Transforming Joint Air and Space Power

The Journal of the JAPCC

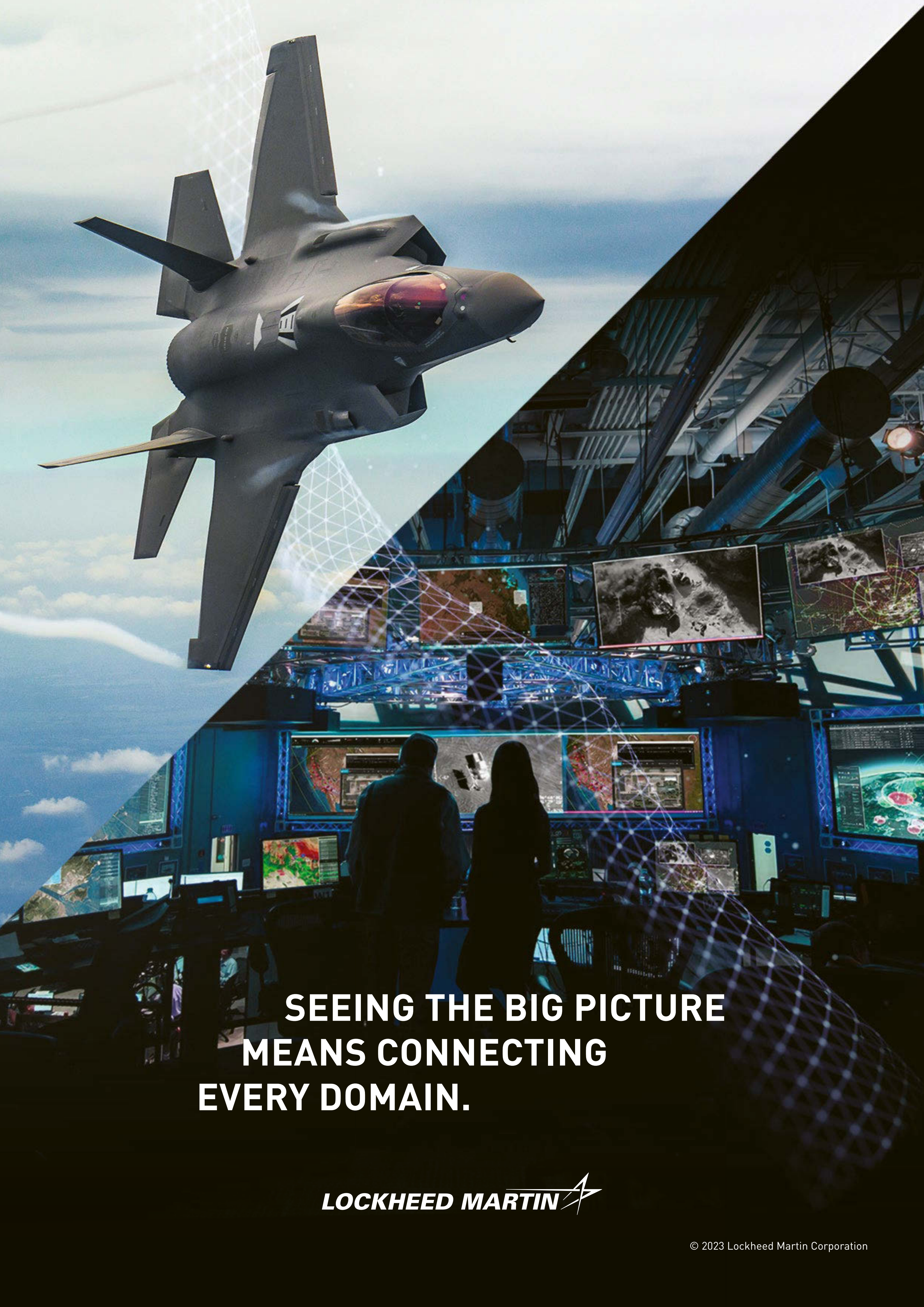
SPECIAL

Air Power in the Russian-Ukrainian War: Myths and Lessons Learned

View from the Command Post

PAGE 14

Edition 35, Winter 2022/2023


SEEING THE BIG PICTURE
MEANS CONNECTING
EVERY DOMAIN.
LOCKHEED MARTIN

Editorial

The quest for peace in Eastern Europe is still in progress. Through resourcefulness and grit, the Ukraine Armed Forces have fought Russia to a standstill and earned the admiration and support of the Western world. Meanwhile, Russia's brazen attempt to assert its influence and reshape the world has become the object of worldwide opprobrium. In combination, they are a validation of our resilient Alliance based on defensive strength.

We, the JAPCC, continue to aspire to translate the most current challenges into workable solutions and inspire ideas to further transform Air and Space Power. Thus, to make our community of Air and Space Power enthusiasts significantly more knowledgeable, versed, and informed we bring to you the 35th edition of the JAPCC Journal. Once again, the offered compendium of select articles aims to pique your interest and increase awareness of some of the latest developments and topics within the Air and Space domains.

This edition opens with Major General Dupont, Commander of the Belgian Air Force, who outlines the current state, challenges, and future projects enabling the necessary giant leap for a next-generation Air Force, while celebrating its 75th anniversary.

Directly from the battlefield, at a time of such great struggle, the leadership of the Ukrainian Air Force judiciously debunks a series of myths related to the ongoing conflict, while adroitly indicating the way to success.

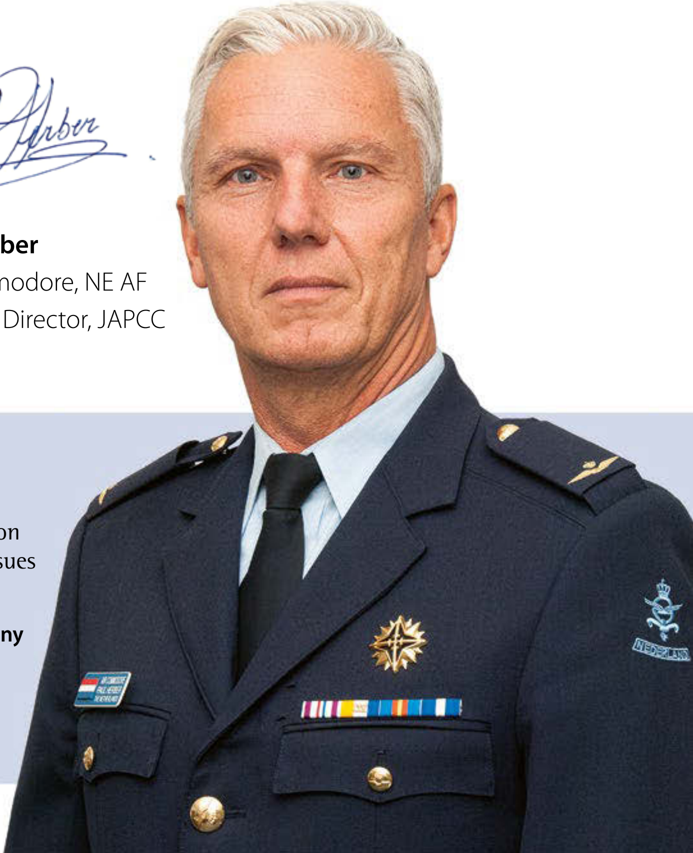
The next series of topics introduces one of the success stories of multinational cooperation within NATO, provides insights into the challenges and available tools to prepare our air and missile defence specialists and forces to NATO standards, and advances quantum technology awareness with its potential applications in the Air and Space domains.

The next three articles examine different aspects of the war in Ukraine, including well-argued insights on the perceived underperformance of the Russian Air Force, how commercial space providers can be a game changer in modern conflict, and finally observations and lessons learned from the Ukrainian cyber battlefield. Next, we take a look at the somewhat arcane field of cultural property protection, which considers the negative strategic effects of ill-advised tactical action and the strategic advantage of protecting cultural property whenever possible. The journal concludes with a summary of the robust discussions and salient points exchanged and debated during the 2022 JAPCC Air and Space Power Conference, themed 'Enhancing NATO Air and Space Power in an Age of Global Competition'.

Thank you for taking the time to read this edition of our Journal. I am confident that many of the articles will pique your interest. I am particularly appreciative of, and would like to express my sincere gratitude to, all our contributing authors. I hope you will find it informative and stimulating, and we greatly appreciate any feedback you may have. Reach out and visit our website at www.japcc.org, like us on LinkedIn or Twitter, or email us at contact@japcc.org.

Herber

Paul Herber
Air Commodore, NE AF
Assistant Director, JAPCC



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

We encourage comments on the articles in order to promote discussion concerning Air and Space Power. Current and past JAPCC Journal issues can be downloaded from www.japcc.org/journals

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

Follow us on Social Media

Table of Contents

Leadership Perspective

Transformation & Capabilities

Viewpoints

Out of the Box

Copyrights

Front Cover: 🄼 A330: © Airbus; Sky: © prasongtakham – stock.adobe.com; Sunrays: © Thaut Images – stock.adobe.com; Network Structure: © Olena – stock.adobe.com
Ad 6: 🄼 © Ted Carlson; *Ad 14:* © Ukrainian Air Force; *Ad 32:* 🄼 © MCD, Hille Hillinga; *Ad 67:* 🄼 © Lena Ha/ Shutterstock.com; *Ad 75:* © JAPCC

Inside the JAPCC

Book Reviews

Imprint:

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

Director
Gen James B. Hecker

Executive Director
Lt Gen Thorsten Poschwatta

Assistant Director
Air Cdre Paul Herber

Editor
Col Matthew E. Hanson

Assistant Editor
Lt Col Ciprian Teletin

Production and Advertising Manager
Mr Simon J. Ingram

Editorial Review Team
Col Maurizio De Angelis,
Col Tyler Niebuhr, Mr Adam T. Jux

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

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

🄼 **Denotes images digitally manipulated**

F-35A PROGRAM TEAM
BELGIAN AIR FORCE
75
EST. 1946
ACC
T. DUPONT

© Belgian Air Force, Michael Moors

Shaping Tomorrow’s Air Force

Many Challenges and Even More Opportunities!

By Major General Thierry Dupont, Commander, Belgian Air Force

An Unprecedented Reality

The geopolitical landscape is unprecedented and scattered more than ever. Facing emerging powers possessing state-of-the-art technologies becomes a day-to-day reality. Threats to our safety and global security evolve continuously. Crude actions and the aggressive rhetoric of external actors and peer competitors pushed us into an unprecedented crisis. Therefore, our Air Force must be capable of meeting the numerous challenges that arise as a result. The endless pursuit of technological lead is not a luxury but a must. Seventy-six years of peace in Europe, something many of us took for granted, was abruptly ended by the Russian aggression against Ukraine. A wake-up call for many of our national and European leaders to invest in and support the collective defence structure. Recent developments in the geopolitical arena not only stress the need for but also accelerate the transformation of our armed forces by identifying shortfalls in technological capabilities and advanced military capacities. Technological progress is a prerequisite to the success of an operation. There is a need to pursue strong cohesion based on solid friendship and mutual trust. Transforming an organization carries more than one challenge and offers many opportunities; it is the art of adapting seamlessly to each fight and future threat at the speed of relevance.

Last year, our Air Force celebrated its 75th anniversary; we look back to a rich history spanning three-quarters of a century. The Belgian air combat capability, supported by our efficient transport fleet, has unceasingly been put at service throughout the last 25 years to safeguard and secure our Alliance and partner nations. Belgian aircraft were involved in homeland operations and abroad over the Balkans, the Baltic States, and the Middle East providing support over Afghanistan, Iraq, Syria, and Libya. By doing so, many of our personnel have been exposed to challenging tactical situations and gained valuable experience. These highly experienced airmen, always ready to deploy with unwavering dedication, are shaping our organization to lead the way to a next-generation Air Force: a genuine revolution encompassing new training, operational concepts, and cutting-edge weapon systems. Transformation and consolidation are necessary to ensure our Air Force is constantly prepared to act under any circumstance on national soil or abroad, and to position our country in a credible way towards our international partners and allies within the framework of established cooperation initiatives.

Navigating Through Many Challenges

Our newly adopted strategic vision, STAR, comprises four pillars: Security & Service, Technology, Ambition, and Resilience. The 2030 goals of the STAR plan are aligned with the parallel processes of the newest European Strategic Compass and the NATO Strategic Concept. This vision focuses on three main areas: personnel, strengthening the industrial and technological backbone, and increasing equipment investments. We position ourselves at the heart of European defence and the European pillar of NATO. Synergies and strengthened international collaborations make it possible to strive for greater efficiency. In the years to come, an additional ten billion euros will be invested in the Belgian armed forces to acquire more sophisticated weapon systems and to build modern maintenance and operational infrastructure. The first Belgian F-35A Lightning II will be delivered in 2023 and we expect to achieve limited operational capability by 2025.

Meanwhile, we will maintain a fully operational combat capability with our current F-16 fleet. Many hurdles will have to be cleared in the coming years; a true challenge, especially for a medium-sized Air Force. In addition to the Airbus A400M, the MQ9B SkyGuardian, and the F-35A, the Belgian Air Force plans to acquire a new fleet of Light Utility, Search and Rescue, and medium to heavy transport helicopters, special operations aircraft, and light tactical transport aircraft. New training concepts will be rolled out for our pilots as well as our maintenance personnel, combining live and synthetic training in Belgium and abroad. We will also significantly increase our participation in the Multinational Multirole Tanker Transport Unit (MMU) and acquire short- and long-range Air and Missile Defence systems for homeland defence and deployed operations. Besides introducing new capabilities and training concepts, we attach great importance to the rapid and innovative development of existing capabilities, resulting in many initiatives and international cooperation possibilities.

Military personnel were often the variable during budget cuts throughout the last decade. However, it is the only genuine engine of our Air Force. Increasing recruitment and adopting new training concepts are required to operate 5th-generation military assets effectively in future highly contested environments. We must be able to operate safely and tactically sound whilst ensuring security and military resilience. A major recruitment plan, *People Our Priority,* was activated a little over a year ago. The first positive signs of these increased recruitment efforts are noticed already at our units. Young, motivated, and well-trained personnel

© Belgian Air Force, Robin Mues

The first Belgian F-35A Lightning II will be delivered in December 2023 with an expected operational capability by 2026.

are indispensable for an organization in full transformation. Ensuring that human resources are not a limiting factor for the transformation towards the Air Force of the future is a true challenge. The quantity and quality of personnel have an immediate and significant impact on the introduction of new weapon systems. Attracting new specialized and skilled personnel and retaining experienced personnel by creating proper incentives and motivational mechanisms is more important than ever. Personnel maintaining and operating 5th-generation weapon systems need to be all-rounders. It is a long-term investment and thus worth the effort. By doing so, I am convinced we will succeed in implementing new high-tech capabilities.

Change management is an often underestimated aspect during an organization's transformation. Yet it is important. A successful transition to the future Belgian Air Force requires keeping our entire workforce aboard. From a leadership point of view, all members must be given the appropriate decision-making authority proportional to their assigned tasks. Empowerment is not only motivating but also a key element for a resilient and adaptive organization in a volatile environment. This concept of leadership and orientation implies the need for a responsive and inclusive command structure. Certain levels of command will be implemented differently in the future, whether it be from an operational or maintenance point of view. A bottom-up approach creates a resilient and healthy organizational culture. This is vital in the long run, especially for an organization relying heavily on its human capital. Finding the right balance between steering and empowerment whilst optimizing the potential of our personnel is the way to go. Yet another challenge and an opportunity to seize!

The Defence and Industry Research Strategy (DIRS) assists the Belgian industry's research and development of new capabilities within a European context. A solid industrial base strengthens European strategic autonomy and allows extensive large-scale cooperation to overcome military shortfalls. Major current and future investments in state-of-the-art equipment will enable our Air Force to protect vital interests and to show resolve to our Alliance. The future Belgian Air Force will remain a reliable international partner whilst being able to project strategic vectors in complex non-permissive theatres anytime, anywhere on the globe.

A few years ago, we initiated the transformation of our Air Force. The first signs became visible in 2019, when the Belgian military Air Traffic Control Centre moved to its new location to develop in-depth synergies with

Skeyes, the civilian ATC provider, leading to efficient use of Air Traffic Control services. The Belgian Airspace Vision 2030, a civil-military initiative, introduces the Flexible Use of Airspace (FUA) concept and prepares the airspace integration of 5th-generation platforms. The result should be an optimal use of airspace for military and civilian users. In 2020, the Belgian Control and Reporting Centre took possession of its new infrastructure and will remain at the heart of NATO's Air Defence capability. The first A400M strategic and tactical transport aircraft joined our Air Force two years ago. The transition towards a performant high-tech transport capability and commissioning a new state-of-the-art maintenance complex have been great successes. It almost doubled the transport capacity compared to its predecessor, the C-130 Hercules, and was put into service during the non-combatant evacuation operation in Afghanistan, Red Kite 2021, only a few months after the first aircraft arrival.

With the introduction of the MQ-9B SkyGuardian and the F-35A Lightning II in less than two years, our Air Force will acquire a strategic Remotely Piloted Aircraft (RPA) and 5th-generation combat capability. These assets are real game changers that require a new mindset to empower and adopt new operational concepts. As many air forces introduce the same, a strong group of users arises. However, we must not be blindsided by the fact that this metamorphosis extends far beyond the material level. Introducing and developing game-changing capabilities is far more than acquiring a new platform; it requires a solid and sustainable infrastructure that meets today's fast-evolving standards. Large construction works are initiated at our airbases. Owing to thorough coordination, we can minimize the impact of these construction works on our operational output. Combining many construction sites with the requirement to meet a preset ambition level is a daily challenge. For instance, the multifunctional F-35 complex at Florennes Airbase needs to be operational by mid-2024 to be ready to receive the first F-35A in 2025. Additionally, these platforms introduce a series of new and noteworthy security challenges with profound influences on infrastructure specifications and design requirements. Fifth-generation security standards require more force protection personnel; yet another recruitment challenge.

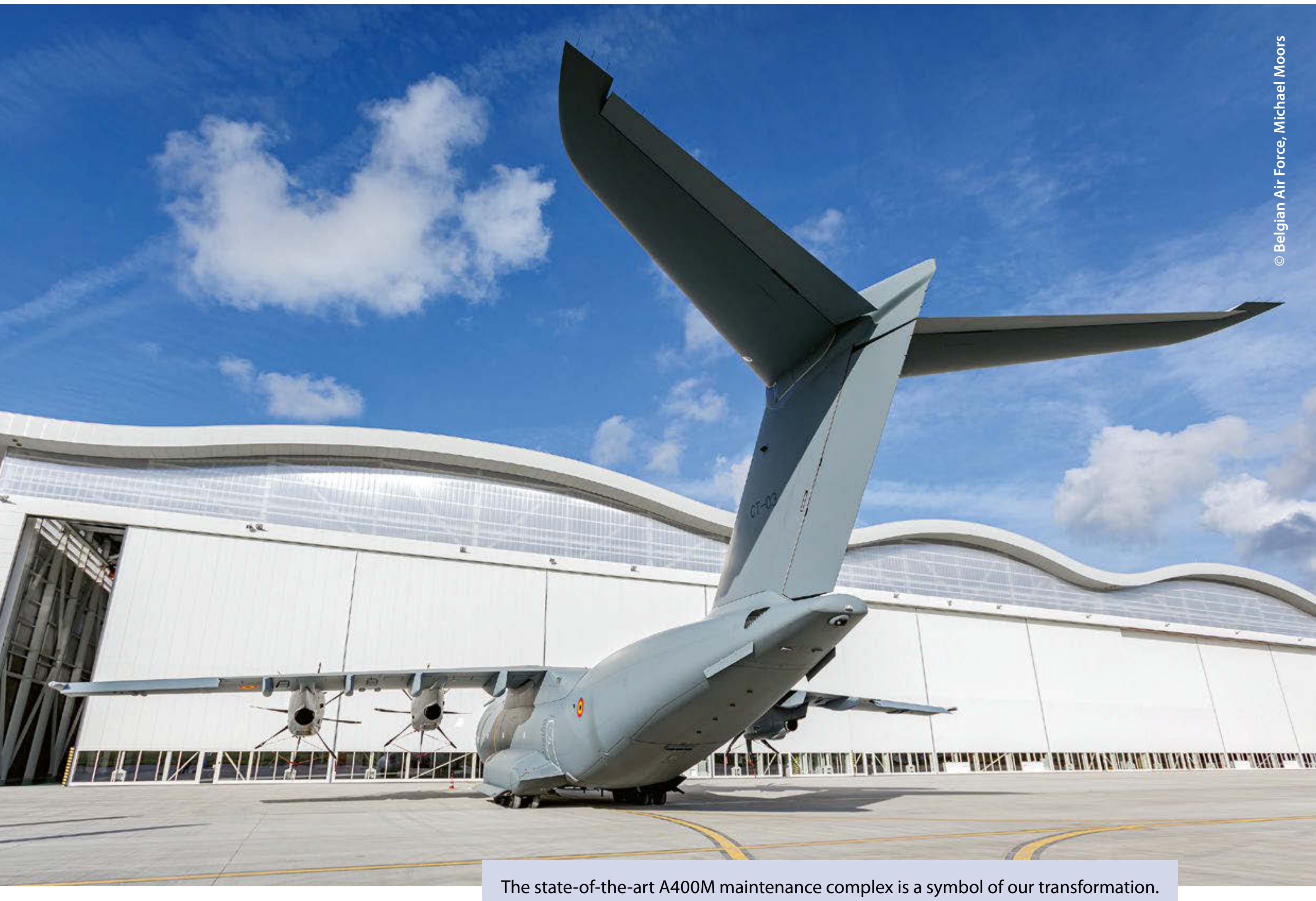
A Giant Capability Leap

The F-35A advanced avionics sensor suite, high-performance self-defence system, and low observability allow it to gain access to highly defended Anti-Access/Area Denial (A2/AD) zones. In a nutshell, great potential! The future Belgian Air Force gains unprecedented operational capabilities and partner integration possibilities, readying itself for the conflicts of tomorrow. Introducing 5th-generation capabilities is a giant technological leap that requires a revised training concept combining live and synthetic training to prepare our pilots, support staff, and technicians. This aircraft far exceeds the capabilities of a 4th-generation multi-role weapon system. Equipped with a myriad of sensors, acting as a node in a hyper-connected network and fitted with state-of-the-art weaponry, the F-35 enables us to act against the most sophisticated adversaries whilst serving as a Battle Manager. Moreover, the groundbreaking capabilities of the F-35 will enable us to generate synchronized effects within the Multi-Domain Operations concept.

Data processing becomes increasingly important while the boundaries between the operational domains (Air, Land, Maritime, Space, Cyber) are blurring. Intelligence is essential to deploy available resources appropriately and efficiently. Analysis and intelligence collection capabilities, both human and technical (imagery, artificial intelligence, exploitation and storage of big data), are needed to allow tactically sound as well as timely strategic coalition decision-making. Data collected by our future F-35s will complement and merge with that of our allies, effectively contributing to optimal data processing and analysis.

The Medium Altitude Long Endurance Remotely Piloted Aircraft System (MALE RPAS) will be able to take off from a permissive area, proceed to the area of interest, and provide valuable continuous battlefield ISR coverage. Introducing the MQ-9B SkyGuardian in the Belgian Air Force provides a historical strategic dimension and a high-performance intelligence capability. Given the multi-mode communications suite, wide-range sensors, and significant loiter time, it provides a unique capability to perform strike coordination and reconnaissance against high-value, fleeing, and time-sensitive targets. Remote Split Operations (RSO) simplify command and control functions as well as the logistical supply needs for the weapons system. It allows the safe projection of a capable ISR asset, even before the start of a conflict, without exposing personnel or equipment unnecessarily to any threat.

A new milestone for building our imagery intelligence Processing, Exploitation, and Dissemination (PED) capability is the recent inauguration of the Belgian Imagery PED Centre at Florennes Airbase as a centre of excellence responsible for aerial footage analysis. Interconnecting coalition intelligence assets and merging and sharing ISR products amongst partners and allies herald a new era of coalition operations. Information management requires persistent development and continued investment in personnel and communications systems. These two aspects are the cornerstone of any next-generation system, be it the MALE or the F-35. It includes connectivity to satellite providers and an information network inherently used by any modern intelligence architecture to store and – above all – analyse collected raw data, as well as disseminate the generated intelligence products near real time. The communication infrastructure for these new capabilities will not only have to be efficient, resilient, modular, and secure but also integrate seamlessly with those of our partners. Understandably, there are challenges to overcome in sharing accurate battlefield situational awareness amongst allies, yet this unique PED capability provides new opportunities.


© Belgian Air Force, Michael Moors

The state-of-the-art A400M maintenance complex is a symbol of our transformation.

© Ted Carlson

Fostering Coalition Effectiveness and Enhancing Interoperability

Ensuring our armed forces are interconnected and interoperable within a broad spectrum of possible conflicts should be at the top of our priority list. Combined planning and synchronized mission execution in a Multi-Domain Operations environment can only be successful with interwoven systems and connected capabilities. Such in-depth international integration at the high end of warfighting requires, above all, a mindset change. To overcome future conflicts we need the capability to easily manoeuvre across all domains, in a synchronized manner, at a speed and efficiency that the opponent cannot match. Our coordinated coalition actions will only then be effective. Information and communication technologies need to be linked through battle networks. Efficient information sharing concerning the activities and resources of a potential adversary strengthens military partnerships. The Alliance's seamless integration, reliant on 4th and 5th generation assets and an efficient combat cloud, provides a huge information advantage.

We must ensure the continuity of operations by strengthening the collective resilience of our critical military infrastructure. More emphasis must be placed on maintaining robustness and resilience in a constantly evolving environment when operating complex fifth-generation systems. Decentralized allied infrastructure and operating from dispersed locations are beneficial to military resilience.

With these considerations in mind, we are obliged to innovate and adapt so that our strategic and tactical warfighting assets integrate seamlessly and effectively in a joint and combined environment. We have to foster coalition effectiveness by integrating new high-end assets, pursuing interoperability, and effectively becoming a node in the coalition's information network, especially in support of operations.

The Importance of Cyberspace

Our society and economy are increasingly digitalized and interconnected and, thus, need to rely on the availability and integrity of digital information, IT systems, and the underlying infrastructure. Technological developments have increased the importance of information and data in our security environment. Fifth-generation weapon systems are, amongst others, heavily dependent on the proper functioning of their networks and possess a digital element that connects them to cyberspace. At the same time, numerous easily accessible and highly sophisticated cyber tools allow our adversaries to directly or indirectly compromise these critical military weapon systems. Targeted cyberattacks come in increasingly diverse forms and can severely cripple our society.

Protecting military information while ensuring the reliability, integrity, and availability of communications, information, and weapon systems are the core tasks of the military cyber capability. Situational understanding in cyberspace is paramount and should be integrated into a common operational picture. To this aim, our armed forces inaugurated the Belgian Defence Cyber Command in October 2022, which is essential to NATO's collective defence, and will consist of four main pillars (security, defensive, intelligence, and offensive). Once again, a large number of highly skilled technicians, analysts, and specialists should be recruited and trained in the cyberspace domain to achieve full operational capability.

Moreover, exclusive partnerships between the Belgian armed forces and high-tech civilian companies exist in order to develop cybersecurity skills and capabilities within the Belgian government and related industry. A transformation plan was developed to evolve from a security operations centre to a security intelligence centre. The build-up of cyber expertise will not be limited to defence and may be of interest to many other sectors facing the growing cybersecurity challenges.

A Bright Future Ahead

The Belgian Air Force is, in essence, based on four pillars that make up its identity: dedicated personnel, new weapon systems, adapted infrastructure, and concepts & procedures. These backbones require an adaptable mindset and reliable connectivity. Undoubtedly, we are steadily evolving towards an Air Force equipped and prepared for the future, ready to adopt and implement new maintenance and operations concepts. Our coalition mindset will also be reflected in future acquisitions and by continuing to build a strong and resilient Air Force able to easily adapt and overcome the rapidly changing threats of tomorrow. Still, many challenges will arise; efficiently allocating our resources is essential to build a resilient structure.

