.[7] As will be discussed later, Putin has made statements which would lead one to believe we will see this 'existential use' of hypersonic weapons in the future.

Coercive threats are inherently less credible against a legitimate deterrent threat. However – and this is where hypersonic weapons may become a credible and conventional alternative to a nuclear capability – a coercer 'tends to bolster their credibility by favouring threats that can be fulfilled in progressive stages'. Nuclear weapons do not provide this option. The destruction wrought is so significant there is too little left of the state to warrant changing its behaviour.[8] The next best thing for military coercive tactics would be to threaten the use of a hypersonic weapon because of its agility and manoeuvrability. Unlike its precision-guided missile cousins, the act of such a surprise attack (if they were to be used) still allows for an operation of progressive attacks to coerce the adversary to change their behaviour. Therefore, deterrence in this instance needs be understood in relation to this uncertainty.

Emerging Hypersonic Tech

Hypersonic development is not new; but, it is important. Why? Because these weapons are primarily designed to breach existing or forthcoming missile defence systems that currently ensure the ability to deter advances from adversaries. Not only can they reach speeds faster than Mach 5 – they are able to manoeuvre. Unlike ballistic missiles, which follow a stable trajectory that allows for missile detection systems to estimate the missile's destination, hypersonics that can manoeuvre at hyper-speed are the new danger.[9] Two systems of interest with this capability are hypersonic glide vehicles and hypersonic cruise missiles. The former is a high-velocity booster, where the missile separates and uses momentum in the upper atmosphere before zeroing in on its target. The latter utilises a SCRAMJET propulsion system to reach its target.[10] Russia, China and the United States all have hypersonic development programs. Russia is at the forefront of fielding this capability, having tested its Avangard glide vehicle in December 2019.[11] Further tests were conducted near Crimea on 9 January 2020, when Russia practiced the launch of the hypersonic air-launched ballistic missile Kinzhal from two MiG-31K fighters. Both are now considered 'in service' and thus deployable capability for the Russian military.

Russian Doctrine and the Use of Hypersonics/Deterrence

So, what does this mean in Russian military doctrine? According to a comprehensive report by David Johnson, 'the role of conventional precision weapons' in strategic deterrence is their instrumentality'.[12] President Putin went so far as to claim that a 'state with such weapons [conventional (non-nuclear) precision weapons] at its disposal seriously increases its offensive potential'. Furthermore, [they] 'are comparable to employment of nuclear weapons in results but more 'acceptable' in political and military terms'.[13]

If it is true, as Putin claims, that his new capability can bring the neutralization of any military threat to Russia then NATO must reconsider its deterrent and defence posture. As Johnson argues though, one cannot take this instrumentality for granted or as a fait-accompli. Strategic deterrence with nuclear weapons is primarily utilised in this instance 'in their non-use'. Putin may have a point; strategic objectives can be advanced by threatening to use hypersonic capabilities, maybe not toward the US but certainly for proximity nations like European members of NATO. As Cummings points out, an air-launched Kinzhal on the Russian western border could target and hit London, Paris or Rome in about 11 minutes; the recently tested Avangard expands this reach both in range and limiting the time to impact even further. Currently, neither the US nor NATO have the capability to intercept or defend against this capability. Thus, NATO must consider how it will interact with Russia in this new world of hypersonic capability.

Just as nuclear weapons change state behaviour and the military escalation calculus, so can the threat of the Russian hypersonic capability.

Rhetoric could quickly escalate to kinetic action and the speed could '[inflict] damage using units that are well-dispersed and may appear unrelated to each other or to the conflict'.[14] To this end, what will need to change for NATO and what questions do NATO partners need to ask themselves?

- Do our current deterrent measures account for the new Russian capability?
- If not, what are we willing to risk if this capability is put into use?
- Who will take the lead and counter the new Russian capability?

Putin has argued that his new hypersonic capability is just as powerful a tool in coercing adversaries as his nuclear capability. But we also know that he is willing to escalate his military capability; no one saw the use of cruise missiles in Syria coming. Therefore, it is prudent for NATO to consider all options in the hypersonic era.