Today, we stand on the verge of a new era for our Air Force. It is a giant leap in terms of capabilities and the possibilities they generate. Our Air Force will be modernized to 5th-generation standards in a few years. Ready for the new normal, offering high-tech combat, transport, helicopter, and RPA fleets to the next-generation airmen, thus enabling them to achieve our ultimate goal, 'projecting Air Power anytime, anywhere on the globe'. We are experiencing historical times and – admittedly – that makes it all quite exciting! ●

Major General Thierry Dupont

graduated from the Polytechnic Department of the Royal Military Academy in 1989. After completing his pilot training, he was assigned to the Mirage 5. In 1995, he completed an F-16 conversion and joined the 2nd Tactical Wing. Four years later, he attended the test pilot training course at the French Test Pilot School in Istres. In January 2002, he was assigned as the Commanding Officer of the No. 1 Squadron in Florennes, transitioning to F-16 MLU under his command. In 2004, he attended the Superior Command and Staff Course at the 'Collège de Défense' in Toronto (CA) and obtained a parallel master's degree in defence policy at the University of Montréal. From 2005, he ensured capability relations with NATO and with the European Defence Agency as a staff member in the Strategy Department of the Defence Headquarters. In 2013, he became the 24th Commander of the 2nd Tactical Wing. Under his command, the unit takes part in multiple missions. In July 2016, he became the first Belgian Head of the Combined Air Operations Centre in Uedem (GE), being responsible for the integrated Air and Missile Defence System of Northern Europe and for the support of Operations led by the 'Joint Forces Air Command' in Ramstein. In May 2018, he became the Deputy Chief of Staff for Operations and Training of the Belgian Defence.

On 17 September 2020, Major General Dupont became the 5th Air Component Commander and the 16th Belgian Air Chief.

He totals over 2,600 flying hours on thirty different types of aircraft.

Air Power in the Russian-Ukrainian War: Myths and Lessons Learned

View from the Command Post

By Lieutenant General Mykola Oleshchuk, UKR Air Force, Commander
By Lieutenant General Viacheslav Shamko, UKR Air Force, Chief of Staff – Deputy Commander
By Colonel Artem Antonov, UKR Air Force, Chief of Military R&D Section

Editor's note: The JAPCC is presenting this article as a personal account from the Ukraine Air Chief and staff in their own words to further the public discourse on the war in Ukraine. The views expressed are those of the authors concerned, without endorsement by the JAPCC or NATO.

We are truly grateful for their insights and first-hand experiences. Please refer to our Disclaimer/ToRs in the imprint.

'Outnumbered and outgunned,
we continue to fly, fight, and win.'
Ghosts of Ukraine

In the winter of 2021–2022, the entire world became an unwilling participant while Ukraine became the hostage of Putin's geopolitical talk show. 'Kremlin's elders' poured out threats and ultimatums unseen since past world wars. Ukraine and the West had been rejecting Moscow's demands for a new division of the world as unthinkable in the 21st century. However, being confident that a great war in Europe would 'never again' repeat and Moscow's threats were blatant blackmail, the European capitals responded rather weakly and indecisively, suffering from the energy and COVID crises and other internal issues.

© Ukrainian Air Force

Consequently, the diplomatic meetings at the highest levels turned out to be barren. On the one hand, this response irritated the Kremlin but, on the other, it persuaded Putin that the West was weak and separated, and that its values and morality were emasculated. While the American partners warned about the inevitability of war, various experts predicted the Ukrainian nation would last only a week before its collapse under the hits of 'the second army in the world'. Being in the whirlpool of the events, Ukraine was hoping for peace whilst preparing for defence.

We were mostly all wrong. The war has indeed begun. It began unexpectedly despite all the warnings and preparations. Even at the Air Force Command Post, at the dawn of 24 February 2022, while watching the take-off and approach of the enemy's air armada and believing that our mission is to preserve peace rather than unleash a war, we hoped that it was just another demonstrative provocation. Putin's hordes did not turn back. However, to Putin's surprise, we met them with stabbing deadly fire, not bread and salt. The war turned out to be full of unexpected events and unanswered questions. Why did Putin dare to invade? What is the role of the West in this war? Why could not 'the second army in the world' break the opponent's resistance with substantially fewer resources, manpower, and means for armed resistance? Why was the Russian Air Force – ten times larger than its Ukrainian counterpart – incapable of gaining air superiority, in fact being neutralized? Could the wide employment of layered Anti-Access/Area Denial (A2/AD) systems fracture the concept of Air Power, marking its decline and the revitalization of Land Power in the modern conflict? Can one successfully wage war without air offensive capability against an adversary who possesses it? Does Ukraine need modern combat aviation and air defence systems if the Russian Air Force can no longer exploit its offensive potential? These questions have been actively discussed in the expert community in Ukraine and abroad. Sometimes the discussions are professional, and sometimes they are superficial. Consequently, together with the lessons learned from this war, we are now faced with a multitude of myths about the local character of this war, the 'paper tiger' and 'hollow force' of the Russian army, about the wonder weapons, unnecessary for the offensive capabilities of Ukraine if the ability to win this war is through a strategy of attrition.

Having no goal to introduce an absolute truth, in this article we aim to analyse and refute the main myths around this war. We hope that this paper will be a useful contribution to the discussion that will help to find the answers to the above questions.

Myth 1. *This is a war between Russia and Ukraine, in which the West should not interfere. Russia started this war to ensure its own security within the area of its own historical interests as a response to another attempt at NATO enlargement.*

Regardless of how it has been perceived elsewhere, from the Kremlin's perspective, Russia has been waging war against the West. For Moscow, Ukraine, to which Putin denies subjectivity and the right to make its own choice, is only a battleground. At the same time, the main enemy is the collective West, specifically western liberalism, which had destroyed the Russian empire twice within the last century. Considering it the main threat for Russian statehood and trying to protect the renewed empire from the next 'greatest geopolitical catastrophe of the century',

© Ukrainian Air Force

© Ukrainian Air Force

Launch of Ukraine SA-10 systems during live fire exercises.

Putin is attempting to destroy the rule-based world order and build a multipolar one on its ruins, where liberalism would not be a threat for his regime and empire anymore. In Putin's strategy, NATO and Ukraine have become the centres of gravity.

Despite Kremlin's rhetoric, Moscow perceives NATO not as a military threat but ideological. It is not the Alliance's missiles and tanks that Putin fears but the ideas of freedom, democracy, free market, and human rights that tie the Alliance's nations together. It is not the mythical NATO military bases in Ukraine that scare the Kremlin (Russia borders five NATO countries, some of which are far closer to Moscow), but the very thought that a culturally and historically close nation would reject the ideas of the totalitarian 'Russkiy Mir' (i.e. Russian World), join the family of free democratic nations, and thus provide an example for the people of Russia. That is why Putin attacks.

Using artillery shells and missiles, he destroys our cities, economy, and civil infrastructure, effectively trying to destroy the Ukrainian identity, culture, and nation. However, he also attacks the West, its unity, democratic institutions, principles and values, economy, energy sector, and welfare – everything that makes the West as it is. And though the citizens of Warsaw, Budapest, or Berlin do not yet hear the air raid alarms, Putin has already deprived them of the choice of 'war or peace'. The only choice left is what to sacrifice. It is either today's well-being, by helping Ukraine right now, or tomorrow's values and way of life, when the Ukrainian fortress will fall under the blows of the eastern hordes. Free nations should answer this question on their own, while we can only state that there is not much time left for doubts and speculations. The Ukrainian nation is bleeding the blood of its children and our resources are running out.

***Myth 2.** The level of the Russian threat to the West is exaggerated. Russia is only another rogue nation with minor influence on world politics and economy. The West is overreacting.*

Many Western nations still largely underestimate and underreact to the Russian threat. Indeed, Russia is no longer a leading economic and political power in the world. However, Russia's challenges to the world order and economy significantly exceed Russian real input.

Firstly, as previously stated, Putin wages this war for ideological reasons. This is the war of autocracy against democracy, tyranny against liberalism. Just as Saddam Hussein attacked Israel during Operation Desert Storm, attempting to ruin the anti-Iraqi coalition and entice Arab nations, Putin attacked the West while trying to unite the rogue nations around himself in his anti-liberal 'crusade'. Putin is not the only adversary in this battle of world views – he already has his own 'coalition'. The Belarusian dictator Lukashenko stands hand in hand with him, fully supporting the war against Ukraine and threatening Eastern Europe. He granted Russian military forces access to Belarusian military bases, airfields, and logistic centres, thus facilitating the attack against Ukraine from the north. International law clearly states such actions constitute direct participation in war. Even though the Belarusian army does not have the courage yet to directly partake in combat, Lukashenko still threatens Ukraine from the north, manoeuvring his army while missile attacks from Belarus on Ukrainian cities are ongoing. Moreover, alongside Lukashenko are the puppet regimes of Southern Ossetia and Abkhazia. Also, we already have information that Iran and North Korea provide weapons and ammunition to Russia. Although China is still in doubt about whether to finally take the way of belligerent autocracy or preserve its midway course, Putin actively engages president Xi trying to convince him that it is time. To summarize, tyrants and dictators of the world are watching how Putin brutally ruins the established world order and guessing whether their time has come.

Secondly, though Putin rejects liberalism, he does not hesitate to exploit its institutions against the West itself in his crusade. By active intervention in the political processes of the western countries, supporting marginal political powers, and conducting anti-democratic propaganda, Putin uses democratic institutions to undermine western nations from the inside. The same approach takes place in the United Nations Security Council and other international organizations where Russia paralysed their work and used them not to preserve the values and freedom they were created to protect, but to contend with them.

© Ukrainian Air Force

Thirdly, even though the population of Russia does not exceed 2 % of the world population and its contribution to the world economy is less than 3 %, by controlling access to the nearly unlimited resources of the Eurasian heartland, Putin has turned raw materials into weapons. Putin's 'Russkiy Mir' is incapable of ensuring development, welfare, and fair economic competition. His tools are blackmail and crises. Hoping to crush the will of Ukrainian and western nations to resist, the Kremlin has deliberately created the world energy and food crises and openly threatens to freeze Europe in winter. That is why the West should re-evaluate the Russian threat, keeping in mind that Putin is not the only one in his crusade and noting that while the 'the pain threshold' of Moscow is substantially low, Putin is still determined to achieve his goals by exploiting Russian strengths and Western weaknesses.

Myth 3. The Russian people are not accountable for the regime's crimes and should not suffer from its consequences and sanctions; only Putin and his inner circle should.

Innocents should not suffer. However, a major portion of the Russian population is complicit with the crimes against Ukraine and, eventually, must share the responsibility with the ruling regime. Though some experts might think that Putin started this war contrary to the will of his people, it is not the correct statement. As Stalin said while interviewed by Herbert Wells: 'Even talented ruling minority is helpless unless it stands on at least the passive support of the millions of people.' It is not Putin who directs missiles at our cities, pours a rain of artillery shells and bombs on our land, rapes our women, and kills our innocent children. It is being done by thousands of scoundrels and criminals in Russian military uniforms. But what shocks us more is the level of enmity and hatred for Ukraine and the West, as well as Russian society's fanatical

© Ukrainian Air Force

support for Putin's policy and the Russian army. Indeed, we do see silent protests of thousands of Russians who disagree on the streets of Moscow, St. Petersburg, and Novosibirsk. But, at the same time, millions of Russians silently (or frequently openly) support this war. Silence will not end violence – it only feeds it. Silence is a consent and continuation of the social contract between Putin's regime and the people, which is complicity in crime. Only the voice of disagreement on the streets of Russian cities can break the bond and, for this, the people of Russia should feel the consequences and the price of their crimes. And possibly, if the voice is loud enough, they will get the chance to rethink their destiny, which they lost when they handed power to Putin.

***Myth 4.** The imbalance in military and economic potentials is too big. Ukraine is incapable of gaining military victory in this war. A compromise should be reached at the negotiation table.*

Any war ends at the negotiation table, but the way to it is through victories on the battlefield. Ukraine is not only capable but also has to gain these victories. If only math equations determined the outcome of wars, wars would lose any sense. 'Mathematical' calculations showed that Kyiv and all of Ukraine would capitulate during the first week of the war. But the Ukrainian fortress has withstood the siege for almost a year and continues to grind Putin's hordes in battle because the equation of war holds not only deterministic elements but also chance, fortune, and the will of the nation to resist. So far, fortune is on our side, and Ukrainian will and confidence in our victory offset the quantitative advantages of the aggressor. Today the war has reached its equilibrium, but the support from the West should break this balance for the benefit of Ukraine.

***Myth 5.** Kremlin has already realized its failures and is ready for negotiations. The 'gestures of good will' are the invitation to agreement and peace.*

The Kremlin's gestures of 'goodwill' are nothing but an effort to politically soften Russian military defeats. The retreat from Kyiv, abandonment of the Zmiinyi Island, and agreements on the grain corridors are the direct results of the successes of the Ukrainian Armed Forces. We observed the same 'gestures of goodwill' near Kharkov and Kherson. The goodwill of the Ukrainian warriors is to defeat the aggressor and liberate our country. This is the only goodwill that exists here. Only overwhelming force and success on the battlefield can make Putin retreat and consider negotiations

© Ukrainian Air Force

UKR CHOD, Gen. Zaluzhnyi, and UKR Air Chief, Lt Gen Oleshchuk, at a firing range, overseeing AF live fire exercises on the eve of the Russian invasion.

about the terms of the de-occupation of Ukrainian territories and the size of reparations. And these are the only negotiation terms acceptable here because any other 'Minsk compromise' will be used by Kremlin for the preparation of the next war, as we saw it after Khasavyurt or the two Minsk accords. The vital interests of both parties are in danger: the survival of the Ukrainian nation versus the survival of Putin's regime, which Putin himself associates with the state and nation. That is why any long-term compromise is impossible and only serves as a short respite to regain strength. Only victory will end this war, and there should be no doubt that the victory will be ours.

***Myth 6.** The Russian army turned out to be a 'paper tiger'. Ukraine does not need substantial military support to fight against the 'hollow force' of the Russian army.*

Underestimation of the enemy is the first step to military catastrophe; this is the mistake that Russians made during the invasion of Ukraine and which we should not repeat. The miscalculations in strategic assumptions (specifically the expected level of resistance of the Ukrainian Armed Forces and the Ukrainian people) resulted in inadequate strategic planning, inappropriate force composition and orders of battle, and unattainable combat tasks for the troops. Consequently, the most combat-worthy units and formations of the Russian Armed Forces were crushed near Kyiv, Chernihiv, Sumy, and Kharkov, and the Kremlin had to reduce its appetite and focus on the South and East of Ukraine.

Though we witnessed a relative equilibrium on the battlefield when winter came, the Russian army had remained a powerful force with huge weapon resources and manpower. Its troops prevailed in terms of firepower, combat aviation, tanks, artillery, and other systems. Their weapons and military equipment are generally up-to-date and meet world standards.

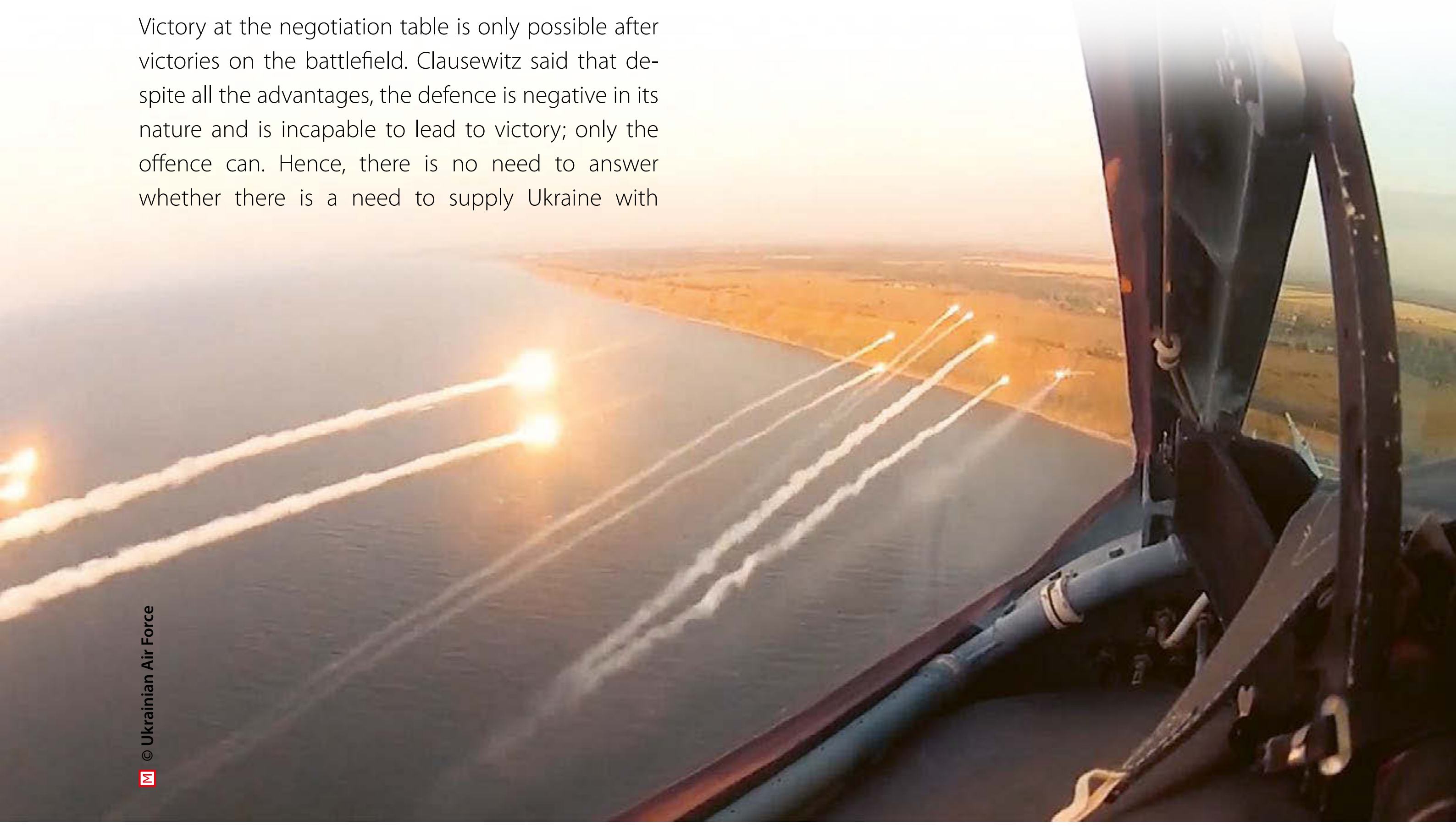
© Ukrainian Air Force

Despite all the losses, Russian Aerospace Forces keep the same groupings along our borders as they had been before the invasion, drawing reserves from Siberia and the Far East to compensate for the losses. Their pilots maintain a high level of training and substantial combat experience. The only change observed after 24 February was a demotivation of the enemy's personnel, which was caused by incompetent leadership and their increased awareness of the absurd nature of this war. Sincerely, not only the will to resist and fight of the Ukrainian people but also the degradation of the military leadership within the Russian army have kept us on the surface during the first weeks of the war and allowed us to reach military parity. However, we need much more to tilt the scales to our benefit in order to knock out the enemy's aviation from our sky and cast out its infantry from our land.

Myth 7. Ukraine does not need offensive weapons, specifically combat aviation, to fight against the aggressor. The only thing needed to survive the war is to strengthen its defence.

Victory at the negotiation table is only possible after victories on the battlefield. Clausewitz said that despite all the advantages, the defence is negative in its nature and is incapable to lead to victory; only the offence can. Hence, there is no need to answer whether there is a need to supply Ukraine with offensive weapons or speculate on the limitation of these supplies. The question that should be answered is the following: What is the aim of the West in supplying any weapons to Ukraine? If the West does it to protect the core values of democracy, liberalism, and the current world order, is it really interested in the victory of Ukraine in its fight against the dark forces of totalitarianism and autocracy? If the answer is 'yes', then Ukraine must receive all weapon systems required for victory in this war, including combat aviation. If the answer is 'no', then the supplies of any weapons have no sense at all.

We are thankful to our partners for their decision to provide up-to-date anti-aircraft missile systems to strengthen our air defence. These systems are already protecting our women and children from Kremlin's missile attacks. However, the best air defence is burning enemy airfields in occupied Crimea, Melitopol, or Chornobaivka and having our aircraft patrolling our skies.



© Ukrainian Air Force

© Ukrainian Air Force

Myth 8. *The Russian-Ukrainian war marks the decline of Air Power as Russia and other opponents heavily invested in and developed a systematic approach to 'fracture' the Air-Land Battle by employing layers of A2/AD systems. The efforts of the Western coalition should primarily be focused on strengthening the Land Power.*

This war has underlined the importance of Air Power in a contemporary conflict as never before. The inability of the Russian Air and Space Forces to utilize its potential, achieve air superiority, and provide support to ground troops has led to a deceleration and subsequently a complete paralysis of the ground offensive. The situation is the opposite for the Ukrainian Air Force as insufficient air capabilities do not allow for conducting deep counteroffensive operations. The parity in the air has contributed to parity on the ground. This war already has the name 'the artillery war', but this is a consequence rather than a conscious choice. A century of technological progress and development of military science was crossed out by one party as a result of the degradation of their military leadership, while by another party as result of the absence of required offensive air capabilities. We find ourselves again at the battle of Somme, digging into the solid Ukrainian land.

The concepts of Air Power, Air-Land Battle, and Multi-Domain Operations are actual as never before. Airspace is an unalienable domain of modern warfare, and the first to gain superiority will get the keys to victory. Though the wide proliferation of A2/AD systems on the battlefield significantly complicates air operations, it does not deny them if adequate planning occurs. Our aviation is purposefully and successfully hunting Russian anti-aircraft systems, and we can assure all that they burn after the HARM strikes, as well as Russian tanks under the hits of Javelins. Unfortunately, our limited resources do not yet allow us to timely and completely use the results of this hunting, build up our efforts, gain the initiative, and ensure the support of our ground troops. We already see how HIMARS systems have changed the character of this war. We can also see how high-precision hits interrupt the logistics routes of the enemy and put its formations in danger. However, though the enemy's logistics are affected, it still works because even a brigade of HIMARS cannot reach the same effect as one aviation squadron by thoroughly isolating a vast area of combat operations. For this, we need up-to-date multi-functional aviation platforms.

Myth 9. *The Ukrainian military is incapable of mastering modern western weapon systems, especially those as complicated as combat aviation, for effective use in the war. The military and technical aid should focus on weapons of Soviet production.*

A small red army will never beat a big red army. Reliance only on the Soviet-production weapons will never allow us to reach a quantitative or qualitative parity with the enemy, saying nothing about gaining an advantage. Our power is in asymmetry, a better level of training, motivation, and the will to fight of our soldiers. Our advantage is also in the quality of our weapons, without which our soldiers are doomed to demonstrate endless heroism. During the first weeks of the war, our pilots – ghosts of Kyiv, Zhitomir, Sumy, Chernihiv, Kharkov, Odessa, Vinnitsa, and from all over Ukraine – entered the air battles flying outdated aircraft against the qualitatively and quantitatively superior enemy, sometimes only three aircraft against eight or five against eighteen. They embraced the fight and heroically gained victories, often with the cost of their lives. However, we would like not to witness this heroism because every case of this type of heroism is the result of hopelessness and despair. As General Patton brilliantly said that 'no bastard ever won a war by dying for his country', we also do not want our pilots, air defenders, and other brothers in arms to die for Ukraine. We do want them to make the scums in the Russian ranks run away from our land, and if they refuse – die for Putin and his absurd ideas. That is why we need up-to-date weapons – the weapons that foster the philosophy of professionalism and the values of human life versus the weapons of Soviet production that profess the philosophy of the mass army of 'workers and peasants'.

We can win only by countering quantity with quality. The arguments regarding the terms for retraining are also senseless. Ukraine is a nation of educated and motivated people. Our warriors have already proven many times that we are strongly motivated to learn fast and use any weapon on the battlefield with unseen efficiency. We were told that our pilots would need no less than six months for retraining. We can assure the experts that they will need not more than three months. But even if it had been six months, and if the decision to provide us multifunctional fighters had been made at the beginning of the war, today they would be in the battle and significantly changing the course of the war. Unfortunately, the delivery procrastination only pushes back the day of our victory and increases its cost. For a year already, our pilots fly outdated aircraft, fight in the minority against the enemy, and, despite all, are able to gain victories. The ghosts of the Ukrainian sky need a chance not only to survive in fights but also to throw away Putin's hordes both from our sky and land.

Conclusion

The Ukrainian nation has been fighting for a year for survival, the right to be free, and the right to choose its future. At the same time, we fight for the values and existence of a democratic world, free from tyranny and autocracy.

This war will determine not only the fate of the Ukrainian nation or the nations of Russia but also the fate of the rule-based world order. The tyrants and autocrats of the whole world are guessing now whether their time has come. The battlefields of Ukraine will show whether Putin will become Fukuyama's 'last man' or the prophet of Huntington's 'clash of civilizations', the person who has ruined the liberal world and caused the decline of the West. The West has already received the declaration of war, and this fact should be admitted as quickly as possible because this war was declared by a daring, insidious, dangerous, and powerful enemy that collects allies under its banners.

'This war has underlined the importance of Air Power in a contemporary conflict as never before. The inability of the Russian Air and Space Forces to utilize its potential, achieve air superiority, and provide support to ground troops has led to a deceleration and subsequently a complete paralysis of the ground offensive.'

Ukraine and the West are still far from the victory and the culmination point in the conflict. Putin's army still preserves its formidable power. Russian economic and military resources are significant, and the Russian besotted society widely supports Kremlin's actions. But we can and have to win. Win by quality over quantity. Despite all efforts, the Russian army still remains a mass army of workers and peasants of the Soviet type. Even its saturation with modern technological platforms did not change its nature. High-technology and costly weapons are thoughtlessly used for terror against the civilian population. Modern high-precision missiles are aimed at apartment houses, shopping malls, civil trains, granaries, public transportation, schools, and hospitals. The enemy has chosen scorched earth tactics, shelling and destroying our cities. The Russian army is a bear that is sick with rabies, a Goliath that lost his eyesight. It ruins everything around in blind rage but is incapable of transforming its power into real achievements on the battlefield. That is why we can and should win.

But the exhaustion strategy is ineffective. The hope that in the war of artillery the rabies will kill the bear before he completely ruins Ukraine is in vain. According to our calculations, Russia can continue this war with the current intensity for at least the next two-three years. Unfortunately, there will be nothing to protect by that time because Ukraine will have turned into ruins. The character of this war should be radically changed. To achieve this, we need to ensure the return of the third dimension onto the battlefield – the power of the Air Force. We need 'the long hand of aviation' for air interdiction, strategic strikes, and support of ground troops. Without this, our ground operations are doomed to stagnation and protracted artillery fights at the defence lines as it was during the First World War. Unfortunately, in this way, we will not be able to gain either advantage or even parity with the enemy because he has overwhelming quantitative prevalence. That is why Ukraine needs an increase in its Air Power, in quantity and, more importantly, in quality.

We do not need parity in numbers, but we do need the advantage in quality. The Ukrainian pilots have already proved their mastery, professionalism, motivation, and ability to carry out extremely hard tasks and achieve success. Russian propaganda announced at least three times the 'complete destruction' of our aviation and air defence. But none of the Russian aircraft dares to fly over the frontline for many months, while the ghosts of Ukraine cause hard losses to the Russian army daily. We have already rejected from our skies the enemy that had almost a ten-fold advantage in quantity and quality. We are waiting for a chance to completely pin him down on the ground and show the way out to his infantry. ●

Lieutenant General
Mykola Oleshchuk

is a graduate of the Zhytomyr Higher School of Air Defence Electronics (1994). He also graduated from the Kharkiv Military University in 2004 (staff college) and the National Defence University of Ukraine (war college) in 2010. Holds a professional bachelor's degree and two master's degrees. Started his career as a crew chief in an AD battery and proceeded to the GBAD brigade commander.
He also served at various staff positions, including the Deputy Chief of Staff of the Air Force Command and the Chief of Staff – Deputy Commander of the Eastern Air Force Command. Since 9 August 2021, he is the appointed Ukrainian Air Force Commander.

Lieutenant General
Viacheslav Shamko

is a graduate of the Dnipropetrovsk Higher Air Defence Command School (1984). He also graduated from the Kharkiv Military University in 1999 (staff college) and the National Defense University of Ukraine in 2005 (war college).
Holds a professional bachelor's degree and two master's degrees.
Started his career as a crew chief in an AD battery and proceeded to the GBAD brigade commander.
He also served at various staff positions, as well as commanded three regional Air Force commands, before he was appointed as the Chief of Staff – Deputy Commander of the Ukrainian Air Force in 2017.

Colonel
Artem Antonov

is a graduate of the Kharkiv Air Force Institute (in 2003). He also graduated from the Baltic Defence College in 2017 (staff course), Latvian National Defence Academy (master's program) and the US Army War College in 2022 (war college). Holds a professional bachelor's degree and two master's degrees. He also holds Candidate of Science degree and Senior Researcher rank.
Since 2018 he heads the Military R&D Section in Air Force Command HQ and responsible for coordinating of such an activity within the Ukrainian Air Force.