Conclusion

When it comes to hypersonic deterrence, political as well as military strategy is key. In the same way as during the Cold War NATO's deterrence strategy was underpinned by the three pillars of political will, military capability and coherent communications among the allies, hypersonic deterrence will need a concerted and coordinated effort to bind political and military strategy together. Strategy and policymakers must shift from a doctrine of mass retaliation to an agile response to new and disruptive technologies. The recent successful testing of Russian hypersonic missiles means that this is not an abstract conversation to have on a theoretical or academic level. Nor is this just a concern raised in the face of Russia's developments given China's force modernisation and the US's own development of hypersonic missiles. It is not just a theory anymore but a real and known threat that could very easily be operationalised by Russia if threatened – or used as a coercive tool to change great power politics.

Dr Cathy Moloney is the Head of the Centre for Defence Research, Australian Defence College. She holds a PhD in Nuclear Policy and International Relations (Griffith University), and a Master of International Politics (1st Class, University of Melbourne).

Endnotes

[1] North Atlantic Treaty Organization. 2019. NATO: Ready For The Future - Adapting the alliance (2018 – 2019). North Atlantic Treaty Organization.

[2] Pape, Robert, A. 1996. Bombing to Win: Air Power and Coercion in War. Ithaca, New York: Cornell University Press. Schelling, Thomas, C. 1966. Arms and Influence. New Haven: Yale University Press.

[3] Breitenbauch, Henrik. 2017. 'NATO: Conventional Deterrence is the New Black.' Germany: The Joint Air Power Competence Centre. 45-51

[4] Schelling, Thomas, C. 1966. Arms and Influence. New Haven: Yale University Press. p. 69-91.

[5] Ibid., p. 96.

[6] Quinlan, M. (1997). Thinking about Nuclear Weapons. London, UK: The Royal United Services Institute for Defence Studies.

[7] Pape, Robert, A. 1996. Bombing to Win: Air Power and Coercion in War. Ithaca, New York: Cornell University Press. p. 7-10

[8] Ibid.

[9] Thompsen, Loren, 'To defeat hypersonic weapons, Pentagon aims to Build Vast Space Sensor Layer', Forbes, 4 Feb. 2020. Accessed 19 Feb. 2020 Available from www.forbes.com.

[10] Cummings, Alan 'Hypersonic Weapons: Tactical uses and Strategic goals', War On The Rocks, 12 Nov. 2019, https://warontherocks.com/2019/11/hypersonic-weapons-tactical-uses-and-strategic-goals. Accessed 23 Jan. 2020.

[11] BBC News. (27. Dec 2019). Russia deploys Avangard hypersonic missile system. BBC News Online. British Broadcasting Corporation.

[12] Johnson, D. (2018). Russia's conventional Precision Strike Capabilities, Regional Crises, and Nuclear Thresholds. Lawrence Livermore National Laboratory. Livermore, California: Center for Global Security Research, p. 46.

[13] Ibid.

[14] Cummings, A. Hypersonic Weapons.

© breakermaximus/shutterstock

Forecasting Change in Military Technology, 2020–2040

XXVIII

By Mr Michael E. O'Hanlon,
Brookings Institution

Note: This essay is an abridged version of the report 'Forecasting change in military technology, 2020 – 2040,' published September 2018 on the Brookings Institution website, www.brookings.edu.

What changes are likely in military technology over the next 20 years? This question is fascinating on its own terms. More importantly, answering it is crucial for making appropriate changes in US and allied weaponry, military operations, wartime preparations, and defense budget priorities. To be sure, technology is advancing fast in many realms. But it is not enough to wave one's arms exuberantly about futuristic military possibilities. The stakes are too high. Defense resource decisions need to be based on concrete analysis that breaks down the categories of major military technological invention and innovation one by one and examines each. Presumably, those areas where things are changing fastest may warrant the most investment, as well as the most creative thinking about how to modify tactics and operational plans to exploit new opportunities (and mitigate new vulnerabilities that adversaries may develop as a result of these same likely advances). Building on the methodology employed in my earlier 2000 book, *Technological Change* *and the Future of Warfare*, and refined further in my recent paper, 'A Retrospective on the So-Called Revolution in Military Affairs, 2000 – 2020,' this paper attempts to look two decades into the future to aid in this important task for American defense planners.

My working hypothesis is that 20 years is long enough to represent a true extrapolation into the future. Yet it is also short enough that existing trends in laboratory research can help us understand the future without indulging in rampant speculation. Since many defense systems take a couple of decades to develop, it should not be an overly daunting task to gauge how the world might look, in terms of deployable military technology, 20 years from now. This approach is not foolproof, as discussed in my forthcoming book, but if undertaken with the proper degree of acknowledged uncertainty, can still be quite useful.

This paper's category-by-category examination of military technology employs the same basic framework that I developed in my book published in 2000, Technological Change and the Future of Warfare. The core of that book was an analysis of ongoing and likely future developments in 29 different types of military-related technologies. My goal was to attempt to determine in which areas the pace of change was likely to be revolutionary over the following 20 years, versus high or moderate. Revolutionary change is defined, notionally, as a type and pace of progress that renders obsolete old weapons, tactics, and operational approaches while making new ones possible. My methodology began with a focus on the foundational concepts of physics, to understand the limits of the possible. I also examined the scientific, engineering, and defense literature on various types of technological research, to understand what was likely to be developed over the 2000 – 2020 time period. Finally, armed with my own initial estimates of key trends in those 29 areas, I then consulted with experts, including at several of the nation's major weapons laboratories, for their feedback and advice. With this research complete, I then argued in the book that in fact only two of the 29 categories of technology were likely to experience truly revolutionary change – and thus to create the potential for military revolution when combined with other kinds of available technologies as well as new operational and strategic concepts. Those two areas of predicted revolutionary advance were computer hardware and computer software.

As discussed further in my concurrent paper 'A Retrospective on the So-Called Revolution in Military Affairs, 2000 – 2020,' I have subsequently concluded that I was right about computers but should have added robotics to the list of technologies likely to experience radical change (my earlier estimate, in 2000, forecast a 'high' pace of change for robotics such as unmanned aerial vehicles, rather than radical or revolutionary progress). Notably, there are now some 20,000 unmanned vehicles of various types in the Department of Defense's (DoD) inventory, and the various new uses to which they have been put during this century, from Iraq and Afghanistan to the broader Middle East and beyond, are remarkable. Enemy forces are increasingly using robotics, too.

I should have also underscored the degree to which progress in computers could create vulnerabilities, as nations increasingly utilized computer systems and software that created potentially gaping weaknesses in their military capabilities. This point proved important enough that in retrospect I should have given it special and separate emphasis. Thus, in my earlier taxonomy, I had one important area of technology where I underestimated the potential for revolutionary advancement, and another where I should have underscored additional dimensions of likely change.

In the earlier book, I also predicted that another seven categories of technology would likely witness high change – chemical sensors, biological sensors, radio communications, laser communications, radio-frequency weapons, nonlethal weapons, and biological weapons. The remaining

19 categories of key military technologies, many of them sensor technologies or major components of weapons platforms like ground combat vehicles, aircraft, ships, and rockets, seemed likely to advance at only modest or moderate rates. In my concurrent paper, I revisit these prognostications one by one. In general, the thrust of my estimates seems to have been mostly correct, though with a number of specific imperfections in which progress that I had forecast to be high or rapid proved to be only moderate, or vice versa. Crucially, however, putting aside robotics, I do not believe that any of the remaining 26 areas of technology did in fact undergo revolutionary change.

Two lessons emerge from this previous analysis. One, the approach I developed in the 2000 book appears useful. Assessing future trends in military technology by examining a number of fairly broad, yet also fairly specific and discrete areas of defense-related technology, and then integrating these individual findings into a broader framework for predicting future war, is valuable. This methodology discourages hyperbole based on cherry-picking areas of technology that may be most (or least) promising. It also helps to identify those specific technological enablers that are most likely to cause any radical change in broader military capabilities – to figure out what might drive a revolution in military affairs, should there be such a thing anytime soon.