© MMU, Norwegian AF

NATO's Multinational MRTT Unit

An Update and Case Study for Future Defence Cooperation

By Lieutenant Colonel Isaiah Oppelaar, US Air Force, JAPCC

Introduction

In the 32nd edition of the Journal of the JAPCC, the 'The Multinational Multi-Role Tanker Transport Fleet Programme' article detailed the organization and structure of the Multinational MRTT Unit (MMU), which employs the KC-30M Multi-Role Tanker Transport (MRTT) aircraft.[1] Since publishing, a number of developments within NATO's Air-to-Air Refuelling (AAR) mission set warrants revisiting this topic.

This article will provide a brief review of the formation of the MMU, update on the progress and the successes over the past year and a half and, most importantly, provide recommendations for NATO and the Alliance members to improve the interoperability of NATO AAR capabilities and a model for future defence cooperation programmes. For this article, MMF (Multinational MRTT Fleet) refers to the aircraft acquisition programme, and MMU refers to the unit responsible for training and equipping the personnel and operating the aircraft.

The MMF Programme

The MMF programme began in 2016 when the Netherlands and Luxembourg signed the Memorandum of Understanding (MoU). Shortly after, Belgium, Germany, Norway, and then the Czech Republic joined by signing the MoU.[2] As additional signatories joined the programme, more aircraft were ordered, resulting in a planned fleet of nine MRTTs operating from two locations. The Main Operating Base in Eindhoven, the Netherlands, will operate five aircraft, and eventually, four aircraft will operate from a designated Forward Operating Base located in Cologne, Germany.

As of this publishing, the MMF consists of seven A330-200 MRTT aircraft with the latest delivered in August 2022 and the last two expected before the end of 2024.[3] The Organisation for Joint Armament Cooperation (OCCAR) in cooperation with NATO Support and Procurement Agency (NSPA) led the procurement of the MRTT aircraft.[4] With the procurement phase nearly complete, OCCAR, whose role was to execute the acquisition of the aircraft, will pass sustainment entirely to NSPA, who is responsible for lifecycle management and sustainment, completing the OCCAR-NSPA cooperation agreement.[5]

The MMU, which encompasses the personnel and support equipment to operate the fleet of aircraft, continues training and certification of pilots, air refuelling operators (AROs), cabin attendants, and maintenance personnel to execute the unit's primary missions, which include air refuelling, airlift, and aeromedical evacuation. The MMU currently has at least 40 qualified pilots, more than 20 fully trained AROs, and 30 qualified cabin attendants. This amount of trained personnel, representing more than half of the required personnel, assures the necessary experience and capability to begin initial operations.

MMU Initial Operational Capability

Initially delayed due to the COVID-19 pandemic, the MMU expects to hold the Initial Operational Capability (IOC) ceremony in the spring of 2023. Typically, the IOC declaration occurs before accepting operational missions. However, critical NATO operational requirements brought the MMU into the mission before such formality.

First used for its passenger transport capability, the MMU supported the evacuation of military personnel and civilians from Afghanistan in August 2021.[6] Following Russia's invasion of Ukraine in February 2022, NATO requested the MMU AAR capability to

© MCD/Arnoud Schoor

support NATO operations along the eastern flank. These missions included NATO enhanced Air Policing, enhanced Vigilance Activities, and Air Shielding to enhance security and guarantee territorial integrity.[7] As of October 2022, the unit has flown more than 175 AAR missions and offloaded more than 6.5 million litres of fuel to more than 800 aircraft. Simultaneously, the MMU began participation in large-scale aircraft deployments and exercises.

In March 2022, the MMU supported exercise Cold Response 22 which was designed to train, rehearse, and validate advanced NATO and bi-lateral plans for reinforcing Norway and the High-North in an Article 5 situation with a realistic threat environment.[8] Then, the MMU again proved its impressive capabilities in August 2022 during exercise Pitch Black, rapidly deploying three MRTT aircraft along with six German Luftwaffe EF-2000 aircraft from Europe to Australia in under 24 hours for sustained operations.[9] During the exercise, the MMU participated in the tactical execution of large force employment offensive counter-air and counter-land operations for almost three weeks in a multinational environment to enhance interoperability among the 17 participating nations.[10]

These recent major accomplishments, many of which were planned and executed concurrently, prove the MMU's readiness to declare IOC and enable the unit to further develop the necessary capabilities to meet the full range of national and NATO requirements.

Current Status and Limitations

The JAPCC manages, tracks, and facilitates the interoperability of AAR assets and receivers across Alliance and partner nations. In this role, the JAPCC develops procedures, doctrine, and technical guidelines for AAR operations and systems development. For the MMU and several nations working to recapitalize their AAR fleets, the mantra is 'a tanker without a clearance is not a tanker'. That is, each type of AAR aircraft must obtain technical and operational clearance to refuel each type of receiver aircraft prior to receiving an operational mission tasking.

NATO standardization document ATP 3.3.4.2.1, 'A Guide to Obtaining Air-to-Air Refuelling Clearances and Compatibility Assessments' provides the necessary guidance for nations looking to establish and maintain the AAR interoperability of their aircraft, whether receiver or tanker. The process, known as a Technical Compatibility Assessment (TCA), 'confirms that the aircraft are (or are not) able to mechanically couple, off-load or on-load fuel, and then decouple without damaging either aircraft or creating an unsafe situation and determines the airworthiness and technical risk of a tanker and receiver pairing'. Nations assess technical compatibility, from category 1 to 3, depending on the analysed level of risk.[11]

After completing a TCA, nations assign a clearance category specifying any limitations discovered during flight testing or if the flight testing has yet to be accomplished. A category 3 clearance means that 'all requisite technical aspects regarding airworthiness/safety of flight for the targeted tanker/receiver pairing have been satisfied through acceptable means of compliance for the targeted scope specified by the nation requesting and/or conducting the analysis'.[12] These clearance categories are bilateral, requiring each nation operating a specific aircraft type within a tanker-receiver pairing to assign a clearance category.

The AAR Clearance and Compatibility Database (AAR Matrix), available on the JAPCC website (https://coi.japcc.org/aar/), reveals that many of the newest tankers operated by NATO and partner nations, including the KC-30M, KC-46A, A-330 MRTT Phénix, and KC-30A, are still in the process of completing the TCAs to establish the AAR clearances.[13]

The MMU KC-30M currently has Category 3 technical compatibility clearance with F-16A/C from 10 different nations, F-35A from the Netherlands, Norway, Italy, and the United States (US), and drogue-only receivers from the German Luftwaffe, including the EF-2000 and TORNADO IDS/ECR. The KC-30M has clearance to refuel six different aircraft types spread across 12 nations. To put this into perspective, the previous tanker flown by the Netherlands was the KDC-10, now retired, which was certified for more than 40 different receiver types from 16 NATO and 10 partner nations. So far, the KC-30M has only 30 % of KDC-10's AAR clearances.

Tanker Interoperability Is a NATO Challenge

The MMU is not navigating the challenges of implementing a new tanker alone. Many nations are incorporating new tanker aircraft that currently lack clearances with the aircraft they need to refuel in the event NATO or a coalition must execute combined operations. The NATO standard used to evaluate these clearances provides risk mitigations, assured safety between nations, and a general procedure for an expedited clearance process called 'read-across'.

'Read-across' is the method for achieving certification for a specific tanker-receiver pairing based on an existing certification of like-aircraft pairing from another nation. This method enables nations to share their engineering and testing information for an approved tanker-receiver pairing, subsequently allowing nations to evaluate the data, determine if it meets their certification requirements, and then either grant a clearance or develop a reduced test plan to complete the certification. 'Read-across' can dramatically reduce the total expense of AAR certification, but it relies on the bilateral sharing of testing and engineering data, often impeded by classification restrictions or other issues.

However, the read-across process does not apply to an aircraft pairing where clearance does not currently exist. For all new aircraft types (MRTT, KC-46A, KC-767A, etc.), every receiver-tanker pairing must be certified before tasking, which necessitates a significant expenditure of time, money, and other resources. Experience shows that aircraft that should be compatible (i.e. on paper) sometimes exhibit suboptimal characteristics during certain flying and refuelling conditions. In several cases, flight restrictions or aircraft modifications are required to enable safe in-flight refuelling.

Despite these challenges, the Alliance will achieve the interoperability needed for operations, but only with intentional peacetime efforts and the deliberate decision by Alliance's members to act, dedicating the time, money, personnel, and ideally data sharing. In the short term, and particularly if tasked to execute an operation similar in scope to Operation Unified Protector, NATO will face a significant challenge as several nations have retired or are retiring their legacy platforms before the replacement aircraft have the necessary certifications to fill the requirement.

Way Ahead and Recommendations

The MMF is an outstanding example of cooperation, burden sharing, and innovative NATO Smart Defence actions.[14] Former NATO Secretary General, Anders Fogh Rasmussen, launched NATO's Smart Defence

© MMU

© US Navy

initiative in 2011 to help the Alliance develop, acquire, and maintain capabilities in a cost-effective and efficient manner.[15] He defined Smart Defence as 'how NATO can help nations to build greater security with fewer resources but more coordination and coherence, so that together we can avoid the financial crisis from becoming a security crisis', reiterating that 'we need a new approach: Smart Defence – ensuring greater security, for less money, by working together with more flexibility'.[16] Along with the NATO Alliance Ground Surveillance (AGS) operating RQ-4Ds from Sigonella, Italy, the MMF is one of several programmes established or matured under the NATO Smart Defence initiative.[17] These programmes bring together nations looking to meet national and NATO Defence Planning Process (NDPP) capability targets without bearing the full cost of a national defence procurement programme.

The MMF programme expects to complete its planned procurement in 2024 and to declare Full Operational Capability (FOC) during the summer of the same year. According to Colonel Jurgen van der Biezen, the Commander of the MMU, the programme's member nations have the option to order an additional aircraft for every 1,100 flying hours added to the programme. As of December 2022, the 10th MRTT aircraft was ordered as Belgium recently increased their national contribution, bringing the programme to more than 10,000 flight hours per year. Additionally, any nation can apply to join the MMU although no nations are currently pursuing this option.[18] The following recommendations can help the MMU achieve its full potential while enabling NATO members to reach national and NDPP targets.

Recommendation 1. Additional NATO nations should join the MMF programme. For many allies, building an internal air refuelling capability is cost prohibitive, but almost all have receiver aircraft. The MMF offers AAR capability at much lower entry cost. Further, with sufficient additional flight hour contributions the nations can agree to negotiate and order additional aircraft under a supplemental purchase agreement, increasing the total fleet size. In addition to improving training and operational capability, these flight hours would enable more nations to complete the required tanker and receiver certifications.

Recommendation 2. Ally and partner nations with receiver aircraft should purchase or otherwise negotiate flight hours directly from MMF member states first to accomplish necessary testing to complete receiver clearances and, second, to accomplish other training or operational needs.[19] Under the MMF programme and potentially through 'Air Transport & Air-to-Air Refuelling and other Exchanges of Services' (ATARES), many NATO nations can use this cashless system to gain access to the MMF capability to complete any required flight testing and document improved tanker interoperability.

Recommendation 3. The US should contribute to the MMF at a level sufficient to enable the acquisition of an additional aircraft. The US has, historically, provided the majority of NATO's AAR capability and operates a diverse and extensive array of receiver aircraft, many of which are not operated by other nations. Joining the MMF would enable rapid certification of all US receiver aircraft, currently in backlog. Furthermore, US certification requirements are rigorous and could be a force multiplier leading to multiple read-across certifications. By joining the programme, the US would increase support to NATO and gain access to the KC-30M airframes and associated capability. This enables testing and certification flights and access to the KC-30M for exercises, operations, planning, and tactics development. This buy-in also increases the US tanker capacity for the Europe and Africa regions without deploying additional US-owned aircraft, already in critically high demand.

Conclusion

The MMF programme is, by all accounts, an enormous success for NATO and the MMF members. Over the coming months and years, the programme will continue to improve the number and diversity of AAR technical and operational compatibility certifications. In a crisis requiring a NATO military response, the MMF will be ready to meet the mission needs of operational commanders. Furthermore, the MMF programme demonstrates the Alliance's stalwart capability and willingness to support and, when necessary, defend itself. With NSPA's oversight and partnership with the European Defence Agency, the MMF proves the viability of cooperative defence programmes, especially those needed to fill critical roles. NATO must build upon the success of this programme and explore other areas where cooperative defence acquisitions can fill national and Alliance capability requirements. ●

[1] Pérez, J.M.C., 'The Multinational Multi-Role Tanker Transport Fleet Programme'. JAPCC Journal Ed. 32.

[2] 'OCCAR and NSPA sign revised cooperation pact for European MRTT project', Air Force Technology. https://www.airforce-technology.com/news/occar-nspa-revised-pact-europe-mrtt/ (accessed 16 December 2022).

[3] 'NSPA delivers sixth and seventh A330 MRTT aircraft to MMF Unit'. https://www.airforce-technology.com/news/nspa-sixth-seventh-mmf-unit/ (accessed 16 December 2022).

[4] OCCAR is an international organization whose core business is the through-life management of cooperative defence equipment programmes established by means of the OCCAR Convention and includes Belgium, France, Germany, Italy, Spain, and the United Kingdom as member states.

[5] NSPA is the executive body of the NATO Support and Procurement Organisation (NSPO), of which all 30 NATO nations are members. Those nations are represented in the NSPO Agency Supervisory Board (ASB), which directs and controls the activities of the NSPA. The Agency's organizational structure is composed of four main business units: Life Cycle Management, Support to Operations, Central Europe Pipeline System, and NATO Airlift Management.

[6] 'Multinational MRTT Fleet Continues To Grow'. https://www.nspa.nato.int/news/2021/multinational-mrtt-fleet-continues-to-grow (accessed 16 December 2022).

[7] 'German and Belgian Fighters on NATO Mission in Estonia', HQ AIRCOM, 24 October 2022. https://ac.nato.int/archive/2022/DEU_BEL_missions_EST (accessed 16 December 2022).

[8] van Boven, J. and van Noye, A., 'Cold Response 22, Media Flight in A330-MRTT', 29 March 2022. https://www.blogbeforeflight.net/2022/03/cold-response-22-media-flight.html (accessed 16 December 2022).

[9] Dubois, G., 'NATO spreads its wings – and shows its claws – over the Pacific'. 19 August 2022. https://www.aviacionline.com/2022/08/nato-spreads-its-wings-and-shows-its-claws-over-the-pacific/ (accessed 16 December 2022).

[10] Waters, S., 'Pitch Black 2022 concludes international interoperability exercise', 12 September 2022. https://www.af.mil/News/Article-Display/Article/3155660/pitch-black-2022-concludes-international-interoperability-exercise/ (accessed 16 December 2022).

[11] NATO Standard ATP-3.3.4.2, 'Air-to-Air Refuelling', edition D, April 2019. https://coi.japcc.org/aar/ (accessed 16 December 2022).

[12] Ibid. 10.

[13] Ibid. 11.

[14] 'Success with cooperative EU-NATO defence acquisitions', The European, 22 May 2022. https://magazine-the-european.com/2022/05/22/success-with-cooperative-eu-nato-defence-acquisitions/ (accessed 16 December 2022).

[15] 'Multinational capability cooperation', NATO, 18 November 2022. https://www.nato.int/cps/en/natohq/topics_163289.htm (accessed 16 December 2022).

[16] 'Building security in an age of austerity', NATO, 5 February 2011. https://www.nato.int/cps/en/natolive/opinions_70400.htm (accessed 16 December 2022).

[17] 'Alliance Ground Surveillance (AGS)', NATO, 20 July 2022. https://www.nato.int/cps/en/natohq/topics_48892.htm (accessed 16 December 2022).

[18] Email from MMU Commander, 5 December 2022.

[19] Ibid. 1.

Lieutenant Colonel Isaiah 'CHAFF' Oppelaar

is a command pilot in the KC-135R/T from the United States of America with more than 130 combat missions supporting Operations Inherent Resolve, Freedom Sentinel, Spartan Shield, New Dawn, and NATO Operation Unified Protector. Currently, he is the Air Mobility Strategist at the Joint Air Power Competence Centre in Kalkar, Germany. In this role, he executes the JAPCC programme of work for air mobility, including leading the global Air-to-Air Refuelling interoperability and compatibility efforts, supporting NATO Allied Air Command's Specialized Heavy Air Refuelling Course (SHARC), and supporting the Military Committee Air Standardization Board as the Chairman of the Air-to-Air Refuelling Working Group.

NATO IAMD Education and Training

Back to the New Normal

By Lieutenant Colonel G. W. Pronk, NE Air Force, JAPCC

Russia's air and missile attacks on Ukraine underscored the importance of Integrated Air and Missile Defence (IAMD) and, more specifically, Surface-Based Air and Missile Defence (SBAMD) as an essential part of NATO's Defensive Counter-Air (DCA) capability. As the military conflict continues, the looming question hangs heavily on NATO's eastern border: are NATO SBAMD forces ready for action at a moment's notice? It is vital to the security of NATO that Air Defence (AD) operators are NATO mission qualified now because they must be ready to act and fight with little or no warning, as a crisis can quickly turn to conflict. After experiencing thirty years of air superiority in NATO operations, the change in threat perspective urges NATO nations to reconsider defence against air threats.

During the Cold War, NATO commanded air force units, which were on high-alert status. They had to adhere to a strict exercise and evaluation schedule to ensure the proper levels of readiness and preparedness to counter any surprise attack from the Warsaw Pact. Although the Cold War lies decades behind us, the essence of enabling a NATO-qualified AD is still the same. It is up to the NATO countries to regain these readiness standards of decades past, enabling a credible 'ready to respond' AD.

IAMD is a cornerstone of our security that requires continuous effort, investment, and dedication both in peacetime and crisis. In NATO, ensuring SBAMD combat readiness is a national responsibility. This article will give a better insight into the challenges and available tools to prepare NATO SBAMD. The Alliance has the required Education and Training (E&T) tools in its inventory, like the IAMD Common Education and Training Program (CET-P), and exercises like Ramstein Legacy (RaLy) and Joint Project Optic Windmill (JPOW). But given that SBAMD is a national responsibility, how can the NATO nations sharpen, shape, and particularly use the existing tools most efficiently?

Background

IAMD protects strategic interests, territory, population centres and (deployed) forces against the full spectrum of air and missile threats. It is an essential and enduring mission across the spectrum of peacetime competition to crisis and conflict. In NATO doctrine,

© MCD, Hille Hillinga

© Corona Borealis Studio/Shutterstock.com

IAMD falls under DCA and, as such, is an integral component of Joint Air Power and a core task for the Joint Force Air Component (JFAC). All NATO AD forces need to comply with the Allied Command Operations Forces Standards if we are to seamlessly integrate effects against a dynamic threat environment.[1]

For IAMD, the total threat spectrum ranges from micro-drones to fifth-generation aircraft, ballistic missiles, and hypersonic threats. IAMD includes all active measures to prevent a potential opponent from effectively employing weapons in or through the air domain. Holistically, IAMD consists of airborne (fighter) AD and SBAMD, which should complement, when applicable, offensive operations to reduce potential air threats. A mix of offensive and defensive capabilities provides credible deterrence but demands well-trained crews. They must operate under utmost concentration in a dynamic environment to neutralize various enemy threats and protect friendly assets.

Requirement: High Readiness

The United States (US) Army AD artillery has a long-standing motto: 'Air Defence, First to Fire!' It is as true now as it was during the Cold War. Since the early 1990s, allied and non-allied operations have all started with an air dominance operation immediately followed by neutralizing the enemy's Command and Control (C2). This sequencing requires that AD must be able to fight in the twilight between crisis and conflict, with little or no warning. In such a situation, a combination of civil and military air procedures and command structures will be enforced, complicating time-critical operations.

SBAMD must be quickly deployable and under high readiness in peacetime, while in crisis or conflict must be able to sustain 24/7 high-intensity operations indefinitely. High readiness requires resilience and redundancy. On top of the high standard of training and readiness, modern SBAMD weapon systems have high-technical demands, both in terms of skilled operators and technicians and in terms of technological infrastructure.

During the Cold War, DCA was a standing NATO mission, and SBAMD forces were essential to NATO's DCA capability. An AD barrier from Norway to Türkiye encompassed surface and air-based AD systems integrated under an air commander. It protected the Alliance

For IAMD the total threat spectrum ranges from micro-drones to fifth-generation aircraft, ballistic missiles, and hypersonic threats.

members against an assumed first air strike from the Warsaw Pact. AD forces could switch to 'war-mode' in minutes or even seconds. After the Cold War, the Alliance decommissioned the surface-to-air missile barrier and SBAMD capabilities diminished or disappeared with nations' desire to harvest the peace dividend. The air defence fighter's role atrophied to only air policing.

Within NATO, the JFAC commands and controls SBAMD as part of DCA. The national Control and Reporting Centres (CRC), which direct SBAMD forces, represent an essential node in the Air C2 architecture.[2] Technology and standardized procedures enable NATO SBAMD forces to fight side-by-side with airborne assets simultaneously without fear of fratricide. This performance is made possible by the JFAC, which is doctrinally responsible for planning the DCA defence design.

Protecting friendly aircraft is as essential as maximizing attrition to enemy air assets. Unfortunately, maintaining SBAMD forces in high-alert status can have deadly consequences. Operators will be under stress in ambiguous situations, urged to make a split-second decision. It could result in fateful incidents, as witnessed in the 1983 Soviet downing of Korean Airlines Flight 007 and the 1988 US Navy downing of Iranian Air Flight 655. A more recent instance is the downing of the Ukraine International Airlines Flight 752 near Teheran in 2020. In the last forty years at least twenty-five similar catastrophic mistakes occurred. One assumes these incidents occur when the taut nerves of military controllers, in a state of high alert, misread their instruments or deviate from (identification) procedures, erroneously identifying commercial flights as hostile. These gruesome incidents underscore the requirement for proper coordination and accurate identification, made even more challenging in the fog and friction of unfolding conflict.

In critical situations like the above, the decision to engage an aircraft or not will result from a split-second decision-making process since there will be no time to 'look it up' or ask for guidance. To achieve a satisfactory military skill level in the AD domain and prevent such tragedies, extensive E&T is needed down to the lowest tactical level. Since most of the work is done in crews, any change to the crew could affect the qualification standard. The complexity of the AD mission drives particular requirements for SBAMD systems and crews. AD crews must be capable of decentralized mission execution at any time, under standing orders and procedures. Good tactics, techniques, and procedures, backed by a diligent E&T programme, develop the ability to act quickly and correctly in demanding situations.

National Responsibilities

After 1991, as the air threat to European NATO countries seemed non-existent, only a few nations maintained their SBAMD forces at NATO training standards.[3] Some withdrew from the NATO evaluation (validation) programme, and others abandoned their SBAMD assets. The current events in Ukraine have changed this mindset.

Within NATO, it is a national responsibility to organize, train, and equip forces before transferring them under NATO command in crisis or conflict. Maintaining certain training levels is essential, and national training activities must lay the foundation of technical competence long before the needs of war. After recruitment, basic training, and weapon handling, the air warfare procedural education will produce a minimally trained AD soldier. From here, the AD soldier starts gaining expertise through advanced education, training, exercises, and evaluations. The evaluation completes the AD training with a NATO quality validation. Thereafter, it is a national responsibility to uphold that standard.

Training Opportunities

IAMD exercises are an essential link in the qualification chain of an AD capability. They practice the art of truly *integrated* air and missile defence by combining land, sea, and air-based systems into a single air defence design. National exercises like Tobruk Legacy, which morphed into the RaLy NATO exercise series, and JPOW (facilitating Steadfast Armour and Ramstein Century NATO exercises), are scarce and cherished events. JPOW takes place in odd years, with RaLy in even years.

Joint Project Optic Windmill is a German-Netherlands-led networked computer-assisted exercise with a simulated air and missile threat that focuses on doctrine, techniques, tactics, and procedures. It enjoys strong support from US EUCOM and the US Missile Defence Agency. JPOW provides IAMD training for ally and partner nations. Players from the strategic to tactical levels exercise their role in NATO's IAMD mission in a near-future (+five years) air threat scenario. By including a concept development and experimentation phase, which precedes the execution phase, it offers the opportunity to demonstrate, practice, evaluate, and validate different IAMD programmes and concepts that may require specific circumstances. A considerable part of NATO's IAMD procedures and parts of its current command structure was developed and evaluated during JPOW exercises.

JPOW and RaLy are the only events where Air C2 crews, airborne assets, and SBAMD units train together in a challenging and realistic scenario.

© DGLC

Ramstein Legacy grew from a Czech Republic-Slovakian initiative into a NATO chapter 1 IAMD exercise. RaLy is a live exercise with a tactical focus to deliver a robust strategic message and improve readiness. RaLy aims to support SACEUR's Concept for the Deterrence and Defence of the Euro-Atlantic area. It incorporates several existing live NATO exercises into one AIRCOM-led exercise, which runs biennially. It uses a tactical data link network, live flying red assets, and can incorporate live electronic warfare. Typically, it also includes a live-firing phase. The exercise's host nation rotates and is generally at the NATO eastern border.

These two exercises are the only events where Air C2 crews, airborne assets, and SBAMD units train together in a challenging and realistic scenario. In these exercises, the action of one directly shows an effect on the other, and mutual trust building inherently leads to improved air defence. The involvement of a NATO JFAC in both exercises is essential because, in the European theatre, we will only fight collectively. It was 'fighting the NATO fight' during these two exercises that indicated the need for the CRCs and JFAC to streamline NATO Air C2 procedures and harmonize the actions of both SBAMD operators and Air C2 crews. These considerations led CAOC Uedem and the JAPCC to create the CET-P.

Common Education and Training Program

Driven by the challenges encountered during the above-mentioned exercises and smaller Air C2 training opportunities, it was clear that additional attention to the NATO DCA battle was required.

In April 2021, Commander CAOC Uedem recommended starting a NATO IAMD CET-P. With AIRCOM's full support, CAOC Uedem and the JAPCC created a framework for a Basic IAMD Training plan in close co-operation with the GE/NE Competence Centre Surface-Based Air & Missile Defence and the IAMD Centre of Excellence (COE). The CET-P Basic IAMD training focuses on the tactical level and contains lessons learned regarding NATO C2 tasks and responsibilities, SBAMD air planning, tactical data links, air reporting, and current threat intelligence. The JAPCC hosted the first three training sessions at their facilities in Kalkar, Germany. The follow-up trajectory for the CET-P will take place under the responsibilities of the IAMD COE in Souda, Crete, Greece. In addition to this basic IAMD training, which has a tactical focus up to the CRC level, the CAOC E&T sections attend to the 'higher echelon' CET-P training, focused on Air C2.

Although basic training is a national responsibility, the CET-P initiative offers valued support to newcomers in the SBAMD realm and to forces that train to operate outside of NATO's area of responsibility or are unfamiliar with NATO procedures. Since CET-P training is scarce (two to three per year), the best efficiency is achieved by training the national trainers, thus enabling them to teach their respective national crews.

Quality Control

There is a more than justified emphasis on the quality control part of E&T to identify capabilities and highlight shortfalls. Quality control validates mission readiness or provides direction for securing it.

NATO's quality control of air entities resides with AIRCOM's Evaluations Division as 'SACEUR's audit team'. SBAMD and other air entities must adhere to the NATO Tactical Evaluation (TACEVAL) or Forces Evaluation (FORCEVAL) Standing Operating Procedures and Instructions, parts of the Allied Command Operations Forces Standards. These directives provide training guidance and evaluation criteria for tactical air units offered to NATO. As a reactive organization, NATO depends on swift responses and units must qualify before operations. AD units must be qualified before the nations offer them to NATO operations. This implies that all AD forces designated for any NATO response or reaction force should be NATO qualified before admission. Therefore, NATO members should strictly adopt and follow the NATO Allied Command Operations Forces Standards for their training.

In addition to the TACEVAL/FORCEVAL, SBAMD units can perform a NATO-evaluated tactical firing. This can be done from the NATO Missile Firing Range at Chania,

Performing a live firing in accordance with NATO standards is a challenge that provides a solid crowning accomplishment for the unit and its nation.

on the Greek Island of Crete, or any firing range with a NATO-supported evaluation team. Performing a live firing in accordance with NATO standards is a challenge that provides a solid crowning accomplishment for the unit and its nation.