Second, to the extent that there were flaws in my approach and my analysis, it is important to understand their origins, and attempt to take remedial action in any future prognostication. Most importantly, it was difficult to predict how military organizations would avail themselves of new technological opportunities – or, alternatively, to allow themselves to remain or become vulnerable in the face of new capabilities possessed by possible adversaries. In other words, the challenge was largely in predicting how entrepreneurial military organizations might, or might not, respond to transformational opportunities for better or worse.

In terms of robotics, US military organizations responded with innovative and entrepreneurial acumen, creating new tactical methods to handle the challenges of complex counterinsurgency and counterterrorism operations. Other military organizations around the world have also made significant progress in this arena.

In regard to computers, however, modern militaries generally have not succeeded. Indeed, they carelessly allowed themselves to build Achilles' heels into their own systems, as well as their supporting national civilian infrastructure that is often essential to the operations of modern military forces. Thus, they have potentially made the performance of future weapons less dependable than past ones had been. In other words, they may even have set themselves back, though it is impossible to know for sure at this point, since we have not seen the kind of interstate warfare among near-peer competitors that would probably be needed to assess the hypothesis accurately.

Those operating in the classified world may have a greater sense than I of the vulnerabilities and opportunities that the United States now faces due to cyber technology. But even they cannot be sure because cyber vulnerabilities are not static. They are always evolving in a game of measures and countermeasures, even faster than in other areas of military operations characterized by these kinds of dynamics, such as electronic warfare. In addition, the ripple effects of any cyberattack often cannot be easily foreseen even when specific vulnerabilities are understood. There may also be important path dependencies about how different types of failures might collectively affect a larger system. It is difficult to evaluate these possibilities by examining individual vulnerabilities alone.

It is not surprising that forecasting the future would be hardest when complex concepts are involved and when large military organizations are the key actors. Scientists can invent new capabilities in ways that are often partially projectable and foreseeable over a 20-year time horizon based on what is known about their present research activities as well as opportunities opened up by the state of modern science and engineering. However, when it comes to combining technologies into systems and operational concepts that can be instrumental in fighting wars, the human dimension of organizational performance, influenced by the external combat environment as well as domestic and bureaucratic politics, introduces new variables into the mix, as the writings of Stephen Rosen, Thomas Ehrhard, Barry Posen, Stephen Biddle, and others attest. The Revolution in Military Affairs (RMA) debate of the 1990s underscored the reality that, while technology can provide the raw materials for military revolutions, those revolutions must ultimately be sparked by entrepreneurship and organizational adaptation. This was true historically, as with the inventions or transformations of the blitzkrieg, integrated air defense, aircraft carrier operations, amphibious assault, anti-submarine warfare systems, and the atomic bomb in the 1930s and 1940s. It remains true today.

To preview the results of this paper, my overall assessment is that technological change of relevance to military innovation may be faster and more consequential in the next 20 years than it has proven to be over the last 20. Notably, it is entirely possible that the ongoing, rapid pace of computer innovation may make the next two decades more revolutionary than the last two. The dynamics in robotics and in cybersecurity discussed here may only intensify. They may be more fully exploited by modern military organizations. They will likely extend in important ways into the artificial intelligence (AI) realm as well. At least, an examination of the last 20 years would seem to suggest the potential for such an acceleration. That is particularly true in light of the fact that multiple countries (most notably China, but also Russia) now have the resources to compete with Western nations in military innovation. Some other areas of technology, perhaps most notably directed energy systems, hypersonic missiles, and certain types of advanced materials, could play important supplemental roles in making the next two decades a true period of military revolution, or at least of very fast and ongoing rapid transformation.