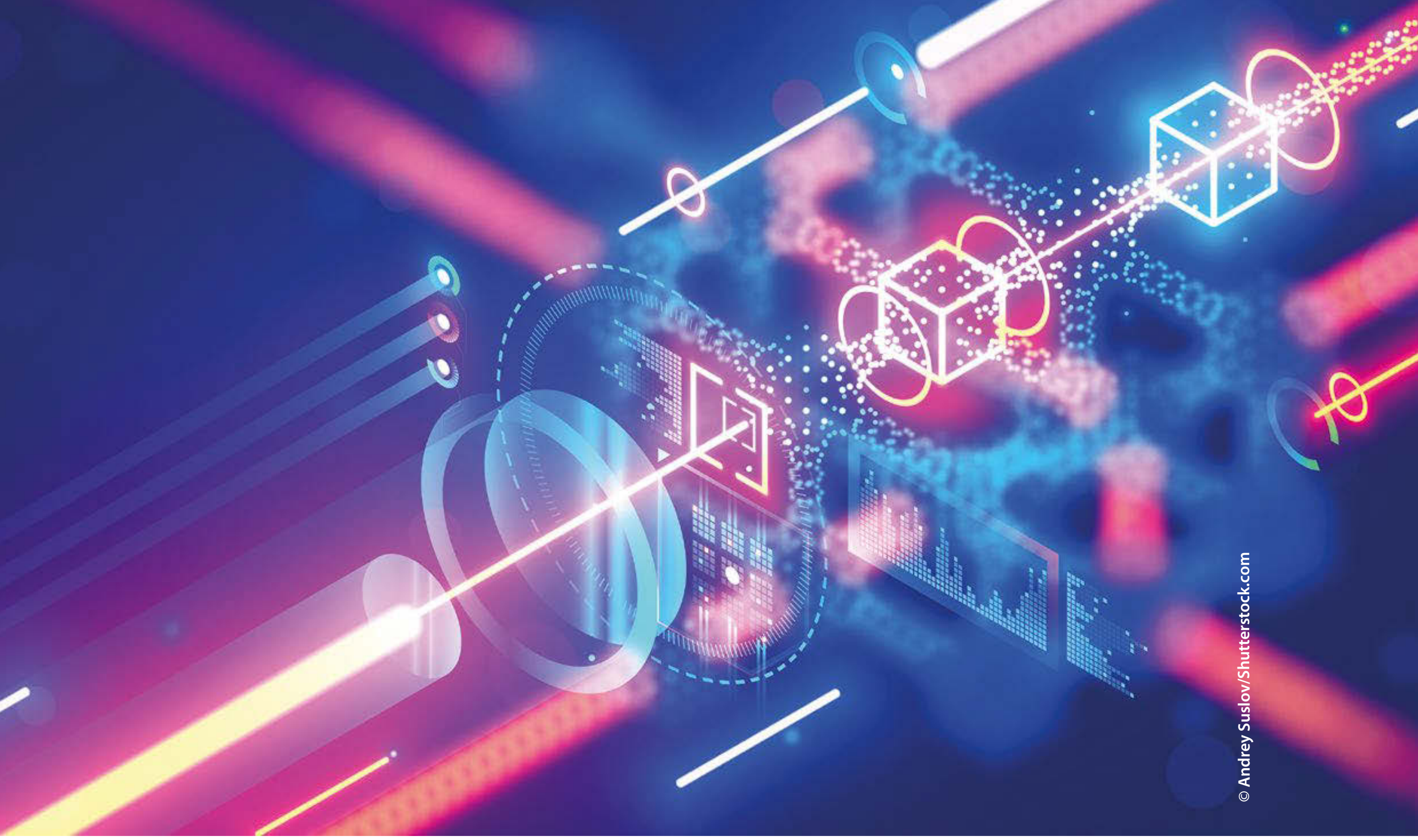
Conclusion

E&T is often undervalued and even easily downsized. Too often, a lack of proper E&T is recognized at the time of crisis when it is too late to adjust. NATO AD forces need to be ready today. Nations, supported by NATO, should take every available step today to ensure the availability of NATO-qualified, combat-ready SBAMD forces for a time when conflict may be upon us. The established E&T opportunities backed up by NATO, national IAMD exercises, and the consequent evaluations constitute the framework for all SBAMD units to achieve the required proficiency levels. The readiness tools are still available and efficient, but we must use them. SBAMD forces are inherently defensive, they are logical to improve deterrence through strength. It is up to the nations to use these tools effectively and judiciously to ultimately increase proficiency, technical interoperability, and readiness! ●

1. Allied Command Operations Forces Standards, Volume II & III.
2. NATO Industrial Advisory Group, Report of Study Group 220, Chapter 7.9.3, '…need for distributed control if the GBAD becomes isolated from the higher echelon (CAOC or JFAC), the concept of distributed control empowers subordinates' commanders, GBAD organization and Operations Centre platforms to cooperate according to a pre-planned combat airpower through a resilient C2 architecture. C2 means will be congested and contested/vulnerable to Cyber and/or Electronic Attack'.
3. Ibid. 1.

Lieutenant Colonel G. W. 'Berry' Pronk

has served for over 40 years in the Royal Netherlands armed forces and has completed operational tours during operations Desert Storm, NATO Display Deterrence (US Operation Iraqi Freedom), and in SFOR, former Yugoslavia. He served in various national command and training positions in Surface Based Air and Missile Defence, as well as staff positions at the Royal Netherlands Air Force Command and The Royal Netherlands Army Command. Internationally, he served at the former HQ Extended Air Defence Task Force (with US Army and German Air Force) and the German Air Force Forces Command, as well as Section Chief Air Operations at J3, NATO SHAPE. Currently, he holds the Subject Matter Expert position for Surface Based Air and Missile Defence at the Joint Air Power Competence Centre in Kalkar, Germany.



© Andrey Suslov/Shutterstock.com

Quantum Technology for Defence

What to Expect for the Air and Space Domains

By Dr Michal Krelina, Czech Technical University in Prague

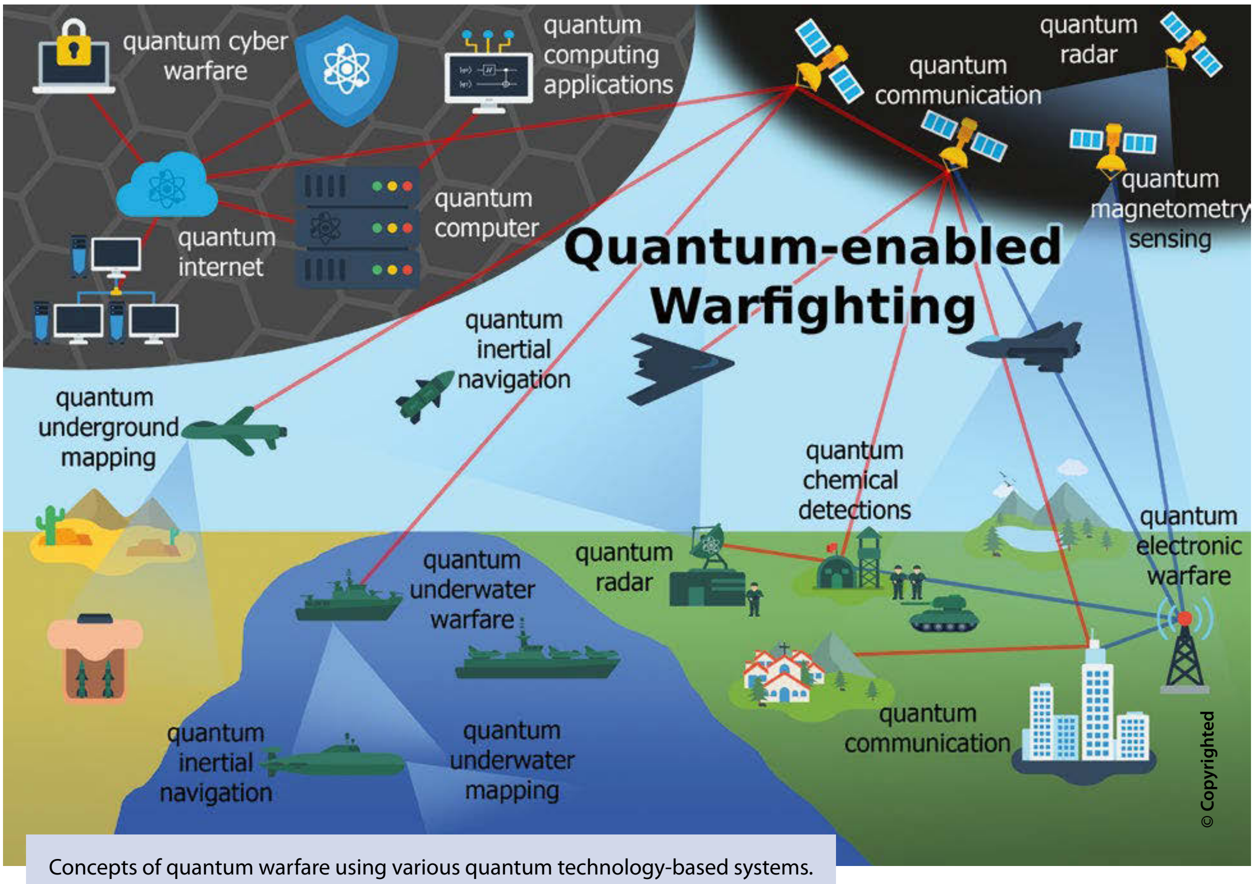
By Lieutenant Colonel Denis Dúbřavčík, CZ Air Force, JAPCC

Introduction

Quantum Technology (QT) has its foundation in quantum mechanics, a discipline more than one hundred years old. The first applications of quantum mechanics, known as Quantum Revolution 1.0, include nuclear fission, lasers, semiconductors, etc., where the statistical aspects of quantum behaviour are exploited. The first quantum revolution had and still has a profound impact on all aspects of society, from the military and international security to the development of atomic weapons, chips, computers, and precise navigation.

Now, we are entering Quantum Revolution 2.0, or QT, where we are exploiting the full spectrum of quantum physics' so-called 'strange' laws at the limits of known physics. In Quantum Revolution 2.0 we exploit the behaviour of individual quantum systems such as the electron, atom, nucleus, molecule, quasiparticles, etc. QTs will not introduce fundamentally new weapons, as happened with nuclear and laser weapons, but rather improve and sharpen present sensing, communication, and computing capabilities. Although most QT's aspects are still in the form of fundamental rather than applied research, we can foresee several highly relevant applications for defence.

QTs are at the forefront of advanced nations' long-term defence planning, including the United States, China, the United Kingdom, Australia, India, Russia, Canada, etc. In February 2021, NATO Defence Ministers endorsed the Emerging and Disruptive Technologies


quantum cyber warfare
quantum computing applications
quantum communication
quantum radar
quantum magnetometry sensing
quantum computer
quantum internet
Quantum-enabled Warfighting
quantum inertial navigation
quantum underground mapping
quantum chemical detections
quantum electronic warfare
quantum radar
quantum underwater warfare
quantum communication
quantum inertial navigation
quantum underwater mapping
© Copyrighted

Concepts of quantum warfare using various quantum technology-based systems.

(EDT) Strategy to promote a coherent approach to developing and adopting dual-use technologies, with quantum-enabled technology being one of the nine technology areas promoted in this strategy.[1]

Other international actors are aggressively pursuing QTs. For example, the Chinese People's Liberation Army has recognized the strategic value and potential decisive advantage of QT,[2] while the European Union has marked QT as an 'emerging technology of global strategic importance' and noted that it will be used 'for sensitive applications in the area of security, and in dual-use applications'.[3] As such, it is clear that QTs are set to play a major role in the defence strategies of nations across the world.

NATO organizations, bodies, and member states are actively studying QTs, both theoretically and experimentally, to cope with the inherent critical technological challenges.[4, 5] At the 2021 NATO Summit, Allied leaders launched the Defence Innovation Accelerator for the North Atlantic (DIANA), with a branch dedicated to QTs.[6] Importantly, QT are a subject of interest in NATO ACT studies.[7] Moreover, the NATO Science and Technology Organization study 'Science & Technology Trends 2020-2040' examined the basis and expectations for QT in NATO while the NATO Conference of National Armaments Directors discussed the implementation plan for QT.[8]

It is important to stress here that most QTs are currently at low Technology Readiness Levels (TRL) and, thus, difficult to accurately predict the actual performance, capability, all possible applications, and timelines. This is known as the Collingridge dilemma that applies when 'a) impacts cannot be easily predicted until the technology is extensively developed and widely used; b) control or change is difficult when the technology has become entrenched'.[9] In this paper, we aim to build awareness of QT by briefly introducing the QT's key elements, their basic applications, the potential utility in the air and space domains, and set realistic expectation for fielded QT.

Key Elements

Why are the QTs so interesting and important? Using fundamental quantum physics' principles can, in theory, lead to exponential speed-up in computation, impressive increase of sensor sensitivity, and unprecedented secure communications. Overall, these areas are covered by the quantum information science discipline. Before we consider individual QTs, we must understand a few fundamentals. The features critical for the QT revolution which we will further examine are the quantum bit, quantum superposition, quantum entanglement, no-cloning theorem, and quantum tunnelling.

The quantum bit, or qubit, is the quantum analogy of the classical information bit. Whereas the classical bit can have only the values of 0 or 1, the qubit is described by a quantum state. The quantum superposition means that a qubit can represent two states simultaneously. Such behaviour has important implications for computational power enhancement. With N qubits, we can represent 2N states (i.e. the number of represented states grows exponentially with the number of qubits). Note that when the quantum measurement is applied at the end of a quantum algorithm the whole superposition collapses into one state only. Therefore, we must run one algorithm several times and draw conclusions based on the statistical distribution of individual states. With multiple repetitions, we can reach exponential speeds. However, such an increase in computational capacity requires the development of new quantum algorithms and departure from conventional computing.[10] There are also many technical complications that challenge our ability to accomplish quantum computing at scale.

The no-cloning theorem states that the quantum data of a qubit (or of an arbitrary quantum state in general) cannot be copied or cloned. On one side, this has significant consequences for increasing the complexity of quantum computers due to the need for more sophisticated quantum error corrections. The quantum errors are corrected indirectly because, as described above, a measurement of an actual state will lead to its destruction. On the other side, it provides unprecedented applications for security that cannot be eavesdropped on. The intruder's interference would require quantum measurement, which would lead to the quantum collapse to one state. Such a situation can be easily discovered by comparing the measurements of the sender and receiver.

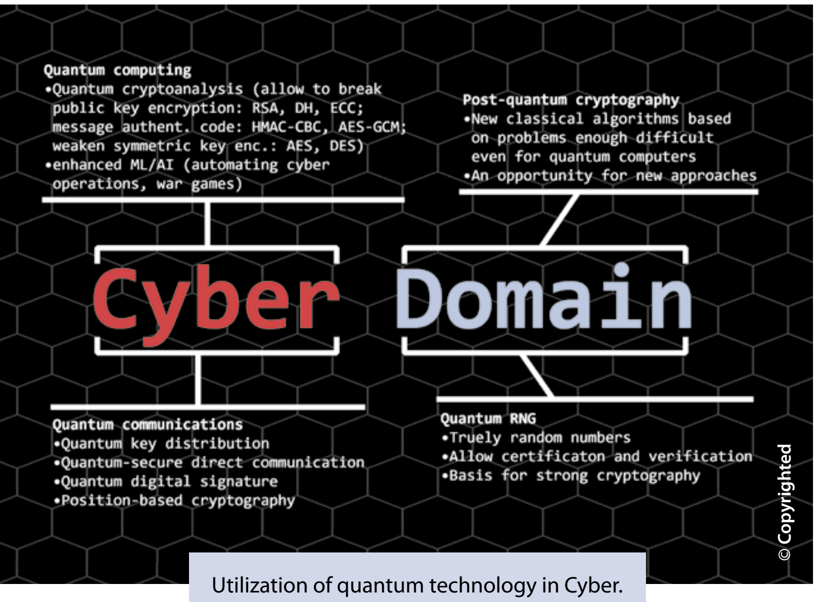
Quantum entanglement is another key concept that refers to the strong correlation between two or more qubits, a link with no classical analogy. In short, any quantum manipulation with one of the entangled qubits will have an instant effect on the other linked qubits, irrespective of the distance or obstacles between them. As such, quantum entanglement is an essential feature for most QTs, allowing them to reach the fundamental limits of present physics defined by the Heisenberg uncertainty principle, and a key element for many quantum algorithms.

In general, qubits and quantum sensing systems can be realized using different quantum-physical properties such as electric current flow in superconducting electronics, polarization or the number of photons, or the spin or energy state of electrons, nuclei, or molecules. All these quantum systems are extremely fragile, and many can be manipulated only at temperatures close to absolute zero (about -273 °C). As such, the above-described quantum properties cannot be applied directly in weapons since even the slightest disturbance leads to the loss of quantum information or sensitivity in quantum sensors. With this basic appreciation of the underlying science, let us consider potential applications.

Basic Applications

To properly understand the potential benefits, we will divide QTs into three categories: quantum computing, quantum networks and communications, and quantum sensing and imaging.

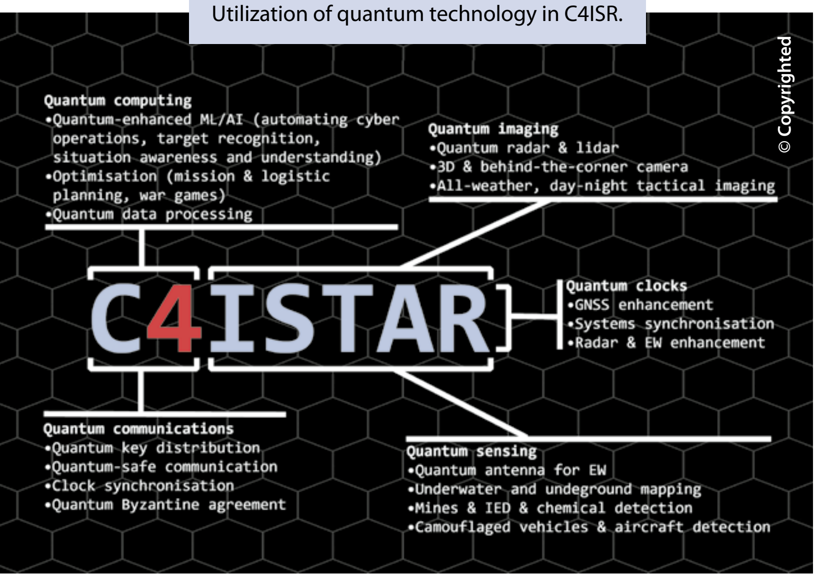
Quantum computing represents universal programmable quantum computers, quantum annealers (an imperfect adiabatic computation), and quantum simulators which can provide considerable computational advantage over classical computers. However, despite the common misconception that the exponential increase in processing speed will affect and take over all the classical computers' tasks and applications, quantum computers will only be efficient in certain highly complex and challenging computational problems. Examples of such problems are quantum simulations (molecule simulation


Quantum computing
•Quantum cryptoanalysis (allow to break public key encryption: RSA, DH, ECC; message authent. code: HMAC-CBC, AES-GCM; weaken symmetric key enc.: AES, DES)
•enhanced ML/AI (automating cyber operations, war games)
Post-quantum cryptography
•New classical algorithms based on problems enough difficult even for quantum computers
•An opportunity for new approaches
Cyber
Domain
Quantum communications
•Quantum key distribution
•Quantum-secure direct communication
•Quantum digital signature
•Position-based cryptography
Quantum RNG
•Truely random numbers
•Allow certificaton and verification
•Basis for strong cryptography
© Copyrighted

Utilization of quantum technology in Cyber.

for chemical and pharmaceutical research, new material development, etc.), quantum cryptoanalyses (breaking of most asymmetric encryption schemes commonly used to encrypt emails, voice and video calls, data transfers, and remote access to intranets), faster searching, faster solving of linear or differential equations, quantum optimizations (e.g. supply chains optimizations, logistics, investment portfolios, or customized medications), and quantum-enhanced machine learning. At the moment, quantum computing for practical deployment is at least ten years away and will not replace classical computers.

Utilization of quantum technology in C4ISR.


© Copyrighted
Quantum computing
•Quantum-enhanced ML/AI (automating cyber operations, target recognition, situation awareness and understanding)
•Optimisation (mission & logistic planning, war games)
•Quantum data processing
Quantum imaging
•Quantum radar & lidar
•3D & behind-the-corner camera
•All-weather, day-night tactical imaging
C4ISTAR
Quantum clocks
•GNSS enhancement
•Systems synchronisation
•Radar & EW enhancement
Quantum communications
•Quantum key distribution
•Quantum-safe communication
•Clock synchronisation
•Quantum Byzantine agreement
Quantum sensing
•Quantum antenna for EW
•Underwater and undeground mapping
•Mines & IED & chemical detection
•Camouflaged vehicles & aircraft detection

Quantum networks and communications aim to transmit quantum information (qubits) across various channels, such as fibre optic lines or free-space communication. The only practical use in first-generation quantum networks is Quantum Key Distribution (QKD). A significant advantage of QKD over conventional asymmetric encryption (also called public-key cryptography) is that any interception or eavesdropping attempt would be noticed immediately. QKD is commercially available for use with optical fibres, and many commercial free-space QKD services are to be launched in the next two to five years. Note that QKD is often described as unhackable. However, this is only true for properly implemented quantum information transmissions; the endpoints, controlled by classical computers, will remain targets for offensive cyber operations.

The next-generation quantum network, called Quantum Information Network (QIN) or quantum internet, differs in its ability to distribute entangled qubits.[11] QIN will offer more services related to security, such as secure identification, position verification, and distributed quantum computing. Significant technical applications will also lead to high-precision clock synchronization and networked quantum sensors. The biggest obstacle to QIN implementation is the need for reliable quantum memory to store quantum information for synchronization and distribution across a network with many intermediate nodes. The QIN could be expected in 2030+.

Quantum sensing aims for more precise measurements of various physical variables such as magnetic or electric fields, gravity gradients, acceleration rotations, and time. Improved time measurements can be used for more precise clocks (used by many current technologies), quantum inertial navigation, underground and undersea exploration, more effective radio frequency communication, etc. Quantum sensing is the most developed QT (highest TRL in average), but the effectiveness of deployed sensors is still very uncertain. However, military applications require a portable or mobile solution with low SWaP (size, weight, and power). At the same time, the spatial resolution of quantum sensors needs to improve, as it is often inversely correlated with sensitivity. For example, detecting a submarine from space may be possible, but using a quantum sensor with a useful degree of precision is unlikely since sufficient spatial resolution will lead to insufficient sensitivity. On the other hand, some quantum sensors, such as those in quantum navigation, are expected to be tested in the relevant field environments within the next five years.

Quantum imaging is a subfield of quantum optics that is active (i.e. some signal is emitted and its reflection needs to be detected) compared to quantum sensors (that measure some external quantity). For any sensor, the Signal-to-Noise Ratio (SNR) represents the fundamental limit of its sensitivity. However, a significantly higher SNR can be reached using quantum entanglement, as the signal itself may be unrecognizable in the background noise without additional knowledge of entanglement. Quantum imaging can improve the existing technology, such as quantum radars, three-dimensional cameras, around-the-corner cameras, gas leakage cameras, and low-visibility vision devices.

Lastly, Post-Quantum Cryptography (PQC), also known as quantum-resistant cryptography, is nothing quantum at all but an evolution of the present asymmetric cryptography. PQC relies on more advanced mathematics that is more difficult to compute, even for quantum computers. As such, PQC can be imagined simply as software/hardware updates to existing systems, although they are usually more computationally demanding. In principle, it can never be proven that PQC is completely secure as new classical or quantum crypto-analytical attacks may occur. Still, PQC will be available soon and resilient against quantum attacks for the foreseeable future. For example, based on the NSA recommendation, the White House published in 2022 a memorandum providing directions for agencies to start the migration to PQC with full implementation by 2035.[12] However, the US Department of Homeland Security is aiming to migrate its systems by 2030.

QT in Air and Space

As in the past with other technologies, defence applications are again the primary drivers of research and development in the field of QT, particularly in the United States and China. While much of this research is often classified, there are several overviews and roadmaps available that outline potential use cases and ideas for the air and space domains.[13] These documents provide a glimpse into the exciting possibilities of QT and its potential to revolutionize the defence industry.

Even though QT has promising potential with real transformational aspirations, due to its complexity it is still poorly understood by non-specialists and its importance is often exaggerated and hyped. At present, being mostly at the laboratory stage with low TRLs complicates realistic estimates of future utility, capabilities, or the role it will play in the future.

Here, we will present the most discussed ideas and possible use cases for the Air and Space domains.

Quantum radar is a quantum imaging system that works similarly to classical radar but at the level of individual photons. Theoretically, it offers various advantages such as higher noise resistance, stealthiness (extremely low intensity and, therefore, low probability of detection), and possible target identification. The principles of quantum LIDAR (light detection and ranging) or RADAR were already demonstrated successfully in laboratories. However, the microwave regime, which is crucial for many types of ground-based radars, presently seems unfeasible.[14] Nevertheless, space-based quantum LIDAR applications in the optical regime remain viable in the medium-to-long term. Conversely, more precise quantum or optical atomic clocks can improve the performance of current radars and electronic warfare systems.

Free-space quantum communication will be an important channel for future quantum internet and will lead to a higher presence of quantum communication assets in air and space. In the next five years, free-space quantum communication is unlikely to be part of military or governmental satellite communication services because its implementation requires new infrastructure and more investments. Moreover, the present performance is too low for practical use and the quantum network's low density makes it very vulnerable. However, quantum communication will be present in the air and space domains mainly for research and development, proof-of-concept demonstrations, and experimental, mainly commercial, applications.

The situation will change with the arrival of reliable quantum memory and high-rate quantum optics. Then, quantum internet with significant space presence may start to build up after 2030. In the future, there is an opportunity to implement quantum communication with laser communication where significant technological overlap exists. Laser communication would offer high-speed data transfer secured by quantum communication. Quantum cryptography is presently considered a secondary developmental effort to PQC. PQC is the preferred solution today since it could be just a software update, has a shorter deployment timescale, and can use the current classical networks or internet infrastructure.

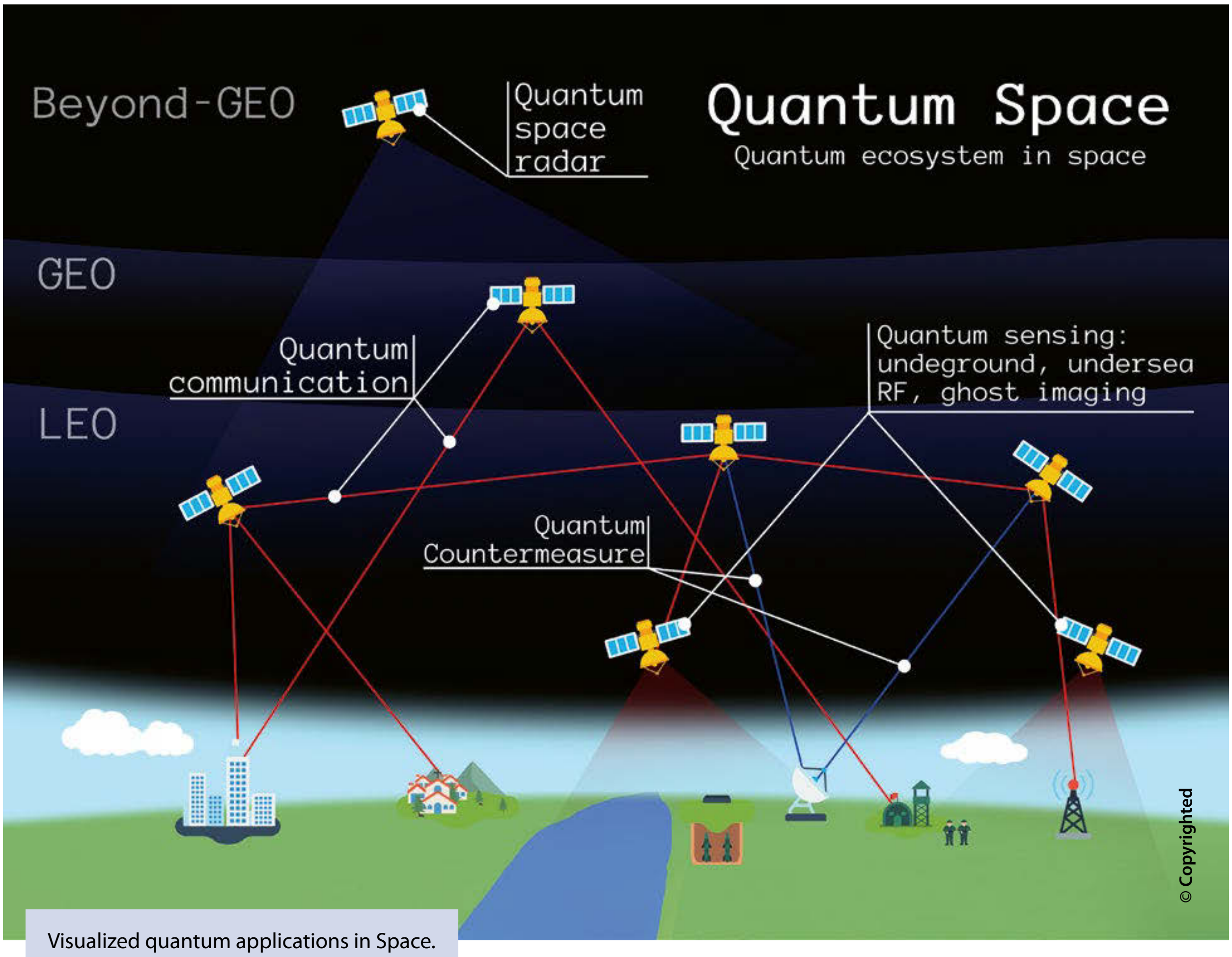
One of the most interesting applications for QT is Intelligence, Surveillance, and Reconnaissance (ISR). Individual QTs offer various sensing and imaging systems that significantly improve the extant ISR systems. Furthermore, fusing quantum ISR capabilities with conventional capabilities may lead to a new epoch in ISR by leveraging the strengths and offsetting the weaknesses of both. However, fully realizing these possibilities will depend upon quantum computing and communications.

Quantum magnetometers and gravimeters are two examples. Quantum magnetometers detect magnetic fields, such as local magnetic anomalies or weak biological magnetic signals. Quantum magnetic sensors are under development for detecting metallic objects generating local magnetic anomalies, such as mines, improvised explosive devices, submarines, camouflaged vehicles, and rotating machinery through walls. They can also serve as an alternate method of underwater navigation. Quantum gravimeters are under development for underground surveillance systems and are tested for detecting underground structures such as caves, tunnels, bunkers, research facilities, or missile silos. Both sensors could be deployed on airborne systems or space assets in low Earth orbit.

The closest QT to real deployment is the quantum radio-frequency (RF) receiver. A quantum RF receiver has improved features such as a wider band, better SNR, smaller size, better angle-of-arrival detection, self-calibration, no metallic parts to generate additional noise, output in optical regime allowing faster signal processing, and measurement of both weak and very strong fields. In the defence context, quantum RF receivers could enable reception of advanced Low Probability of Intercept/Low Probability of Detection (LPI/LPD) communications and over-the-horizon RF signals, resistance to RF interference and jamming, RF direction finding, and terahertz frequency imaging. In the future, quantum RF receivers can become the standard RF receiver for multiple systems, e.g. for 5G and the Internet of Things. Quantum RF receivers are expected to be equally helpful to expanding our communications, improving the detection of adversary signals, and calibrating the existing RF devices.

Quantum imaging systems could further serve in Intelligence, Surveillance, Target Acquisition, and Reconnaissance roles. These include all-weather, day-night tactical sensing in long/short-range, active/passive regimes, and stealth detection modes. They can work as low-light or low-SNR vision devices in environments with clouds, fog, dust, smoke, and jungle foliage or at night; for example, to assist helicopter pilots to land in dusty, foggy, or smoky environments.

Quantum inertial navigation is another relevant technology for the air domain and is analogous to classical inertial navigation but using quantum sensors. Individual parts are being tested in laboratories and relevant environments with stabilities sufficient for military use. However, creating a complete quantum inertial measurement unit is still challenging. General expectations are that quantum inertial



Visualized quantum applications in Space.

navigation will attain drift rates of only a few hundred metres per month compared to current marine-grade inertial navigation (for military ships and submarines) with a drift of 1.8 km/day.[15] The first users will probably be submarines with the least restrictive SWaP parameters. In time, we can expect more miniaturization and deployment in planes, drones, and missiles.

Quantum computing has great potential in many applications, such as improved machine learning and artificial intelligence, better aerodynamic designs, faster simulations, etc. All are expected to bring significant improvements in areas such as ISR processing and command and control. However, quantum computing is not expected to be operational for 10–20+ years, compared to 5–10+ years for quantum communication or 3+ years for quantum sensing.[16]

Conclusions

Quantum technologies hold great promise in the long term for a broad spectrum of applications, from sensing to communications to computing, but should not be assumed to revolutionize defence applications in the foreseeable future.

Even though principles were proven successful in laboratories, the transition from laboratory to real-world applications is still in progress. Requirements, such as low SWaP, mobility, and cost, still represent significant limiting factors.

For a good reason, QTs have captured our attention and imagination. Based on theoretical and laboratory work, we have an appreciation of the technology and its possible uses in real-world applications. Towards that end, NATO's role is to set goals and standards to encourage development and ensure interoperability. Meanwhile, Allied nations must invest in the necessary research and look for dual-use opportunities to speed development and reduce cost. With this understanding, we can pursue the great promise of QT with a realistic understanding of the timeline and effort involved.

[1] 'Emerging and Disruptive Technologies', NATO, December 2022. https://www.nato.int/cps/en/natohq/topics_184303.htm (accessed 3 January 2023).

[2] Kania, E. and Costello, J., 'Quantum Leap (Part 2): The Strategic Implications of Quantum Technologies', The Jamestown Foundation, 21 December 2016. https://jamestown.org/program/quantum-leap-part-2-strategic-implications-quantum-technologies/ (accessed 12 December 2022).

[3] 'Horizon Europe - Work Programme 2021–2022 – 7. Digital, Industry and Space', European Commission, 23 August 2021. https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/wp-call/2021-2022/wp-7-digital-industry-and-space_horizon-2021-2022_en.pdf (accessed 12 December 2022).

[4] 'Quantum Computing and Artificial Intelligence Expected to Revolutionize ISR', NATO ACT, 30 September 2022. https://act.nato.int/articles/quantum-computing-and-artificial-intelligence-expected-revolutionize-isr (accessed 12 December 2022).

[5] 'Using Quantum Technologies to Make Communications Secure', NATO, 27 September 2022. https://www.nato.int/cps/en/natohq/news_207634.htm (accessed 12 December 2022).

[6] Naujokaitytė, G. and Burke, F., 'NATO to launch €1B fund for high tech start-ups in dual use technologies', Science|Business, 12 April 2022. https://sciencebusiness.net/news/nato-launch-eu1b-fund-high-tech-start-ups-dual-use-technologies (accessed 12 December 2022).

[7] 'NATO Exploring Quantum Technology for Future Challenges', NATO ACT, 14 October 2022. https://www.act.nato.int/articles/nato-exploring-quantum-technology-future-challenges (accessed 12 December 2022).

[8] Reding, D. F. and Eaton, J., 'Science & Technology Trends 2020-2040', NATO Science & Technology Organization, 2020. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf (accessed 12 December 2022).

[9] Roberson, T., 'Talking about responsible quantum: Awareness is the absolute minimum … that we need to do', arXiv.org. https://doi.org/10.48550/arXiv.2112.01378 (accessed 18 October 2022).

[10] Biercuk, M. J. and Fontaine, R., 'The Leap into Quantum Technology: A Primer for National Security Professionals', War on the Rocks, 17 November 2017. https://warontherocks.com/2017/11/leap-quantum-technology-primer-national-security-professionals/ (accessed 12 December 2022).

[11] Wehner, S., Elkouss, D. and Hanson, R., 'Quantum Internet: A vision for the road ahead', Science, Vol. 362, no. 6412, 19 October 2018. https://doi.org/10.1126/science.aam9288 (accessed 12 December 2022).

[12] Young, S. D., 'Memorandum for the heads of executive departments and agencies – Migrating to Post-Quantum Cryptography', The White House's Office of Management and Budget, 18 November 2022. https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf (accessed 23 January 2023).

[13] Krelina, M., 'Quantum Technology for Military Applications', EPJ Quantum Technology 8 December 2021. https://doi.org/10.1140/epjqt/s40507-021-00113-y (accessed 18 October 2022).

[14] Daum, F., 'Quantum Radar Cost and Practical Issues', IEEE Aerospace and Electronic Systems Magazine, November 2020. https://doi.org/10.1109/MAES.2020.2982755 (accessed 28 October 2022).

[15] Travagnin, M., 'Cold Atom Interferometry for Inertial Navigation Sensors', Joint Research Centre, European Commission, 2020. https://data.europa.eu/doi/10.2760/237221 (accessed 28 October 2022).

[16] Ibid. 12.

Dr Michal Krelina

is a research scientist at the Czech Technical University in Prague, the Czech Republic, and a quantum security expert in the GOVSATCOM programme at the EUSPA (European Union Agency for the Space Programme). His original background is in high-energy theoretical particle and nuclear physics. Michal is a consultant, analyst, and strategist in quantum technology, emphasizing security and defence applications. His quantum technology research focuses on mapping quantum technology military applications, exploring quantum technology roles in future conflicts, quantum technology risk and threat assessment, and consulting for different departments of NATO and various defence and law enforcement organizations. He has a PhD in experimental nuclear physics.

Lieutenant Colonel Denis Dúbřavčík

was enlisted in the Czech Air Force in 1996. He graduated from the Brno Military Academy with a BSc in Military Rocket and Aircraft Systems and an MSc in Mechanical Engineering. He is a graduate of the Squadron Officers School at Maxwell Airbase, US. He served, among other functions, as a weapons instructor and commander of the 212th Tactical Squadron at Air Force Base Čáslav, the Czech Republic. He is a pilot and instructor on the L-159 ALCA aircraft with more than 1,500 flight hours. He is currently serving in the Assessment, Coordination, and Engagement Branch of the JAPCC as the Plans, Concepts, Development, and Vision Staff Officer.

Russian Air Force's Performance in Ukraine

Air Operations: The Fall of a Myth

By Lieutenant Colonel Rafael Ichaso Franco,
SP Air Force, JAPCC

© Andrey Suslov/Shutterstock.com

Introduction

On 24 February 2022, the world witnessed outrage over Russian missiles attacking multiple targets in Ukraine, waves of helicopters at very low altitudes in what appeared to be aerial assaults on various airports, and reports about paratrooper assaults. Convoys of armoured vehicles and trucks entered Ukrainian territory from multiple avenues. However, the world did not see the powerful Russian Aerospace Forces: the Vozdushno-Kosmicheskiye Sily (VKS). Where was the VKS?

During the first days of the Russian invasion, there were hardly any images of jet fighters. Those available were of aircraft flying at low or very low altitudes and, in many cases, later identified as Ukrainian aircraft trying to avoid the Russian Air Defence. Soon, videos of the first fighter shoot-downs, both Russian and Ukrainian, appeared mainly on social media channels. Most of them were aircraft flying at low or very low altitudes within the range of MANPADS and, of course, Ukrainian surface-to-air defence systems. The lost aircraft were not only obsolete and slow Su-25s but also powerful Su-30s, Su-34s, and Su-35s.[1]

Traditionally, the VKS has always bet on a robust surface-to-air defence to protect the land forces' advance, with aviation filling the gaps to defend Russian territory; long-range aviation and army aviation would act as flying 'artillery' as part of the offensive. However, in the last decades, VKS has heavily invested in technological improvements, such as Active Electronically Scanned Array radars, long-range air-to-air missiles, high manoeuvrability, and some stealth capabilities. These improvements reinforced the idea that the VKS was shifting its doctrine to a much more focused role of traditional air superiority, especially with the addition of the Su-30 family of fighters including the new Su-57 stealth fighter. NATO regarded Russia as a potential peer adversary and, consequently, trained and prepared its forces to face a powerful VKS with highly capable fighters aimed at achieving air supremacy. With such a high estimation of Russia's air combat capability, how is it possible that the VKS did not achieve air supremacy in Ukraine, or at least air superiority, not to mention suffer such high attrition? The explanation may be simple: the VKS's air doctrine differs from NATO's, with Russian planners still treating military aviation as mere 'flying artillery'.

The VKS has not operated as expected, and this article will address the possible reasons and the lessons identified from the Russian VKS's performance in Ukraine. This article will consider several aspects related to joint planning, integration, training, and experience. The opinions in this article are based on open-source information and will undoubtedly be refined as more information becomes available.

Potential Reasons

No Air Power in Joint Planning

Russian planners were probably contemplating a rapid and overwhelming land invasion that would not give the Ukrainian defence time to react. Therefore, a sizeable preparatory air campaign would not be helpful, as it would eliminate the element of surprise. Furthermore, after this rapid land offensive, with the subsequent fall of Kyiv, the entire country would fall and a large-scale VKS operation would not be needed. As observed, there was no preparatory air campaign, just initial attacks hours before the invasion by aircraft and cruise and ballistic missiles.

In the first days of the invasion, the VKS appeared to be effective against the Ukrainian Air Force and Air

© Shchus/Shutterstock.com

© Fasttailwind/Shutterstock.com

Russian Sukhoi Su-35S Flanker firing unguided air-to-ground rockets at Dubrovichi shooting range.

Defence.[2] However, Ukrainian military assets, such as surviving jet fighters, the Türkisch Bayraktar Unmanned Combat Aerial Vehicles (TB2 UCAV), and surface-to-air defences continued to operate without effective interference from the VKS.[3] Moreover, Ukrainian airpower, especially their TB2 UCAVs and surface-to-air defences, caused many losses to the Russian forces in this phase of the war.

A situation that got the world's attention was the approximately sixty-kilometre-long convoy of vehicles headed for Kyiv without much apparent protection against air or ground attacks. Many memes published on social media showed the supposed feelings of A-10 pilots watching the convoy in such a predicament.[4] This reflects the gross failure of Russia's operational planning, the overestimation of VKS's capability to protect the Russian ground forces, and the underestimation of the Ukrainian defenders.

'…the VKS took advantage of its technological superiority by using long-range air-to-air missiles to target Ukrainian fighters from long distances, even from Russia's mainland.'

Coordination and integration between Russian aircraft and air defence has been historically poor, especially with their Land Forces Air Defence (PVO-SV). For example, during Russia's 2008 invasion of Georgia, friendly fire between Russian forces and Russian proxy forces in Ossetia downed three out of the six Russian aircraft lost.[5] Russia has limited Identification, Friend, or Foe (IFF) capabilities, poor procedural controls, and reduced joint training between the VKS and PVO-SV; therefore, the probability of procedural errors and fratricide is high.[6] These facts, supplemented by the partial and gradual recovery of Ukrainian surface-to-air capabilities after initial losses, left the Russian ground forces bereft of air support.

The lack of training (especially joint training) and planning integration probably fostered mistrust between the different branches of the Russian forces.[7] Russia's ground-based air defence remains a severe threat, even to its own aviation.[8]

Lack of Effective Adaptability

As stated before, the Ukrainian surface-to-air defence gradually reconstituted certain capabilities once Russia refocused on the land war. To avoid the threat, Russia's aircraft were forced to perform entire missions from friendly territory with standoff munitions or low-altitude tactics, thus becoming exposed to Ukraine's and even their own MANPADS.[9]

One month after the invasion, once the Ukrainian defence was reorganized and had effectively engaged the enemy forces, Russia finally reacted and boosted its flights by almost fifty percent. Throughout July and August, Russia further increased its air presence over Ukraine, especially after Ukraine's retaliatory strikes into the Saky airport, the main Naval Aviation base in Crimea.[10, 11]

'In the last decades, VKS has heavily invested in technological improvements […]. These improvements reinforced the idea that the VKS was shifting its doctrine to a much more focused role of traditional air superiority, especially with the addition of the new Su-57 stealth fighter.'

However, due to the high attrition, the VKS reacted and adjusted its tactics by reducing the number of flights over Ukrainian-controlled territory and operating mainly from Belarus, Crimea, or the Russian mainland, especially at night, with strategic bombers carrying cruise missiles and flying at high altitudes to improve endurance. Additionally, and with sure success, the VKS took advantage of its technological superiority by using long-range air-to-air missiles to target Ukrainian fighters from long distances, even from Russia's mainland.[12]

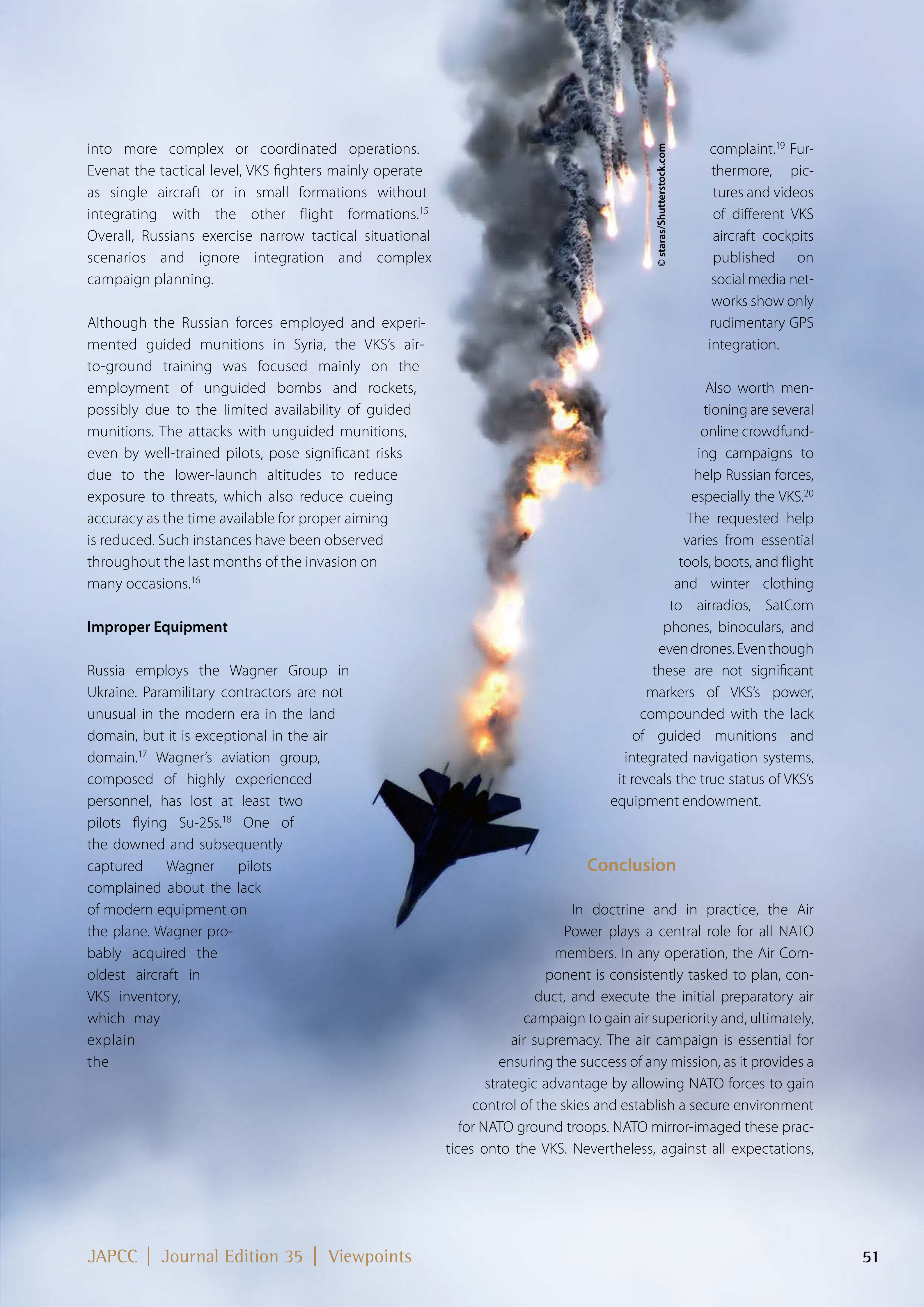
The decision to operate mainly outside of Ukraine's territory led to a drastic decrease in downed aircraft. However, the Russian Army Aviation had to continue flying in support of their land forces, thus operating close to or inside Ukrainian-controlled territory. Yet even when operating under the umbrella of Russian-based air defence, the attrition rate for Army Aviation continued to increase.[13]

With this adaptation, the VKS aimed to reduce losses while supporting the invasion. However, the lack of guided munitions and platforms capable of striking at night negatively impacted the precision of their attacks and, thus, the support to their ground troops.

Inadequate Experience and Training

The VKS does have combat experience. It has been involved for years in the Syrian Civil War, Crimea, and Georgia. However, they executed mainly air-to-ground missions under insignificant threats from air defence fighters or surface-to-air systems, in contrast to the current scenario in Ukraine. Furthermore, recent statistics released by the Russia's Ministry of Defence revealed that, in the last years, VKS fighter pilots averaged around 100–120 flight hours, military-transport pilots around 120–140 flight hours, and long-range aviation crews and army aviation pilots approximately 100 flight hours annually.[14] By comparison, all are well below NATO proficiency standards.

Additionally, this data only reveals the flight hours rather than the quality of training. VKS exercises vary in size and tactical challenges, including night flights, very high or very low-altitude flights, adverse weather conditions, or operating from alternate airfields. However, these individually challenging tasks were apparently rehearsed without integrating


© staras/Shutterstock.com

into more complex or coordinated operations. Evenat the tactical level, VKS fighters mainly operate as single aircraft or in small formations without integrating with the other flight formations.[15] Overall, Russians exercise narrow tactical situational scenarios and ignore integration and complex campaign planning.

Although the Russian forces employed and experimented guided munitions in Syria, the VKS's air-to-ground training was focused mainly on the employment of unguided bombs and rockets, possibly due to the limited availability of guided munitions. The attacks with unguided munitions, even by well-trained pilots, pose significant risks due to the lower-launch altitudes to reduce exposure to threats, which also reduce cueing accuracy as the time available for proper aiming is reduced. Such instances have been observed throughout the last months of the invasion on many occasions.[16]

Improper Equipment

Russia employs the Wagner Group in Ukraine. Paramilitary contractors are not unusual in the modern era in the land domain, but it is exceptional in the air domain.[17] Wagner's aviation group, composed of highly experienced personnel, has lost at least two pilots flying Su-25s.[18] One of the downed and subsequently captured Wagner pilots complained about the lack of modern equipment on the plane. Wagner probably acquired the oldest aircraft in VKS inventory, which may explain the complaint.[19] Furthermore, pictures and videos of different VKS aircraft cockpits published on social media networks show only rudimentary GPS integration.

Also worth mentioning are several online crowdfunding campaigns to help Russian forces, especially the VKS.[20] The requested help varies from essential tools, boots, and flight and winter clothing to airradios, SatCom phones, binoculars, and even drones. Even though these are not significant markers of VKS's power, compounded with the lack of guided munitions and integrated navigation systems, it reveals the true status of VKS's equipment endowment.

Conclusion

In doctrine and in practice, the Air Power plays a central role for all NATO members. In any operation, the Air Component is consistently tasked to plan, conduct, and execute the initial preparatory air campaign to gain air superiority and, ultimately, air supremacy. The air campaign is essential for ensuring the success of any mission, as it provides a strategic advantage by allowing NATO forces to gain control of the skies and establish a secure environment for NATO ground troops. NATO mirror-imaged these practices onto the VKS. Nevertheless, against all expectations, the VKS employed traditional tactics and was unable to perform complex operations; instead, it operated as an extension of the Army's artillery. Consequently, the surprisingly 'low' presence and performance of Russian Air Power in the Ukraine war has been a shock to everyone. Yet, as the conflict progresses the situation continues to evolve.

The possible causes for the VKS's apparent reluctance to run large composite air operations with large numbers of tactical aircraft are manifold, from fears of suffering excessive losses, insufficient training, and improper equipment to poor planning and lack of coordination capabilities at both the strategic and tactical levels. However, the actual explanation can also be that the VKS's doctrine differs from NATO's. Russian planners may deem military aviation as highly responsive flying artillery while relying on surface-to-air assets to provide air defence, with aviation filling the possible gaps. One conclusion seems clear: without air superiority the ground troops remain quite exposed, gravely hampering the land campaign.

Notwithstanding the VKS's inability to secure the air domain, there are valuable lessons to learn from Russia's performance in the war in Ukraine. Despite Russia's lacklustre performance in the air domain, NATO should not draw the wrong conclusions. Fleets can be rebuilt and rearmed, the doctrine will evolve, and commanders can learn the lessons of undervaluing Air Power. For NATO, the Ukraine experience validates the prominent role of Air Power, both offensively and defensively, and the need to continue to modernize and retain a high state of readiness. ●

[1] Mitzer, S., et al., 'List Of Aircraft Losses During The 2022 Russian Invasion Of Ukraine', Oryx, 2022. https://www.oryxspioenkop.com/2022/03/list-of-aircraft-losses-during-2022.html (accessed 24 November 2022).

[2] Bronk, J., Reynolds, N. and Watling, J., 'The Russian Air War and Ukrainian Requirements for Air Defence'. https://rusi.org/explore-our-research/publications/special-resources/russian-air-war-and-ukrainian-requirements-air-defence (accessed 11 November 2022).

[3] Ibid.

[4] Demerly, T., 'A-10 pilots explain why stopping Russia's 40-mile convoy near Kyiv would be a very dangerous mission', The Aviationist. https://www.businessinsider.com/a10-pilots-stopping-russian-convoy-in-ukraine-would-be-dangerous-2022-3 (accessed 3 November 2022).

[5] Solovyov, D., 'Friendly fire downed Russia jets in Georgia-report', Reuters, 2009. https://www.reuters.com/article/idUSL8262192 (accessed 18 October 2022).

[6] Withington, T., 'Defending Mother Russia's Skies', RUSI. https://www.rusi.org/explore-our-research/publications/commentary/defending-mother-russias-skies/ (accessed 2 September 2022).

[7] Chotiner, I., 'Is the Russian Military a paper tiger?', The New Yorker. https://www.newyorker.com/news/q-and-a/is-the-russian-military-a-paper-tiger (accessed 2 November 2022).

[8] Ibid. 6.

[9] Ibid.

[10] Sands, L., 'Saky airfield: Ukraine claims Crimea blasts responsibility after denial', BBC News. https://www.bbc.com/news/world-europe-62821044 (accessed 5 November 2022).

[11] Kholodnova, A., 'Russia has increased aviation activity around Ukraine. On average, there were almost 150 departures per day'. https://babel.ua/en/news/83014-russia-has-increased-aviation-activity-around-ukraine-on-average-there-were-almost-150-departures-per-day (accessed 21 November 2022).

[12] Ibid.

[13] Lamothe, D., 'Russian air force action increases despite flood of antiaircraft missiles into Ukraine', The Washington Post. https://www.washingtonpost.com/national-security/2022/03/22/ukraine-russia-air-force/ (accessed 15 November 2022).

[14] https://hushkit.net/2021/03/23/everything-you-always-wanted-to-know-russian-air-power-but-were-afraid-to-ask-with-guy-plopsky-part-1-how-good-is-russian-air-force-training/ (accessed 15 November 2022).

[15] Ibid. 2.

[16] Ibid. 14.

[17] 'What is Russia's Wagner Group of mercenaries in Ukraine?', BBC News. https://www.bbc.com/news/world-60947877 (accessed 11 November 2022).

[18] Roscoe, M., 'Captured Wagner Group Pilot says: Russian aircraft have big problems with navigation', EuroWeekly News. https://euroweeklynews.com/2022/06/21/captured-wagner-group-pilot-says-russian-aircraft-have-big-problems-with-navigation/ (accessed 25 November 2022).

[19] Altman, H., '63-Year-Old Retired Russian Fighter Pilot Shot Down In Su-25 Over Ukraine', The Warzone. https://www.thedrive.com/the-war-zone/63-year-old-retired-russian-fighter-pilot-shot-down-in-su-25-over-ukraine (accessed 25 November 2022).

[20] Trevithick, J., ''Crowdfunded' Aid For Russian Jet Squadron Looks Like Someone Raided A Home Depot', The Warzone. https://www.thedrive.com/the-war-zone/crowdfunded-aid-for-russian-jet-squadron-looks-like-someone-raided-a-home-depot (accessed 16 November 2022).

Lieutenant Colonel Rafael Ichaso Franco

joined the Spanish Air Force in 1993. He was assigned to the 15th Fighter Wing from 1998–2005 and 2007–2009, and in between was an Instructor Pilot in the Fighter Weapons School, 23rd Wing. In 2009, he was assigned as Flying Instructor at the Air Force Academy. From 2013 to 2016, he served in NATO HQ AIRCOM, Ramstein, Evaluations Division as Flying Forces Project Officer and evaluator. He attended the Armed Forces Joint Staff Course in 2017. Before his assignment to the JAPCC, he served in the Spanish Air Combat Command.

He has more than 2700 hours flown in C-101, F-5, and EF-18.