My assessment of trends in key areas of military-relevant technology is organized into four categories. The first is sensors, of many different types, which gather data of relevance to military operations. The second comprises the computer and communications systems that process and distribute that data. Third are major weapons platforms and key enabling technologies for those platforms. Fourth are other types of weapons systems and other technologies, many relatively new. Within these four general areas, all of the 29 sub-categories of technology that I employed in the 2000 book are retained here, in addition to 10 new sub-categories. Four of the 10 are within the computers and communications category: offensive cyber capabilities, systemic or 'internet of things' networking, quantum computing, and artificial intelligence and big data. Two are within the projectiles, propulsion, and platforms category – battery-powered engines and satellites. Four more are within the final, miscellaneous category: chemical weapons, nanomaterials, 3D printing, and human enhancement devices as well as substances. I now proceed with this discussion, organized with the four major categories mentioned above.

Michael O'Hanlon is a senior fellow, and director of research, in Foreign Policy at the Brookings Institution, where he specializes in US defense strategy, the use of military force, and American national security policy. He is an adjunct professor at Columbia, Georgetown, and Syracuse universities, and a member of the International Institute for Strategic Studies.

Joint Air Power Competence Centre
JAPCC

The Executive Director's Closing Remarks

Lt Gen Klaus Habersetzer, DEU Air Force

Executive Director, Joint Air Power Competence Centre

It is my hope that the essays provided in our Conference Read Ahead have been informative and enlightening. Our goal is for these essays to inspire and provoke discussion during our upcoming conference concerning the role of Joint Air and Space Power in NATO deterrence and defence. As the Executive Director of the Joint Air Power Competence Centre, I wanted to take this opportunity to offer my perspective and highlight some elements of the theme of this year's conference on Leveraging Emerging Technology.

In the fall of 2019, when we first selected the theme for the 2020 Conference, we didn't realize how quickly we would be leveraging new technologies in the conduct of our daily activities. The challenges associated with COVID-19 Pandemic have pushed the use of various communications technologies to the forefront, as we adapted to new ways to execute missions on behalf of the Alliance while practicing social distancing in the hopes of slowing the spread of the corona-virus.

And NATO's Mission has expanded. The recognition of Space as NATO's newest operational domain late last year, coupled with the establishment of Space Commands in France, the United Kingdom, and the

United States, has catalyzed a focus and excitement related to Space not seen in decades. As other Alliance Nations determine their national way ahead with regards to Space, NATO is determining the ways in which it will implement Space within the command structure. Space Experts assigned to the JAPCC continue to provide independent thought and analysis in support of decision-makers, and one of the Conference Panels will focus on Space. Not only on how NATO can leverage emerging Space-related technologies, but also on policy, doctrinal, and operational considerations.

At the same time that NATO’s role in Space has been increasing, certain terrestrial missions remain front and centre. Nations dealing with the recent pandemic also saw a continuing need for NATO’s Air Policing Activities, intercepting non-NATO aligned aircraft sometimes operating near NATO military forces. The activities were taking place at the same time as an increase in disinformation campaigns associated with the global pandemic, in an attempt to sow confusion, create discord, and undermine the Alliance. These types of activities are part of a larger Information Competition involving the manipulation of information and disruption of the electronic pathways which our information travels across. Fortunately, our Conference will include a Panel which addresses the gray zone associated with the Information Environment, including the competition and technologies utilized therein.

Our ability to successfully compete in the information environment directly affects NATO’s ability to manage the Battlespace. Not only must NATO be able to command and control its forces during military operations, but it must look to safeguard and expand its capability. By utilizing artificial intelligence NATO can seek ways to rapidly process data and assess information to improve its current ability to control the Joint All-Domain Battlespace. Moreover, the Alliance can explore new options for defending the systems and networks it relies on for command and control with deep learning algorithms. The Conference Panel focused on Battlespace Management will explore these technological horizons, and more.