© NicoElNino/Shutterstock.com

The Impact of Commercial Space in Times of Conflict

From a Fortuitous Boost to a Potential Solution

By Major Arda Ayan, TÜ Air Force, JAPCC
By Major Brian Ladd, US Space Force, JAPCC

Commercial Space Steps in the Spotlight

In today's connected world, communication and information offered by and through Space capabilities impact people's everyday lives. Russia's war of aggression against Ukraine has highlighted what may happen if existing networks are denied. The harsh reality of a 'day without Space' was never entirely obvious before. In response to Russia's invasion, the Western world lost no time authorizing several economic sanctions, including those that degraded the Russian Space programme. Russia, one of the major competitors in the so-called 'Space Race' since its inception, responded in the Space domain by threatening to destroy cooperation on the International Space Station (ISS), suspending Soyuz rocket launches, and jamming Global Positioning System (GPS) satellite signals. Space-capable nations and Alliance members have utilized military and governmental systems to mitigate Russia's actions in the Space domain so far. However, few could have foreseen that, just sixty years after the launch of the first commercial Space mission, Telstar 1, in 1962, a nation's essential wartime requirements may depend on a tweeted request to a private company for internet services.

In response to Russia's war of aggression, the commercial Space enterprise stepped in to cover the gap with communications, remote sensing, and launch capabilities. Aided by commercial Space, Ukraine transitioned from terrestrial to Space-based communication in a matter of days, despite expectations that it would take months, even years. This article will provide a brief history of cooperation and interdependence in the Space domain, describe how commercial Space responded to the events in Ukraine, and finally develop some observations and recommendations

Satellite image © 2023 Maxar Technologies

for both non-NATO nations and Alliance members to incorporate commercial Space. The war in Ukraine has provided essential lessons on how countries outside NATO territory, with limited or no Space capabilities, can leverage commercial Space to overcome the dependency on terrestrial communication systems and disruption of Space data, products, and services (DPS) to succeed on the battlefield.

Cooperation and Interdependence

The first Space collaboration occurred in 1975 when the United States (US) and the Soviet Union shared a ride on the Soviet Soyuz capsule in the first crewed international Space mission. Relations strengthened in 1993 when the US and Russia officially became full partners in the ISS. The joint missions ensured the presence of at least one crew member on board the station from each country at all times.[1] Also, the European Space Agency (ESA) and the Russian Federal Space Agency entered long-term cooperation in 2005, with Russia providing Soyuz launch capability from the ESA spaceport in French Guiana.[2] This spaceport acts as the primary launch location for ESA, affording multiple orbits.

The US-Russia relationship soured after Russia's 2014 invasion of Crimea. The US determined that Russia posed a strategic threat and, therefore, directed the Space industry to develop a dedicated Space launch programme, ceased scientific and industrial cooperation with the Russian Space industry, and denied export licenses for high-technology items that could aid Russian military capabilities. On the other front, ESA and most Alliance members maintained the Soyuz launches with Russia, after the invasion of Crimea, without taking any actions to develop alternatives.

Over the last several years, Russia's overall share in the international Space-launch market diminished due to a combination of factors. These include the rise of private Space-launch competitors lowering the launch costs, the legacy Space industry's failure to innovate or expand beyond its ageing Space-launch service fleet, and the sanctions imposed following Russia's 2014 annexation of Crimea. Although Russia remains one of the top three launching countries (averaging 14 to 24 percent of annual orbital launches, between 2017 and 2021, compared to 20 to 32 percent for the US during the same period), most Russian on-orbit assets rely on outdated technology. Moreover, most Russian Space assets launched in the twenty-first century either

Russian convoy north of Kyiv, 28 February 2022.

depended on Western technology or used service modules made in Russia which were outfitted with cutting-edge payloads produced by foreign manufacturers. Post-Crimea sanctions gravely undermined the status quo for the Russian Space industry.

Key Events Related to Ukraine War

Space is essential for Alliance's deterrence and defence posture; therefore, it is valuable to detail events in the fifth domain related to Ukraine. Even though the war started on 24 February, several earlier hostile actions by Russia, such as anti-satellite tests and jamming attempts over Europe, were already indicators. The following are highlights of the key events observed in the Space domain before and during the invasion of Ukraine, which affected the western world.

- In November 2021, Russia successfully demonstrated its ability to destroy a satellite in Low Earth Orbit (LEO), resulting in over 1,500 pieces of orbital debris. This event represented a warning to western nations and commercial companies which might oppose Russia.
- Since December 2021, Ukraine observed continuous and increasing GPS signal interference.[3]
- On 4 February 2022, during the Russia-China summit, the parties agreed there would be no forbidden areas of cooperation.[4] China had no objections over the war in Ukraine, and Roscosmos, the Russian Space Agency, sought China's support to mitigate western sanctions with components and partnership in Space missions.
- The US intelligence agencies more than doubled their procurement of commercial electro-optical images, which were further disseminated to the Ukrainian defence.[5]
- The US formally blamed Russia for a cyberattack on Viasat's KA-SAT satellite internet network, in late February. US-based Viasat provides KA-SAT broadband internet access services in Europe through a network of distributors. Viasat's customers also include the US government.[6]
- On 26 February, Roscosmos halted cooperation with Europe on Soyuz launches from the ESA's launch facility in French Guiana in response to European sanctions for Russia's invasion of Ukraine.[7] This caused at least ten planned launches to find alternate launch solutions resulting in substantial delays of months or even years.[8]
- Russia announced its intent to withdraw from the ISS programme after 2024 and use all resources to develop a new Russian Space station later in this decade.[9]

© Valeriy Georgian/Shutterstock.com

Deployed Starlink terminal supporting on-going combat operations in Bakhmut, Ukraine, 13 September 2022.

- On 11 April, the US confirmed that the Russian GPS jamming efforts interfered with civilian and military airborne operations in Ukraine.[10]
- The ESA cut ties with Russia by cancelling their plans to cooperate on a series of lunar missions and officially ended cooperation with Russia on the ExoMars mission on 12 July 2022.[11]

Russia's dependence on Western payloads developed into a severe need and, as a result of the West's export ban on high-tech goods, Russia is now unable to complete the satellites currently under construction. Meanwhile, Russia's Space capabilities are degrading while Ukraine is expanding its access through commercial providers, improving its relative standing to Russia, and showcasing how commercial enterprises can make a critical wartime impact.

Commercial Game Changers

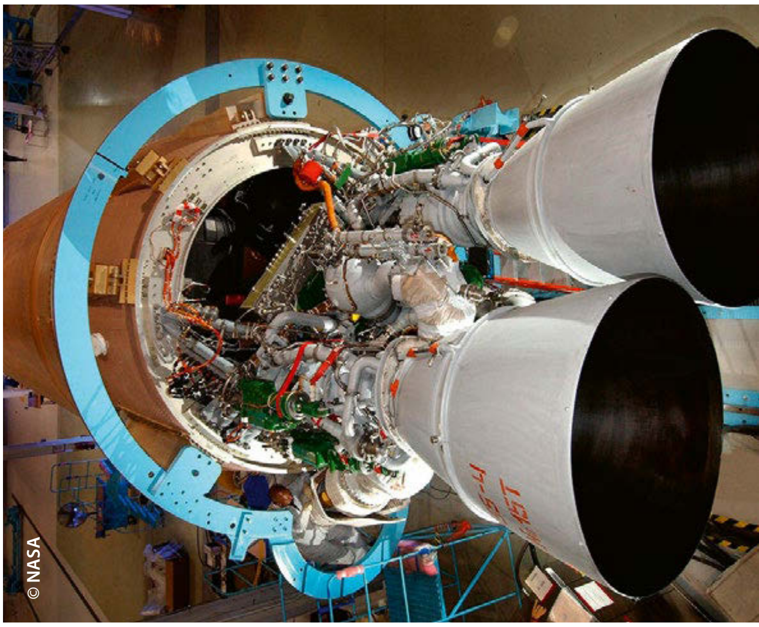
Without its own satellite capabilities, Ukraine has benefitted enormously from an unprecedented amount of remote sensing data from external sources, which provided near real-time information on Russian wartime actions. Many western technological advancements have expanded the amount of high-quality, near-real-time satellite imagery available to private citizens, businesses, and military intelligence. Prior to Russia's invasion, the commercial Space industry had primarily focused on developing closer ties to nations with dedicated Space programmes or filling the growing needs of civilian populations for high-speed internet, entertainment (TV/Radio), and weather forecasts. Now, a new norm has emerged to provide Space services to those nations with limited to no Space capabilities. SpaceX has a significant share in making 'commercial Space' a buzzword with its support to Ukraine, proof that commercial support can directly influence the course of the conflict. SpaceX's ability to deliver high-speed communications and internet access in war-torn parts of Ukraine is the best example of the new norm.

In addition to SpaceX's support with high-speed broadband communications, several other commercial satellite imagery providers, such as Maxar, BlackSky, and Planet, have collectively changed the game for non-Space-faring Ukraine. Russia damaged Ukraine's cellular network in the early stages of the conflict, which made it difficult for Ukrainian troops and leaders to maintain effective command and control (C2). The Ukraine minister of digital transformation reached out on Twitter with an urgent request to Starlink services, a satellite internet constellation of over 3,000 high-speed wideband communication satellites in Low Earth Orbit, to fill the gap. SpaceX first adjusted the orbital configuration of its huge constellation to improve coverage of the region. Then, SpaceX had delivered over 10,000 ground terminals for Ukrainian defence forces and for private usage. Now, approximately 150,000 Ukrainians utilize the service daily as their primary form of high-speed communications.[12]

In March 2022, Russia employed their considerable offensive cyber forces and electronic warfare systems to degrade the Starlink system. SpaceX demonstrated its agility and resilience, and a day later its engineers patched the code and thwarted the attack.[13] Since then, Russian hackers have increased their futile attempts to take down Starlink.

Ukraine's drone warfare campaign demonstrates Starlink's role as a battlefield equalizer. Ukraine has deployed their drone force for real-time intelligence to report precise enemy locations for artillery, anti-tank, and kamikaze attacks. Starlink has been instrumental in Ukraine's counteroffensive by providing clear communications. A short outage on 30 September emphasized Starlink's importance in this war. At the time, Ukrainian commanders had to halt the attack until services resumed. To date, Starlink has donated roughly 20,000 Starlink terminals in support of Ukraine's defence, but the capability it delivers is fragile. The operating cost for the Starlink systems in Ukraine reached $100 million by the end of 2022, a cost that SpaceX claims as unsustainable without investment from the US government, raising the prospect of losing such a vital enabler.[14] While Starlink is not singly responsible for Ukraine's success, it is hard to argue that Ukraine's success so far would have been possible without it.

In the early days of the invasion, intelligence on Russian troop movements was critical for defence. As Ukraine did not achieve air dominance and lacked Space-based ISR assets, it direly needed intelligence support and resilient and secure communications. Apart from the already mentioned civilian Space companies, a new group called Space Industry for Ukraine (SIFU) – representing 18 Space companies – recognized Ukraine's urgent needs and worked directly with Ukraine's defence forces to provide support.[15] SIFU provided the necessary combination of electro-optical and synthetic aperture radar imagery required to locate enemy forces in the early stages of the conflict regardless of the weather conditions and time of image acquisition. The SIFU data now provides information for battlefield assessments during the ongoing counterattack.


© NASA

The overt involvement of the commercial Space enterprise on the side of a combatant is not without risk. Russia recently demonstrated its ability to target and destroy a satellite operating in the same orbit as Starlink and commercial remote sensing satellites. Additionally, a Russian official threatened that 'Quasi-civilian infrastructure may be a legitimate target for a retaliatory strike'.[16] Despite such threats, the commercial Space industry continues to valiantly support the Ukraine government.

Observations and Recommendations

In the 1990s, the West became over-reliant on Russian Space lift. NATO's Space-capable nations should invest more in domestic launch programmes and increase their support to well-established commercial launch providers in lieu of Russian rockets.

© Kamal photography/Shutterstock.com

SpaceX demonstrated exceptional built-in agility by immediately modifying the Starlink constellation's orbital configuration following Ukraine's request and rapidly responding to Russian cyber and electronic warfare threats. Space-capable NATO nations should amend national decision-making processes and procurement procedures to develop and procure those Space capabilities providing increased options to respond to new threats.

The commercial Space industry demonstrated its effectiveness in communications and remote sensing by rapidly adapting to the conflict. Non-NATO nations without mature Space programmes should invest in establishing networks with commercial companies to provide Space-based DPS and ensure Space support to operations in the event of a crisis.

The commercial Space industry can support the Alliance by augmenting currently available national Space capabilities. Regardless of their Space programmes' capacity, NATO nations should analyse the current war to identify possible gaps and evaluate if commercial industry can fill these gaps or provide redundancy in the Space domain for enhanced resiliency.

Conclusion

The evolution in the uses of Space and rapid advances in Space technology have created new opportunities, risks, vulnerabilities, and potential threats. While Space was first developed for peaceful purposes, it can also be used for aggression. Satellites can be hacked, jammed, or weaponized and kinetic or non-kinetic anti-satellite weapons could cripple communications and affect the Alliance's ability to operate.

The threat of Russian aggression is now more than ever a reality, increasingly felt by the former Soviet bloc nations. Countries outside of NATO that cannot directly benefit from NATO's collective defence umbrella, and do not have a robust Space capability, should look towards the successful role played by the commercial Space providers in this war and should prioritize developing relationships prior to a future conflict. The lessons learned are not limited to non-NATO countries but are helpful to the Alliance too. The Alliance needs to work directly with industry to analyse and implement the best practices and to develop tactics, techniques, and procedures to respond to Space and counter-Space threats such as those encountered by SpaceX during the war.

The support for Ukraine's territorial integrity, independence and sovereignty will undoubtedly continue in the coming period. The conflict in Ukraine has shown the world that a nation presented with almost impossible odds can leverage commercial Space capabilities as a great equalizer and a potential solution for all nations in future conflicts. The current situation in Ukraine incorporates the success stories of a nation with strong determination and highlights the need for cooperation and solidarity in the sphere of Space. With these 'powers from the heavens', any nation's odds in the face of aggression increase dramatically. ●

'A nation that risks death for its life and freedom will never be defeated.' ***Mustafa Kemal Atatürk***

1. https://time.com/6220640/us-russian-space-station-collaboration (accessed 10 October 2022).
2. https://www.esa.int/Enabling_Support/Space_Transportation/International_cooperation #:~:text=The%20agreement%20between%20ESA%20and,Guiana%20as%20a%20 launch%20base (accessed 14 November 2022).
3. https://www.he360.com/hawkeye-360-signal-detection-reveals-gps-interference-in-ukraine/ (accessed 12 September 2022).
4. https://www.reuters.com/world/china/moscow-beijing-partnership-has-no-limits-2022-02-04/ (accessed 16 November 2022).
5. https://spacenews.com/as-russia-prepared-to-invade-u-s-government-and-satellite-imagery-suppliers-teamed-up-to-help-ukraine/ (accessed 27 September 2022).
6. https://spacenews.com/as-us-blames-russia-for-ka-sat-hack-starlink-sees-growing-threat/ (accessed 17 November 2022).
7. https://spacenews.com/russia-halts-soyuz-launches-from-french-guiana/ (accessed 2 September 2022).
8. https://spacenews.com/soyuz-embargo-strands-satellites-with-limited-launch-options/ (accessed 22 November 2022).
9. https://www.space.com/news/live/russia-ukraine-invasion-space-impacts-updates (accessed 8 September 2022).
10. Ibid.
11. https://edition.cnn.com/2022/07/12/world/exomars-terminated-russia-european-space-agency-scn/index.html (accessed 10 August 2022).
12. https://www.aa.com.tr/en/russia-ukraine-war/150-000-people-in-ukraine-communicating-daily-via-spacexs-starlink/2578402 (accessed 18 November 2022).
13. https://www.dailymail.co.uk/sciencetech/article-10744069/Elon-Musks-SpaceX-Starlink-rapidly-fought-Russian-jamming-attack-Ukraine.html (accessed 24 November 2022).
14. https://edition.cnn.com/2022/10/13/politics/elon-musk-spacex-starlink-ukraine/index.html (accessed 20 October 2022).
15. https://www.space.com/space-industry-for-ukraine-companies-humanitarian-aid (accessed 1 September 2022).
16. https://www.reuters.com/article/ukraine-crisis-russia-satellites-idAFKBN2RN07K (accessed 28 November 2022).

Major Arda Ayan

graduated from the Turkish Air Force Academy in 2005 with a Bachelor's degree in Computer Engineering and was stationed as a SHORAD (Short Range Air Defence) officer at the 6th Main Jet Base Anti-Aircraft Battalion Command. Following his Master's degree in Space Sciences, in 2014, he was appointed as a satellite mission planning officer in the Reconnaissance Satellite Battalion Command within the Air Force Intelligence Department. In charge of Göktürk-1 and Göktürk-2 remote sensing satellites, he took on the duties of Satellite Control Officer and Satellite Operators' Supervisor, respectively, in the military Earth observation satellite command and control centre in Türkiye. Since August 2021, he has been serving as Space SME at the JAPCC.

Major Brian Ladd

graduated from Bowling Green State University in 2005 with a Bachelor's degree in History and received his commission by AFROTC. His first tour was at the 4th Space Operations Squadron at Schriever AFB in Colorado Springs, CO, where he was a Satellite Operator of the MILSTAR communications system. His other operational tour was as the Liaison Officer at RAF Fylingdales Strategic Missile Warning Radar. He has completed many Space Staff assignments at Joint Base Pearl Harbor-Hickam, Vandenberg AFB, and Offutt AFB. He transitioned to the US Space Force in October 2020. Since June 2021, he has been serving as the Chief of Cyber and Space Readiness at the JAPCC.

© whiteMocca/Shutterstock.com

Insights from the Ukrainian Cyber Battlefield

Is the Private Sector a Game Changer?

By Lieutenant Colonel Antonios Chochtoulas, GR Air Force, JAPCC

Introduction

Russia's invasion of Ukraine on 24 February shocked the entire world and created the most significant security crisis in Europe since the Second World War. Along with traditional kinetic warfare, Russia has conducted large-scale cyber operations in Ukraine before and after the invasion. Since the start of the invasion, at least six different state-linked hacker groups have conducted nearly 240 cyber operations against Ukrainian civilian and military targets. By examining Russia's cyber offensive, we can draw insights on cyber resiliency from Ukraine's response.

Malicious software combined with malicious tools and advanced hacking techniques were used against Ukraine's public infrastructure, universities, and the private sector. Advanced Persistent Threat (APT) groups linked with Russian intelligence agencies are the actors behind this ongoing campaign. A cyber-attacker is designated as an APT when it attacks a network or a system in a targeted manner over a long period of time. Typically, this actor is well trained and often linked to or even controlled by a state.

Despite its reputation in cyber warfare, Russia did not manage to deliver decisive cyber strikes against

Ukraine's Information Technology (IT) infrastructure. The attacker's methods and tools were previously effective, but this time the outcome differed from what many expected. In addition to reduced effectiveness, the volume of Russian cyberattacks was less than defence and cyber experts expected.

Ukraine's success so far in defending against Russia's cyber offensive can be attributed to three elements: the government's preparations in the years before the war, cyber defence assistance from NATO and EU countries, and the involvement of private companies like Microsoft, Amazon, and SpaceX, which offered commercial solutions like digital cloud services and Starlink which provided critical communications infrastructure.

This article is based on publicly available information. Its purpose is to present, in short, the major cyber incidents of this war and to provide insights on the Ukrainian government's successful defence, with support from foreign countries and private companies, against Russian cyberattacks. It will further identify the lessons learned and provide recommendations to NATO and non-NATO countries on how to enhance their cyber resilience.

Historical Background

Russia has systematically used cyberattacks against Ukraine. Hackers linked with Russian intelligence agencies have conducted cyber offensive operations in Ukraine at least since Russia's 2014 annexation of Crimea. Their targets included government sites, universities, power companies, the banking sector, and other critical infrastructure. In those early days, Russia aimed to cause public frustration and weaken their political adversaries in the Ukrainian political system. In some cases, the attackers deployed malicious software never used before, making Ukraine a testbed for new cyber weapons.[1]

Starting in 2014, the pro-Russian hacktivist[2] group *CyberBerkut*, linked to the foreign military intelligence agency of the General Staff of the Russian Armed Forces, commonly known as the GRU, compromised the Ukrainian central election system by installing malware in the system to undermine trust in the election process and cause political instability.[3] In addition, on the day of the elections, *CyberBerkut* launched a massive Distributed Denial-of-Service (DDoS) attack campaign to delay the final election tally and discredit the election process in the eyes of the public. The attack was unsuccessful, as it did not delegitimize the winner. Ukrainian cybersecurity personnel removed the malware from the system on time, preventing it from releasing false results. However, the final vote tally was delayed for two hours.

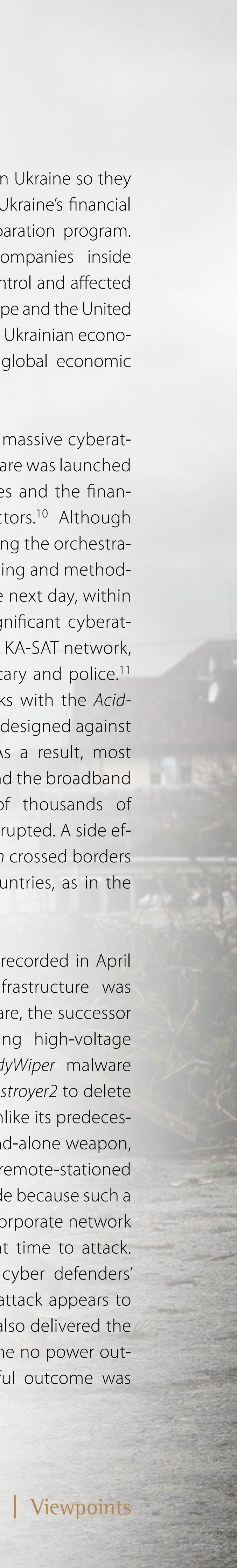
'Since the start of the invasion, at least six different state-linked hacker groups have conducted nearly 240 cyber operations against Ukrainian civilian and military targets.'

In 2015, *Sandworm*, an APT group linked to the GRU, managed to conduct the first-ever publicly acknowledged cyberattack on a power grid.[4] The attackers managed to remotely gain control of the Supervisory Control and Data Acquisition (SCADA) systems in three Ukrainian energy distribution companies and disrupt the power supply in an equal number of Western Ukraine provinces. About 225,000 people were left without electricity for up to six hours.[5] In 2016, almost a year after the previous attack, the Ukrainian energy grid was targeted again. This time the attackers deployed the *Industroyer* malware, which became the biggest threat to industrial control systems since Stuxnet.[6] *Industroyer* was used to remotely gain control of electricity substation switches and circuit breakers. This was accomplished by installing a backdoor into the target system that exploited the protocols used by Industrial Control Systems (ICS) throughout the critical infrastructure. This cyberattack affected a large part of Ukraine's capital and was attributed to the *Electrum* APT group, which is directly associated with *Sandworm*.[7]

The worst cyber incident in Ukraine occurred in 2017, when the Russian APT group *Telebots*, also linked to *Sandworm*, deployed the destructive *NotPetya* malware against Ukraine's financial and energy sectors. *NotPetya* took its name from its resemblance to the ransomware *Petya*, which struck in early 2016 and extorted victims for the key to unlock their files. This time, *NotPetya*, regardless of whether the victim paid, sabotaged 10 % of the computers in Ukraine so they could not boot.[8] It spread all over Ukraine's financial sector through a popular tax preparation program. Although the attack targeted companies inside Ukraine, the malware got out of control and affected multinational companies across Europe and the United States (US). The exact impact on the Ukrainian economy is unclear, but the estimated global economic losses exceeded $10 billion.[9]

The day before Russia's invasion, a massive cyberattack using the *HermeticWiper* malware was launched on Ukraine's government machines and the financial, aviation, IT, and energy sectors.[10] Although there is no hard evidence connecting the orchestrators of this attack to Russia, the timing and methodology used strongly suggest it. The next day, within hours of the invasion, another significant cyberattack took place against the Viasat's KA-SAT network, widely used by the Ukrainian military and police.[11] The attack combined DDoS attacks with the *AcidRain* malware, which was specially designed against telecommunication equipment. As a result, most Viasat modems were inoperable and the broadband internet service for hundreds of thousands of Ukrainians and the military was disrupted. A side effect of this attack was that *AcidRain* crossed borders and impacted other European countries, as in the *NotPetya* case.[12]

The following major incident was recorded in April 2022, when Ukraine's energy infrastructure was attacked by the *Industroyer2* malware, the successor of *Industroyer*, specifically targeting high-voltage electrical substations.[13] The *CaddyWiper* malware was also deployed along with *Industroyer2* to delete the traces of the attack. Notably, unlike its predecessor, *Industroyer2* was used as a stand-alone weapon, requiring no intervention from a remote-stationed operator. This is a significant upgrade because such a weapon could be implanted in a corporate network and stay idle, waiting for the right time to attack. Such behaviour complicates the cyber defenders' role in preventing an attack. This attack appears to be the work of Sandworm, which also delivered the 2016 *Industroyer* attack, but this time no power outages were reported. The successful outcome was



due to the immediate response of Ukraine's cyber defence authorities, who have gained significant experience in recent years, and the assistance from Microsoft and ESET.[14]

Collaboration with the Private Sector

The Ukrainian government and armed forces overcame the initial shock of the invasion and successfully addressed these non-kinetic attacks. Ukraine's Computer Emergency Response Team (CERT-UA) worked with private companies to minimize the effects of Russia's cyber offensive and keep all the critical systems running with minimal interruption. A week

© Kutsenko Volodymyr/Shutterstock.com

© Peshkova/Shutterstock.com

before the invasion, when war seemed imminent, the Ukrainian government got worried about the security of their data and searched for ways to protect it. Until then, Ukrainian law required particular government and public sector data to be stored on servers physically located in the country. The government changed the law, allowing sensitive government and private sector data to be transferred to cloud servers outside the country.[15] Next, under pressure from the events, the Ukrainian government made a public call for help. Amazon Web Services and Microsoft, the world's biggest cloud service providers, were among the first companies to respond to that call.

In the following days and weeks, these companies provided help, support, and the means (IT equipment and data centres outside Ukraine) for data migration from across all sectors of Ukraine. Thus, vast amounts of data were moved to the cloud. Most Ukrainian ministries, universities, and private companies have benefitted from this collaboration.[16] In effect, Ukraine traded data sovereignty for improved cyber defence against Russian kinetic and non-kinetic attacks. Due to this strategy, not only was the Ukrainian government able to function properly through today, but the population was able to continue a relatively normal online life during the war: banks remained open, universities could still provide education, most public services were available, etc. All of these significantly impacted the nation's morale and certainly helped sustain Ukraine's resistance to the invasion.

Another interesting aspect was the cooperation of CERT-UA with private cybersecurity companies to monitor and identify potential cyberattacks. Even before the 2022 *Industroyer2* attack, researchers from Microsoft[17] and ESET[18] were remotely monitoring the networks in Ukraine and performing real-time data analysis to identify potential malicious activity. In addition, during Ukraine's cyber operations the first confirmed utilization of Artificial Intelligence (AI) was recorded. According to Microsoft president Brad Smith, Ukraine successfully used AI to detect, identify, and defeat a Russian cyberattack without human intervention.[19] This has definitely contributed to the Ukrainian success.

Resilient and secure communications are essential for any military operation. After the cyberattack against Viasat's satellite communications infrastructure the Ukrainian military was left without satellite communications. This situation undermined the country's entire defence. The gap was quickly filled by another US private company, SpaceX, which offered Ukraine free access to its Starlink satellite internet services. Ukraine quickly adopted the service as a replacement for the compromised government military communications system, which has proven extremely useful and successful. The system has also proven its resilience against signal jamming, as SpaceX's CEO Elon Musk stated recently.[20]

Considerations

The lack of verifiable information about successful Russian cyberattacks during the war complicates

© Blackboard/Shutterstock.com

the picture. Ukraine is likely not publicly revealing the full extent of the impacts of Russian cyber offensives on its infrastructure, lest Russia has a clear picture of the efficiency of its cyber operations. Nevertheless, the last Russian drone campaign from October against the Ukrainian energy infrastructure may signify that Russia could not use a cyberattack towards that goal. On the other hand, Russia might be keeping some of its cyber capabilities in reserve for future operations or is already working on a new yet undisclosed cyber offensive. In either case, Ukraine's years of preparation seem to have paid off.

Data is at the core of the information age, and events like the 2017 *NotPetya* cyberattack have shown that cyberspace does not have ordinary borders. Collateral damage from cyberattacks can occur far beyond the original target. Malicious software might quickly spread across countries and affect government and business data worldwide. The public and private sectors cannot overlook the potential damage of such a crisis. New strategies that could enhance resilience against such attacks must be implemented. As the Ukrainian example shows, the benefits of data migration to out-of-country clouds may overcome disadvantages such as loss of data sovereignty and may be a solution. Another consideration is that big corporate data centres that provide cloud services are more difficult for APT groups to compromise than local ones.

The Alliance is confronted by cyber, space, hybrid, and other asymmetric threats and the malicious use of Emerging and Disruptive Technologies (EDT).[21] EDTs, such as AI and space-based broadband internet services, are not only expected to be game changers in future warfare but have already been tested and proved on the battlefield. Global competition becomes more intense as EDTs change the character of conflict and acquire strategic importance. However, notwithstanding the opportunities brought to the fore by EDTs, they also threaten the Alliance. By leveraging emerging technologies, adversaries could achieve technological primacy and, through that, influence the outcome on the battlefield.

Conclusion

Following the 2022 NATO Madrid Summit, the Alliance decided to use national assets to build and exercise a rapid response cyber capability to respond in the event of a significant cyberattack. Building on the lessons learned from the war in Ukraine, the Alliance should develop new capabilities in the fields of data storage and cyber resilience. Such developments could only happen with the collaboration of the private sector, and the EU and other political entities could participate and benefit too. Data migration should also be considered for the military domains, although most military data and communications are classified. In the future, quantum cryptography could allow the exchange of classified data in a military cloud that could be geographically distributed across allied countries' data centres.

On the other hand, as private companies become part of the conflict, nations should take the proper measures to protect them in cyberspace. National authorities should provide the proper framework for cybersecurity cooperation with the private sector and work closely to address cyberattacks effectively. Furthermore, national laws and policies should increase resources to investigate, disrupt, and prosecute malicious cyber activity, and impose higher penalties for cybercrime and insider enablers. Nations should also leverage diplomatic and economic tools against nations that provide cover for malicious cyber actors. Nations should also dedicate additional funding and set higher standards for strengthening SCADA and other vulnerable industry systems against cyber threats.

The Alliance continues to face distinct threats from all strategic directions and must adapt to the evolving threats in cyberspace. NATO and its allies require strong and resilient cyber defence to fulfil their core tasks of deterrence and defence, crisis prevention and management, and cooperative security.[22] As Ukraine's cyber defence shows, collaboration with the private sector is a proven method to defend our networks and operations against adversaries indiscriminately wielding sophisticated cyber weapons. Having in mind that 'resilience is a national responsibility and a collective commitment', we should enhance the Alliance's cyber resilience through nationally-developed goals and capabilities to achieve Alliance's objectives.[23]

[1] https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/ (accessed 18 October 2022).

[2] Derived from combining the words 'Hack' and 'Activism', hacktivism is the act of hacking, or breaking into a computer system, for politically or socially motivated purposes.

[3] https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed (accessed 18 October 2022).

[4] https://www.cisa.gov/uscert/ncas/alerts/aa22-110a (accessed 20 October 2022).

[5] Whitehead, D.E. et al., 'Ukraine cyber-induced power outage: Analysis and practical mitigation strategies', 70th Annual Conference for Protective Relay Engineers (CPRE), 2017, pp. 1–8.

[6] https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/ (accessed 19 October 2022).

[7] https://www.gov.uk/government/news/uk-exposes-series-of-russian-cyber-attacks-against-olympic-and-paralympic-games (accessed 31 October 2022).

[8] https://www.eset.com/us/about/newsroom/corporate-blog/petya-ransomware-what-we-know-now/?utm_source=welivesecurity.com&utm_medium=referral&utm_campaign=autotagging&utm_content=ukraine-crisis-digital-security-resource-center&utm_term=en (accessed 1 November 2022).

[9] Greenberg, A., 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History', Wired, 22 August 2018.

[10] https://cyberlaw.ccdcoe.org/wiki/HermeticWiper_malware_attack_(2022) (accessed 4 November 2022).

[11] https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview (accessed 4 November 2022).

[12] https://www.reuters.com/world/satellite-outage-caused-huge-loss-communications-wars-outset-ukrainian-official-2022-03-15/ (accessed 7 November 2022).

[13] https://cert.gov.ua/article/39518 (accessed 7 November 2022).

[14] https://cip.gov.ua/en/news/viktor-zhora-vzyav-uchast-u-profilnii-konferenciyi-z-kiberbezpeki-black-hat-usa-2022-u-las-vegasi (accessed 15 November 2022).

[15] https://www.aboutamazon.com/news/aws/safeguarding-ukraines-data-to-preserve-its-present-and-build-its-future (accessed 10 October 2022).

[16] https://www.infosecurity-magazine.com/interviews/interview-microsoft-migrating-data/ (accessed 10 October 2022).

[17] 'Defending Ukraine: Early Lessons from the Cyber War', Microsoft, 2022.

[18] ESET Threat Report, T1, 2022.

[19] https://www.ekathimerini.com/opinion/interviews/1197775/building-defenses-for-cyberwarfare/ (accessed 14 November 2022).

[20] https://spacenews.com/russian-invasion-of-ukraine-exposes-cybersecurity-threat-to-commercial-satellites/ (accessed 4 November 2022).

[21] Madrid Summit Declaration, NATO, 2022.

[22] NATO, Cyber defence. https://www.nato.int/cps/en/natohq/topics_78170.htm (accessed 17 November 2022).

[23] NATO 2022 Strategic Concept. https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/220629-factsheet-strategic-concept-en.pdf (accessed 17 November 2022).

Lieutenant Colonel Antonios Chochtoulas

graduated from the Hellenic Air Force (HAF) Academy in 1999. He holds a Master of Science in Computer Science, and his subject matter expertise is Cybersecurity and Systems Administration. He initially served as a programmer and, after that, as a Database and System Administrator of HAF's proprietary Logistics Information System. Throughout his career in HAF, he was involved in several Cybersecurity projects and participated in Cyber military exercises. Currently, he is the Cyberspace SME at the JAPCC.

Targeting with Due Regard to Cultural Property

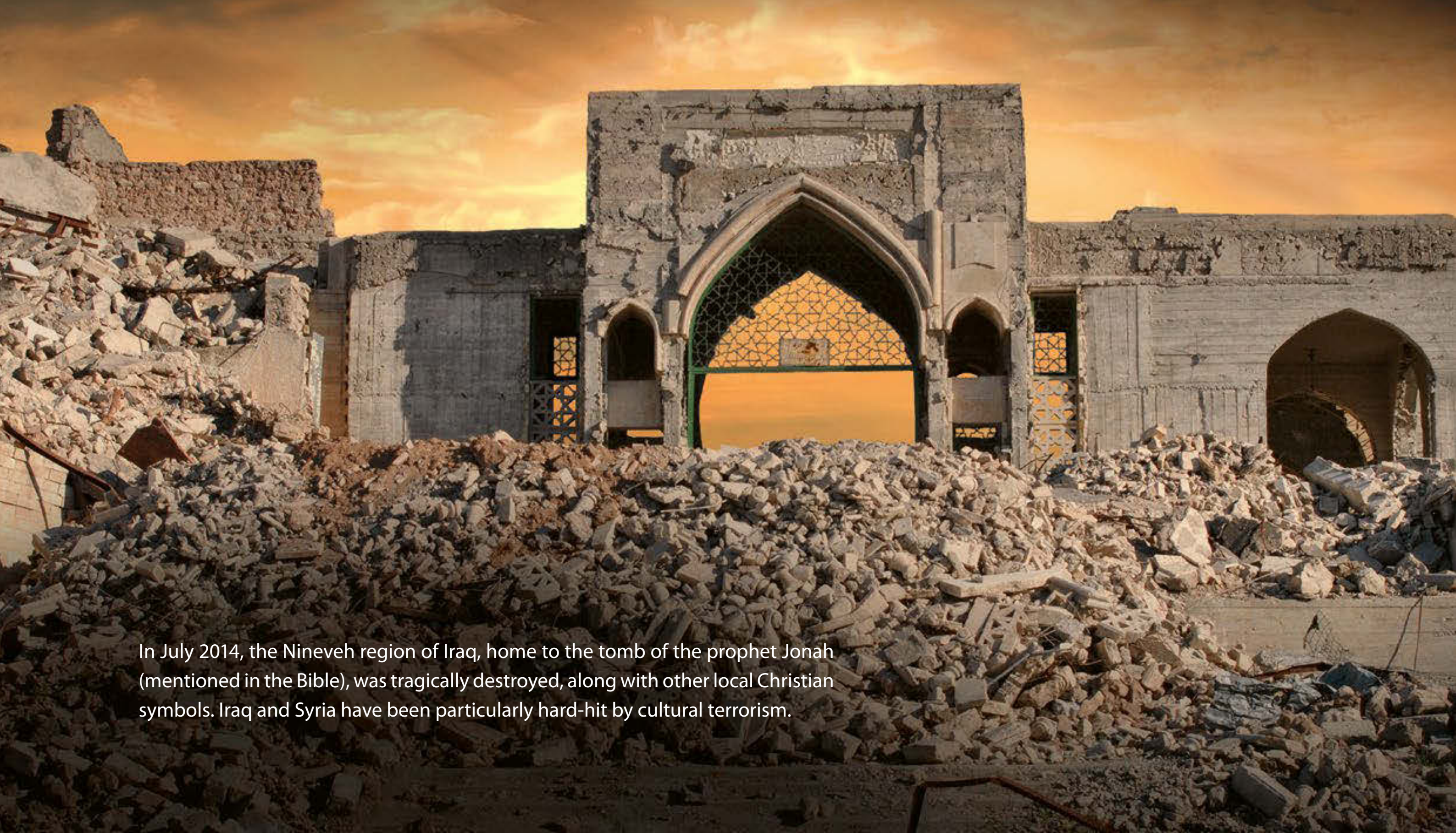
By Mr Adam Jux, BA, Civilian Targeting Consultant
By Prof Adrian Parker, BSc, DPhil, FSA, FRGS, FRAI, VR

Introduction

Damage and destruction of Cultural Property (CP) is a regrettable feature of warfare throughout history. The reasons range from the incidental, such as careless indifference, collateral damage coincident to legitimate acts, or lack of knowledge of CP, to the intentional, such as indiscriminate use of wide-area effects weapons or the intentional erasure of cultural sites to undermine an adversary's resolve. Even when conducted under the banner of military necessity, the damage is often irreversible. Destruction, damage, or misappropriation of CP as an attack on a sector of society is an affront to the laws of war and can have far-reaching consequences, acting as a driver of conflict.

Many will know of the 2014 film 'The Monuments Men', based on the true story of a team who sought to preserve priceless pieces of art from destruction or theft during the Second World War. Whilst their perseverance will live on in history, the value placed on CP in conflict is not limited to artworks and paintings. CP includes 'the tangible, visual and totemic cultural expression of a community, a society, a nation and, ultimately, of humankind'.[1] It is thus an expression of cultural identity and community cohesion.

Protecting CP during armed conflict is a legally mandated military task, and is applicable to all phases of military activities and operations. Cultural Property Protection (CPP) requirements fall under the framework



In July 2014, the Nineveh region of Iraq, home to the tomb of the prophet Jonah (mentioned in the Bible), was tragically destroyed, along with other local Christian symbols. Iraq and Syria have been particularly hard-hit by cultural terrorism.

© Lena Ha/Shutterstock.com

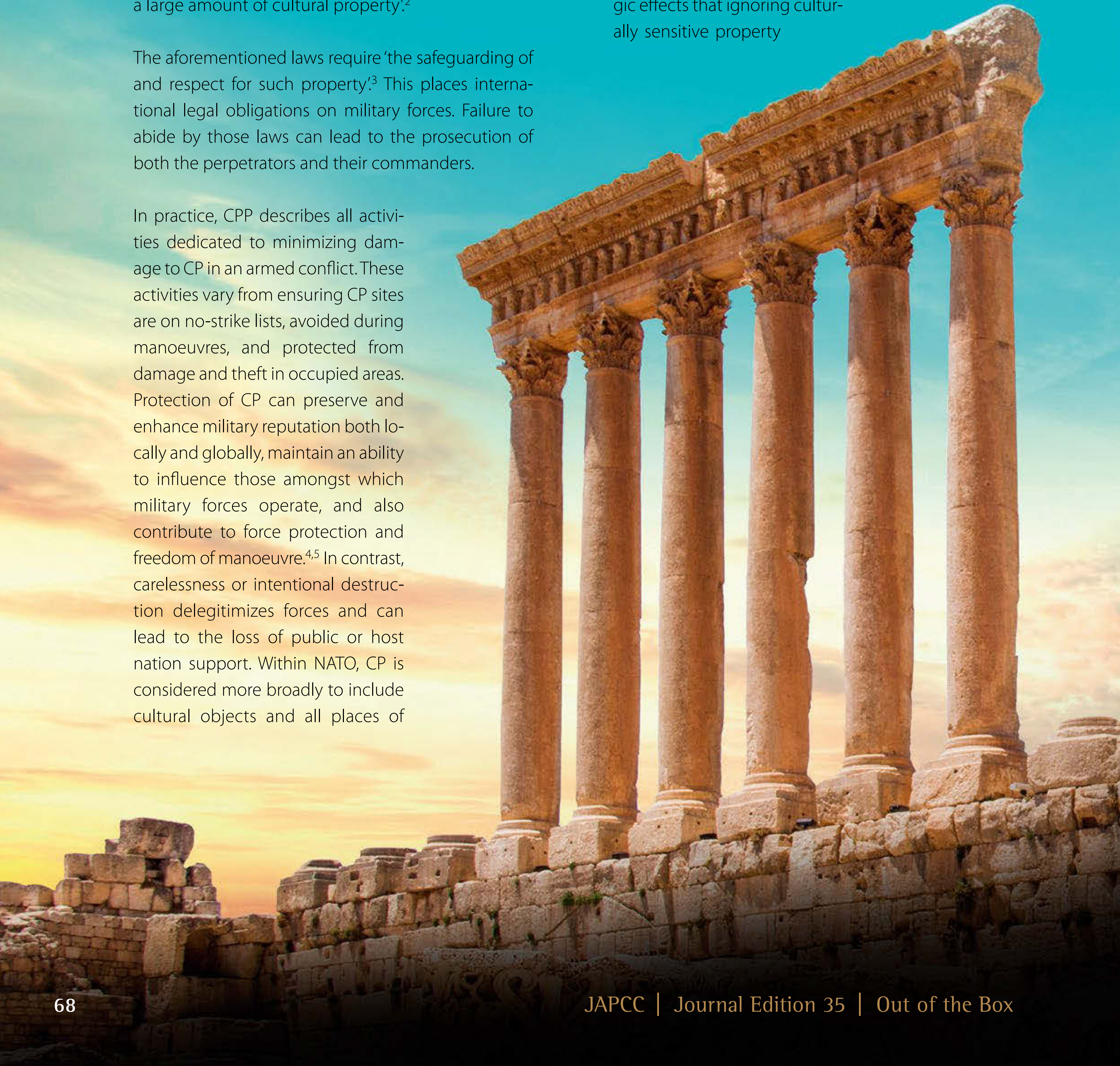
of the International Law of Armed Conflict (LOAC). Specific CPP obligations are embedded in the 1954 Hague Convention for the Protection of Cultural Property in the event of armed conflict (the 'Hague Convention'); its two additional protocols (from 1954 and 1999) clarify and complement the original treaty.

In international law, CP is defined as 'movable or immovable property of great importance to the cultural heritage of every people, such as monuments of architecture, art, or history…buildings whose main and effective purpose is to preserve or exhibit the movable cultural property…and centres containing a large amount of cultural property'.[2]

The aforementioned laws require 'the safeguarding of and respect for such property'.[3] This places international legal obligations on military forces. Failure to abide by those laws can lead to the prosecution of both the perpetrators and their commanders.

In practice, CPP describes all activities dedicated to minimizing damage to CP in an armed conflict. These activities vary from ensuring CP sites are on no-strike lists, avoided during manoeuvres, and protected from damage and theft in occupied areas. Protection of CP can preserve and enhance military reputation both locally and globally, maintain an ability to influence those amongst which military forces operate, and also contribute to force protection and freedom of manoeuvre.[4,5] In contrast, carelessness or intentional destruction delegitimizes forces and can lead to the loss of public or host nation support. Within NATO, CP is considered more broadly to include cultural objects and all places of worship. NATO thus defines CP as moveable or immovable property that enjoys recognition and protection under customary international law and, as applicable, treaty law.[6]

The wider international community should be assured that NATO, along with its allies and partners and aided governmental and non-governmental actors, has procedures in place for the respect and consideration of CPP at all stages of a conflict, should such an occasion arise. This paper serves to address the importance of minimizing collateral effects on CP during times of conflict and the strategic effects that ignoring culturally sensitive property



can bring to bear. It will include a precis of targeting procedure regarding CP, examples of military units engaged in CPP and how those units bring CPP into exercises, as well as recommendations for the future.

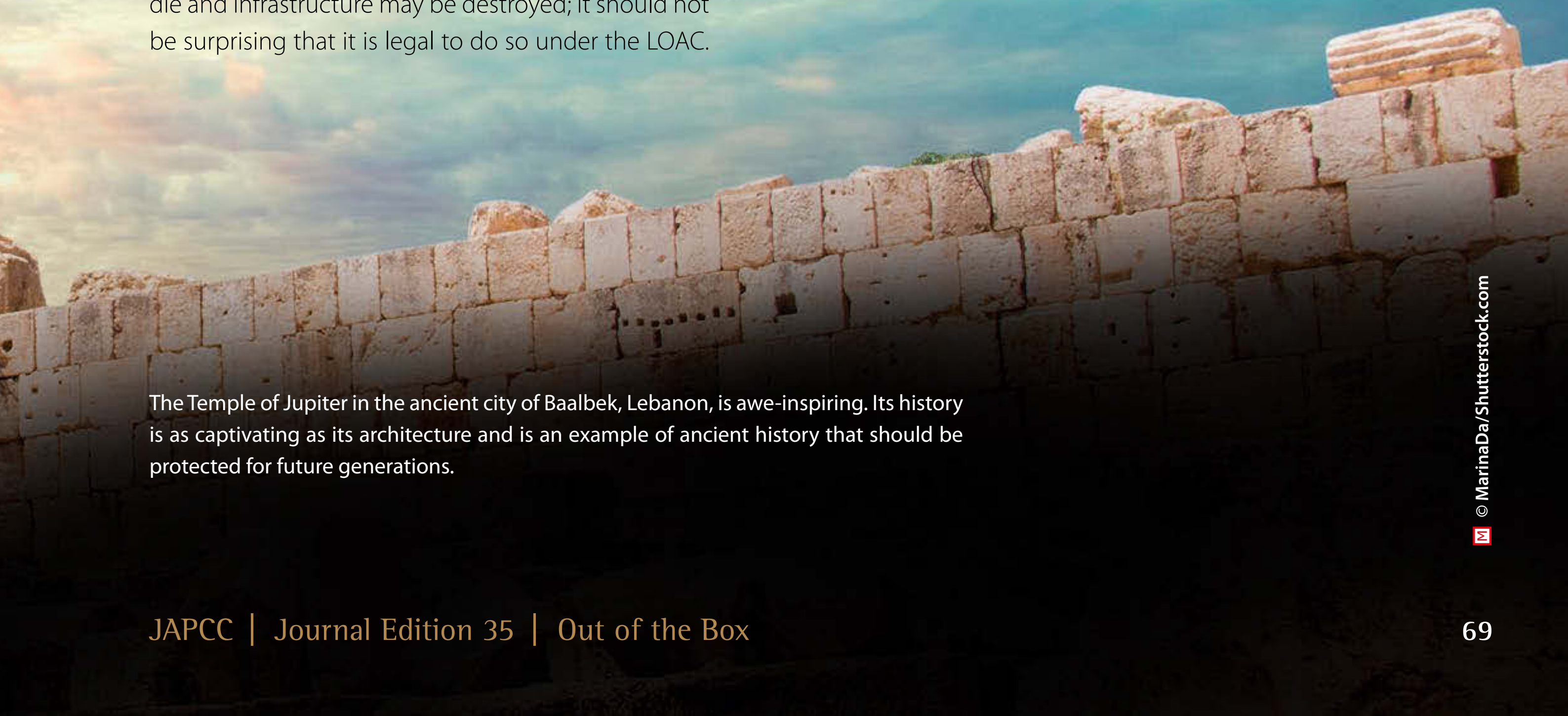
Targeting Procedures and CPP

Precision weapons have revolutionized modern warfare, but are beyond many combatants' technical capabilities, and, when present, are always in limited supply. This results in significant risks to CP. If CP sites are not considered in the operational planning processes, the potential for accidental damage increases significantly. Collateral damage to CP may be the result of wilful disregard (legitimate or illegitimate) or error, but in either case can yield a propaganda opportunity for the adversary. Damage to CP, whether lawful or not, can affect reputation, the ability to influence communities within the area of operations, and may lead to reprisal attacks that further escalate tensions, spread violence, and affect force protection.

NATO conducts targeting through a set of repeatable and measurable procedures that allow for the lawful targeting of an adversary. Should NATO (or any combatant) not act lawfully, it may be brought before the International Criminal Court according to established procedures. All sides must be accountable for their actions, as the means to inflict damage or destruction carries with it great responsibility; NATO conducts its actions transparently.

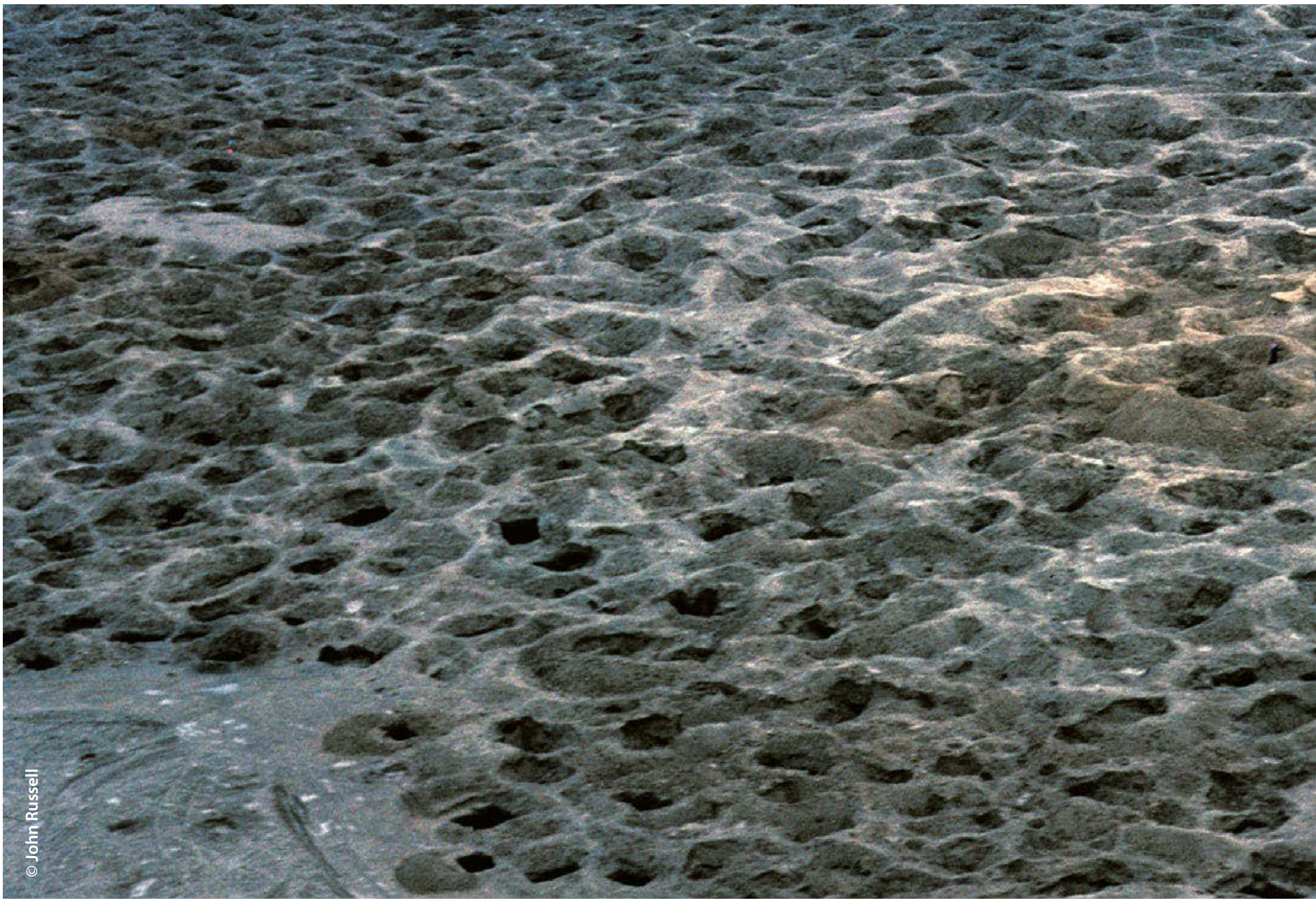
Conflicts involve committing acts where people may die and infrastructure may be destroyed; it should not be surprising that it is legal to do so under the LOAC. Military forces would not be able to operate without the legal means to carry out their tasks and missions. As such, the LOAC is shaped by the principles of necessity, distinction, humanity, and proportionality no less than any other aspect of the targeting methodology. The consideration of CP during the targeting process is both an international legal and moral obligation, and a practical necessity. Apart from the No-Strike List and the Restricted Target List, CP should also be included in the Collateral Damage Estimation (CDE), in which targeteers, lawyers, commanders, and others assess the magnitude of expected collateral damage for planned strikes. Contrary to common belief, CDE procedures exist for the protection of civilian personnel and infrastructure. A rigorous target development process is essential to enable commanders to make informed determinations of necessity, proportionality, and collateral damage risk when prosecuting targets on or near CP.

NATO not only acts transparently and has good measures to avoid unnecessary damage, but it goes further to liaise with specialized organizations that focus on collateral concerns that could cause unnecessary pain, suffering, or loss of support from a host nation. Examples may include liaising with local civilian organizations responsible for safeguarding CP, deconfliction with Non-Governmental Organizations (NGOs) conducting humanitarian flights into a conflict zone, or, as this article will examine next, with organizations such as the Blue Shield, an NGO specialized in CPP.



The Temple of Jupiter in the ancient city of Baalbek, Lebanon, is awe-inspiring. Its history is as captivating as its architecture and is an example of ancient history that should be protected for future generations.