Our final Conference Panel will look at Future Developments, those technologies which might have an impact to military operations not in the next few years, in but 5 – 10 years and beyond. What will the future hold, professionally and operationally, when the military sees a significantly increased number of systems operated remotely? Moreover, what will be the impact on military operations once 5G infrastructures are firmly rooted across the nations and continents? Identifying these nascent technological developments and forecasting their arrivals can help inform key NATO Defence Planning Process elements including the Strategic Foresight Analysis and NATO Warfighting Capstone Concept. These in turn will guide the development of capability requirements and force structure targets to ensure the Alliance is prepared to receive and implement new technologies and to continue to accomplish its three Core Tasks in the decades to come.

The themes covered in these essays are certainly not all-inclusive, but they represent the most inclusive and comprehensive JAPCC Conference Read Ahead ever published. The collected essays are from military and civilian service members, academic and civilian think thanks, and our industry partners from around the globe. I invite you to visit our conference website to further explore details regarding the panels, the topics and themes and the registration for this year's conference: https://www.japcc.org/conference/

In closing, I hope you will enjoy the reading and that this has piqued your interest to do so. We hope that through exposing a cross-section of ideas and opinions we will spark a debate that ultimately will help to shape the future of NATO Air and Space Power. There is much work to be done to ensure NATO can leverage the myriad emerging technologies to conduct Air and Space Operations more capably. Your thoughts, insights and perspectives on these topics will be a welcome and important part of our discussion.

I sincerely hope to see you this fall in Essen!

Klaus Habersetzer
Lieutenant General, DEU AF
Executive Director, JAPCC

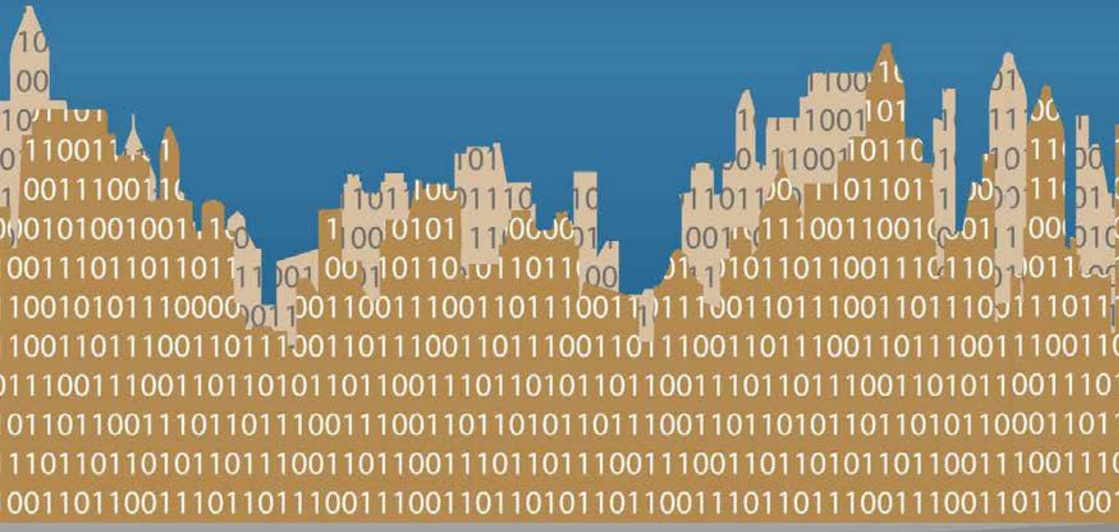
Conference Itinerary

as of June 2020

8 December 2020
Icebreaker and Industry Showcase

9 December 2020
Inaugural Session with JAPCC Director's Opening Address
Keynote Speech
Panel 1: Space
Director's Luncheon and Lunch Buffet
Panel 2: Competing in the Information Environment
Director and VIP Tour of Industry Showcases
Networking Dinner and Industry Showcase

10 December 2020
Keynote Speech
Panel 3: Battlespace Management
Lunch Buffet
Panel 4: Future Developments
Wrap-up and Director's Closing Remarks



Joint Air Power Competence Centre
von-Seydlitz-Kaserne | Römerstraße 140 | 47546 Kalkar (Germany)

Visit us in the web:

www.japcc.org