© MarinaDa/Shutterstock.com



© John Russell

Extant CPP Actors

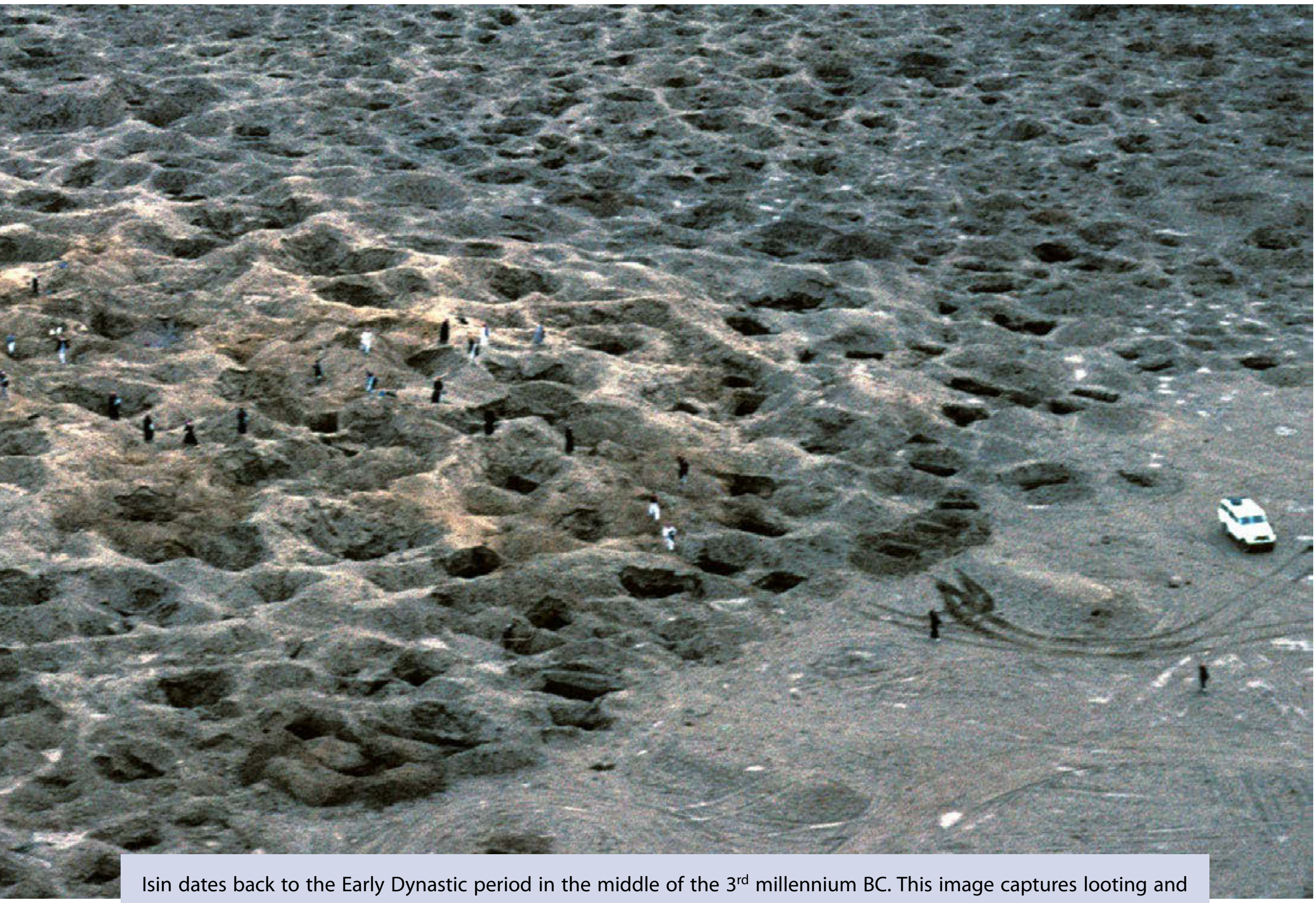
UK Reserve Forces CPP Unit

The United Kingdom (UK) military established a CPP unit in 2018, comprised of specialized reservists with expertise in CPP, such as building surveying and conservation, artefact conservation, cultural heritage, archaeology, etc. Their role is to deliver the CPP capability and provide support to exercises, targeting, and operational planning, training for the armed forces, advice to commanders and staffs, and coordination with civilian authorities responsible for CP safeguarding of in the event of an armed conflict.[7]

This unit is embedded in the 77th Brigade's Outreach Group that also enables operations by facilitating civil-military cooperation between the force, non-military actors, and the civil environment. It also acts as the defence coordinating authority for support to the delivery of human security operational outputs and contributes to cross-government stabilization and reconstruction efforts.[8]

US 10th Mountain Division (Light Infantry)

Since September 2016, the United States (US) has also sought to form partnerships with CPP actors. Specifically, the 10th Mountain Division has combined with the Cultural Resources Team (CRT) at Fort Drum, New York, to enhance training to include CP aspects. For example, 'when soldiers reported that Iraqi insurgents were using headstones as firing points, the CRT constructed culturally reminiscent replica cemeteries and added them to urban sprawl and urban terrain training sites on Fort Drum so that dealing with such



Isin dates back to the Early Dynastic period in the middle of the 3rd millennium BC. This image captures looting and destruction pits carried out by Iraqis in the archaeological site of Isin during 2003. The pits completely destroyed the site.

scenarios could be practiced. And, after the global news media featured reports of damage to the ancient city of Babylon by US and Polish forces in 2004, the CRT constructed mock ruins in the training areas to offer field training opportunities to identify, avoid, and respect ancient places as well as sites regarded as sacred by indigenous peoples during the course of military operations.'[9]

CPP capability further developed through the US Army Civil Affairs & Psychological Operations Command (Airborne), to increase knowledge and understanding in protecting and preserving CP in armed conflict. The 10th Mountain Division has developed a training programme for all Army Reserve Civil Affairs soldiers (Course 38G/6V Heritage and Preservation) that provides support to areas including Joint Intelligence Preparation of the Operational Environment, as well as training on the practicalities of CPP in a conflict zone with hazards, forensic documentation, and handling of damaged materials.

Blue Shield International

Blue Shield International is 'committed to the protection of the world's cultural property, and is concerned with protecting the tangible and intangible cultural and natural heritage in the event of armed conflict, natural- or human-made disaster.'[10] Why should a military organization liaise with Blue Shield or other similar NGOs? Why not just avoid cultural sites?

As you would expect of a modern military force, NATO identifies any aspects within an operational area that might be controversial, sensitive, or protected. Local knowledge and advice from experts in the field is essential. The advice provided by Blue Shield may avoid second or third-order effects, such as the loss of public support. Regardless of the legitimacy of strikes under LOAC, reprisals from the local population for damaged or destroyed CP have the potential to foment protests and civil unrest. Furthermore, the damage and unrest are easily exploited by adversary media and could harm Alliance's reputation and affect mission success. Just because you can, does not necessarily mean you should.

'Precision weapons…are beyond many combatants' technical capabilities, and, when present, are always in limited supply. This results in significant risks to Cultural Property.'

In the past, Blue Shield was responsible for advising and training military personnel in CPP aspects, such as evacuation, refugee resettlement, and damage assessment. In tactical training scenarios, Blue Shield hires local actors to portray citizens with information, in varying forms of distress, and highlight that cultural heritage preservation is actually about protecting the domestic culture and people.

Protecting Objects of Cultural Significance

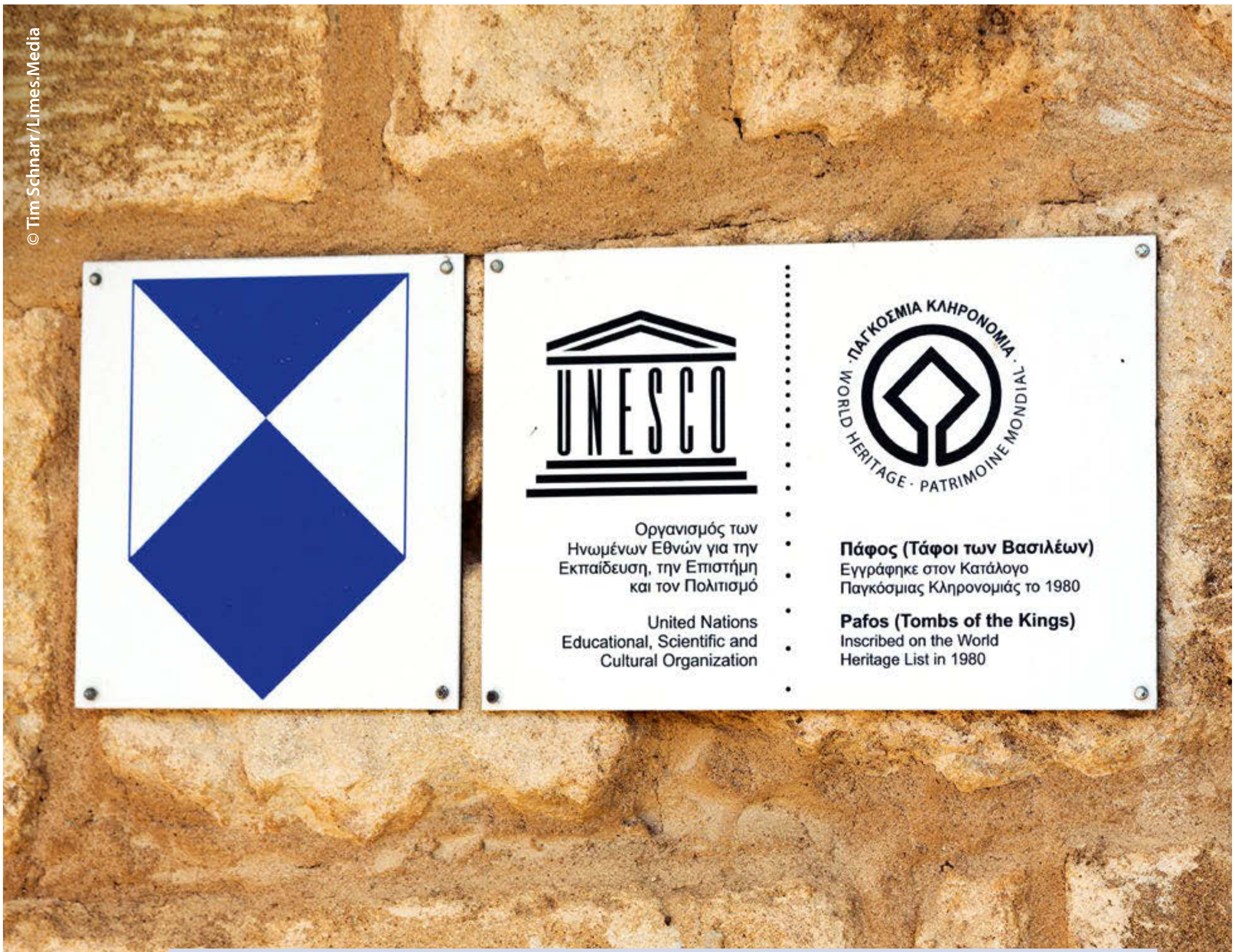
NATO goes to great lengths to identify all locations of CP wherever it operates. This includes places of worship, e.g. mosques and churches, monuments of architecture, art, or history, and buildings whose main purpose is to preserve or exhibit movable CP. It is also no secret that NATO has policies in place to protect such locations of cultural significance as a force multiplier. Regrettably, organized crime and other combatants have exploited these policies by hiding in and operating in the vicinity of CP with the expectation that NATO would not target them.

In general, targeting CP is prohibited.[11] However, under LOAC, there is an exception for military necessity, wherein such locations may be targeted under circumstances that suspend their protective status. For example, CP may be targeted if the enemy occupies it, thereby making it a legitimate military target. The target then may be struck if there is 'no feasible alternative to obtaining a similar military advantage' and if at the time of the attack the destruction, capture, or neutralization offers 'a definite military advantage'.[12]

NATO boards target through a process that ensures all aspects of a potential strike are valid and accountable from a legal, strategic, political, and intelligence perspective. In such forums, all significant aspects of any potential target are highlighted either by the host nation representatives or experts on gender, CP, STRATCOM, etc. In this best available – yet still imperfect – way, commanders make the delicate decisions balancing operational necessity and the imperative to preserve the lives of friendly forces. After all, we cannot put the value of property above that of human life. That said, if there is an option to preserve both, then knowing the cultural significance will aid commanders in their decision-making process.

In their book, 'Just War, Ethics in Modern Warfare', the authors explain that 'we must not do things, however legitimate in themselves, if in our honest and considered opinion the good they achieve is likely to be outweighed by the harm they inflict on those who ought not to be harmed'.[13] Thus, targeting a legitimate military objective should prohibit causing disproportionate damage to CP; the benefit of the attack must outweigh the loss.

Proportionality is one of the most subjective and unclear criteria to prove from a legal perspective. There are two aspects, namely: the hard-to-identify second-order effects and the unclear amount of gain from a military perspective in destroying an asset sheltered within a protected space. Proportionality does not mean that a threat can be ignored. If destroying it prematurely ends a conflict or potentially saves lives, is it then justified? There will always be adverse media highlighting controversial decisions made in conflict, but the transparent processes described helps ensure due diligence when making difficult decisions.



© Tim Schnart/Limes.Media

Recognized protected infrastructure markings like this example in Cyprus are found all over the world.

CP in NATO Exercises

How do we ensure the continuation of due regard towards CP in NATO? NATO's Joint Warfare Centre (JWC) is the primary unit for exercising and certifying the Alliance's capability to conduct all aspects of offensive and defensive operations. In recent years, the JWC modified training scenarios to include gender and cultural aspects to create more challenging cultural dilemmas for exercise participants.

The inclusion of CPP and gender have since been taken forward in major NATO exercises. Exercise Steadfast Jackal 2021 witnessed modern, real-world dilemmas relating to historical tribal cross-border conflicts, in austere conditions, outside NATO territory, and included matriarchal gender injects and protection of historical tribal locations for consideration within the targeting process. The exercise was well received, notably for leading the training audience outside of its comfort zone compared to previous large-scale exercises that treated limited resources as the primary challenge. Within this scenario, key leader engagement was paramount in identifying those cultural and strategic dilemmas that might otherwise have rendered the Alliance's presence abroad untenable.

Recommendations

Commanders at every level should seriously consider all aspects of CPP, and acknowledge the second and third-order effects that collateral damage to CP might bring. Utilizing expert advice in areas requiring unique perspectives would extensively aid and enhance the decision-making process.

Headquarters and commanders should embrace NGOs and invite them to contribute to the creation of detailed databases with locations of cultural significance. It is also in the interests of any civil organization vested in protecting CP to engage with the military to ensure it is protected. This is a symbiotic relationship for the greater good.

Conclusion

Numerous initiatives over recent years have enhanced the means by which NATO allies conduct themselves in conflict. Quite rightly, all organizations should strive to test and adjust their procedures and be the best at their professions. As we evolve with technological advances, so too we must perpetually review our processes to ensure we have all the information required to make informed decisions.

Recognizing CPP as a force multiplier highlights the value of avoiding potential strategic complications due to ill-advised tactical actions during conflict. For legal and moral reasons combatants must do everything possible to protect cultural property. ●

1. Joint Service Publication, 'Human Security in Defence (JSP 985)', vol. 1, UK Ministry of Defence, December 2021.
2. 'Convention on the Protection of Cultural Property in the Event of Armed Conflict with Regulations for the Execution of the Convention', art. 1, the Hague, 14 May 1954.
3. Ibid., art. 2.
4. Ibid. 1.
5. Civil-Military Cooperation Centre of Excellence (CCOE), 'Cultural Property Protection Makes Sense', 2020.
6. Bi-Strategic Command Directive 086-005, 'Implementing Cultural Property Protection in NATO and NATO-led operations and missions', SH/J9/CL/SG/TT001345.
7. UK Army Website. https://www.army.mod.uk/who-we-are/formations-divisions-brigades/6th-united-kingdom-division/77-brigade/groups/ (accessed 29 September 2022).
8. Ibid.
9. International Humanitarian Law. https://ihl-in-action.icrc.org/case-study/united-states-training-military-personnel-protection-cultural-heritage (accessed 29 September 2022).
10. Blue Shield International. https://theblueshield.org/about-us/who-we-are/ (accessed 29 September 2022).
11. Ibid. 2, art. 4(1).
12. 'Second Protocol to the Hague Convention of 1954 for the Protection of Cultural Property in the Event of Armed Conflict', 1999, art. 1(f), 6(a).
13. Guthrie, C. and Quinlan, M., 'Just War. The Just War Tradition: Ethics in Modern Warfare', London: Bloomsbury, 2007.

Mr Adam T. Jux

is a retired Royal Air Force Officer who served in the Royal Australian Air Force and the Australian Army over his 27 years of military experience. He is a qualified targeteer and has worked in the discipline for the last 14 years, including on operations. He has instructed in targeting and collateral damage estimation and has mentored targeting at the Joint and Component levels. He has published a number of articles and contributed to white paper research regarding targeting in general and its interaction with intelligence and other disciplines. He is currently working as a civilian targeting consultant for NATO's Joint Warfare Centre in Stavanger, Norway, under contract for Calian Europe AS.

Prof Adrian Parker

is a Royal Air Force Reserve Officer serving in the UK Cultural Property Protection Unit. The CPPU is a Defence capability established to ensure that cultural property is protected from damage and looting, to provide advice, training, and support to operational planning processes, and can investigate, record, and report cultural property issues from any area of operations. In his civilian profession, he is an academic (professor) specializing in geoarchaeology, climate change, and heritage protection and management.

© 2021 Black Salmon/Shutterstock.com

Enhancing NATO Air and Space Power in an Age of Global Competition

A Review of the JAPCC's Joint Air and Space Power Conference 2022

By Colonel Thomas Schroll, Conference Director, GE Air Force, JAPCC

Introduction

'Our world is contested and unpredictable'. 'Pervasive instability' and 'strategic competition define our broader security environment'. The challenges and 'threats we face are global and interconnected'. Overall, 'the Euro-Atlantic area is not at Peace'. This is how NATO's newest Strategic Concept, endorsed at the Madrid Summit, describes the current security environment.

The intent of the Joint Air and Space Power Conference 2022 and its overarching theme 'Enhancing NATO Air and Space Power in an Age of Global Competition' was to broaden our view beyond the wars we currently see and take into account the whole range of global security and defence challenges we face. As usual, the conference offered a forum to leaders and experts on defence from national and international staffs and headquarters, from industry and academia, to consider and discuss the development of our defence capabilities and how we build and operate our forces across all domains.

Together with a three hundred-strong audience, our two distinguished keynote speakers and the panellists explored the conference theme along four main questions: What is global competition and what are the implications for our security? What are the consequences for deterrence and defence? How can we enhance defence and industrial processes to deliver the capabilities we need? And, how do we ensure our forces are ready to provide for effective defence?

The JAPCC very much appreciates the frank, sound, and profound exchange of thoughts and opinions in the Chatham House Rule environment of the conference. What follows is a summation of the key points made and the ensuing discussions rather than the view of any particular speaker or participant. It does not offer a complete summary of the conference but will serve as a reminder and basis for further analysis and assessment.

© Moon Light PhotoStudio/Shutterstock.com

Global Competition – It Is About Power

In economic terms, competition is supposed to allow us to get better things faster and cheaper. Ideally, competition will increase the level of our common wealth. This positive connotation contrasts with the global competition we perceive today in the sense of a systemic rivalry of major state powers. Competitors like Russia and China primarily define their interests in terms of comprehensive state power. They strive to influence and potentially dominate other countries, and underpin their power with military force. Their obvious intent is to reset the rules of the international order, and they are willing to use the military option unilaterally if they deem it to be in their distinct national interest. For an increase of external power, they even seem willing to accept losses in other sectors, including wealth and economic growth.

The Russian war against Ukraine is an obvious case of this prioritization in foreign policy and is in line with other Russian foreign policy activities that started over a decade ago. Russia defines itself as an empire, claiming rights to a sphere of influence over adjacent states who might have difficulty enforcing their inherent right to sovereignty. The Russian president's broader objectives are to achieve military dominance over as much European territory as possible, split Europe from the United States (US), and re-integrate the former USSR.

A similar understanding and somehow congruent vision of world policy can be found in the perspectives offered by the Chinese president and leader of the Chinese Communist Party (CCP), Xi Jinping. His vision is to make China, latest by 2050, a centre-stage actor bolstered by military power that shapes – and, if necessary, dictates – norms, rules, and values of the international order. We must be aware that in China, national law supersedes international law, and rules and norms are accepted as long as they suit their interests. However, of equal importance is Xi Jinping's focus on the domestic dominance and survivability of the CCP. Consequently, and in contrast to the Russian president, maintaining the status quo could be an option for Xi Jinping as long as it supports his objectives.

How much pain China is willing to endure to further pursue its ambition to increase and use its power in its nearer and broader neighbourhoods is a question to be further assessed. In general, it seems wise to better understand China's various dependencies with respect to cooperation and exchange with our economies. The CCP will attentively follow Western states' reactions to Russia's aggression in Ukraine to assess the level of unity and resolve of NATO, the EU, their members, and partner nations.

Implications for Our Security

The competition we face today is global in nature and will persist over many years. We have entered a phase of ongoing competition and conflict, which does not fit into the traditional binary categories of war or peace. Contemporary challenges are not bound by geography, and what happens in one part of the world has the potential to reach all corners. A conflict in any region, for example the Indo-Pacific, will have ramifications for Europe and vice versa. This is the flip side of globalization.

Authoritarian and revisionist state competitors seem willing to use all available levers to reach their goals: diplomatic and economic coercion, disinformation and control of information flow, and, ultimately, the military instrument of power. This may be perceived as a 'weaponization of everything', meaning that nearly every field of interaction may become a battlespace, or at least an area of harsh contest with severe effects on the global economy, worldwide wealth, and well-being. Some states have already been exposed to significant coercive diplomacy and unilateral economic coercion. Not only as a punishment but in particular to demonstrate to others the price of such actions.

Maintaining the rules of the liberal world order in this blurring continuum of peacetime competition at conflict threshold and avoiding a future war requires cautious employment of all elements of national power: diplomatic proficiency, economic statecraft, information superiority, science and technological prowess, and not least domestic resilience. Defence based on military power is only one aspect of a whole of government approach to global competition.

'…Russia and China primarily define their interests in terms of comprehensive state power. They strive to influence and potentially dominate other countries, and underpin their power with military force.'

For defence, challenges have occurred and will occur in the air, land, maritime, cyber, and information domains, as well as in and through space. In this context, NATO is and will remain the cornerstone of the defence of Europe. The EU and its members are contributing to it and can do more to bolster their defence efforts and be more united, capable, and active. As the High Representative of the EU for Foreign Affairs and Security Policy stated: 'The EU has to learn the language of power.' Properly understood, an increased strategic autonomy will at the same time strengthen NATO as long as the EU's security and defence policy efforts are fully coherent with NATO.

Consequences – Deterrence Is Back on the Agenda

During the Cold War, both sides were interested in maintaining the status quo, whereas today we are confronted with Russia's communicated and

Joint Air & Space Power Conference
2022
Enhancing NATO Air and Space Power in an Age of Global Competition
© JAPCC

The 2022 JAPCC's Joint Air and Space Power Conference provided a unique setting to enable far-reaching debates for high-ranking leaders and experts from politics and the military, as well as from academia and industry.

demonstrated intent to redraw borders. Before the Russian large-scale military invasion of Ukraine, NATO and EU nations were divided over how to clearly communicate the consequences of such a step. Instead of us deterring Russia, it can be said that Russia deterred us. The good news is that after 24 February 2022, both NATO and the EU, through their swift united and determined reactions, showed resolve, demonstrated coherence, and confirmed the values that bind them together.

Russia's decision to wage war against Ukraine, combined with its nuclear signalling, revisionist rhetoric, and the demonstrated readiness of other actors to coerce others, urges us to rethink deterrence. A revised understanding must consider credibility, capability, and, communication as the so-called pillars of deterrence.

More than ever, deterrence is not just about the nuclear arsenal; it has an essential conventional component and will have to cover the whole spectrum of military threats and malicious violent activities. Deterrence is a whole-of-government effort that has to be effective in the 'grey zone' as well. Diplomatic activities and economic sanctions are part of it. Already below the level of armed conflict, it is about denying revisionist and authoritarian actors the incremental gains that might give them the impression of insufficient will and determination of democracies to counter their activities.

On the hard side of defence, deterrence needs resolve and robust presence. Participants debated whether the deterrence by punishment posture, represented by NATO's tripwire force at its north-eastern flank, is sufficient to guarantee 'Article 5'. The decision to move forward to a deterrence by denial posture through prepositioning more substantial forces is an appropriate first answer to the changed threat situation.

Credible deterrence will also need to be bolstered by resilience. It starts with measures to diversify our sources of energy supply and other raw materials, goods, and services and will have to include increased efforts to protect our critical infrastructure.

© JAPCC

Top three JAPCC leadership engaging with delegates at the 2022 Joint Air and Space Power Conference, Essen, Germany. (From left to right, Lt Gen Poschwatta, Air Cdre Herber, and General Hecker).

Consequences for Defence – Air Superiority Is a Priority

Looking at the war in Ukraine, it seems more important to realize what we do not see than what is conspicuous. Russia has not been able or willing to launch a comprehensive air campaign, neither at the beginning nor later. Currently, the war in Ukraine can be seen as a First World War type of warfare, notable for the lack of air superiority by either side. It demonstrates the enduring relevance of achieving air superiority as a prerequisite for – though never the sole guarantor of – success in warfare.

In particular, we have to bolster our integrated air and missile defence where we have a double need for long-range and shorter-range mobile air defence systems to build a reliable Anti-Access/Area Denial (A2/AD) capability. This will have to include European-owned and operated assets for an upper-layer defence over Europe, which currently, except for the extant US assets, does not exist. Other required capabilities include deep-precision strike capabilities to successfully perform counter-air missions. We will most probably need additional fifth-generation aircraft, jammers, ISR (Intelligence, Surveillance, and Reconnaissance), and advanced Command and Control (C2) capabilities.

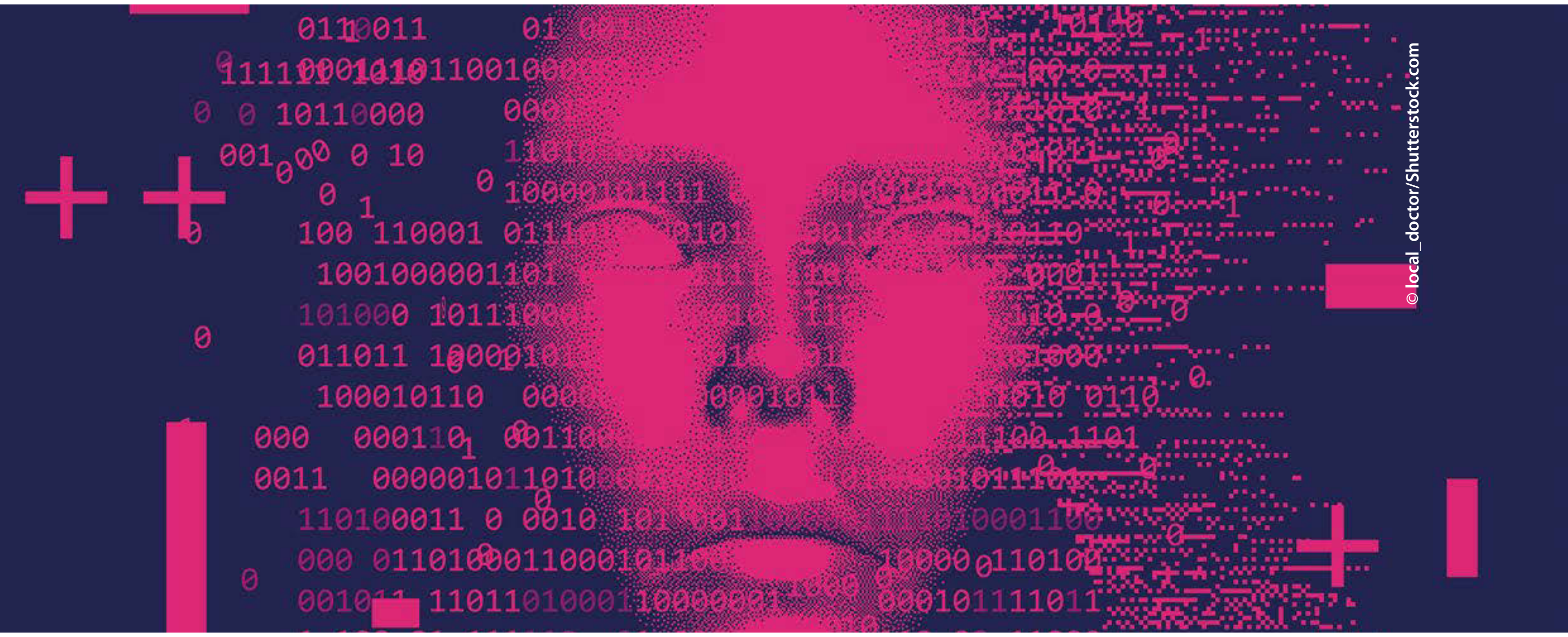
In the face of a threat spectrum ranging from weaponized commercial drones to hypersonic missiles, we will have to catch up fast and realize a system of systems approach to defence with interoperable links across domains. Considering the developments in anti-satellite capabilities, a fully layered defence will have to acknowledge our defences' dependence on space capabilities.

Technology advancement is a crucial driver for our security and defence. Those who can make the best use of available technology will have information dominance, decision dominance, and, engagement and escalation dominance across all operational domains. To achieve this, the Alliance and its partners will have to look for fundamental game-changing technologies but also consider that the right concepts, approaches, and structures must be in place to reap the benefits of technology.

Interoperability through standardization is crucial. It seems that NATO nations have been much better in these aspects before the 1990s. Indeed, our nations have and sometimes pursue different interests. However, for defence purposes, we have to align our efforts and build those capabilities needed to maintain and, in certain areas, rebuild a defensive advantage.

NATO must continue to become more agile and resilient; this is a requirement to establish credible deterrence today and enable SACEUR to win tomorrow's fight, should it ever come.

- **Integrated multi-domain defence.** A joint and flexible approach to a fluid environment.
- **Cross-domain command.** Investing in the art of command, critical thinking, and audacious action.


© local_doctor/Shutterstock.com

Enhancing the Force – Capability Requirements

NATO's Allied Command Transformation focuses on developing our capabilities to succeed in conflict and future combat environments. What do we spend on the war of 2040 against an advanced enemy? The NATO Warfighting Capstone Concept, published in 2021, offers an organizing principle and a guiding rationale to inform the alignment of Alliance warfare development efforts. It sets out the so-called Warfare Development Imperatives to realize operations across domains:

- **Cognitive superiority.** Understanding of the threats, adversaries, and the environment NATO operates in.
- **Layered resilience.** Withstanding immediate shocks and be prepared to persevere in challenging situations over long periods.
- **Influence and power projection.** Being proactive in taking the initiative through various means to reach set objectives.

Having fleets of interoperable – or better yet interchangeable – combat and support platforms, plus the compatible C2, ISR, and operational planning systems, is crucial to succeeding in a future multi-domain operational environment. Moreover, all legacy systems will have to be incorporated to efficiently communicate and operate along with the newer platforms. Modern warfare is information-centric; secure data distribution across domains will be pivotal for success.

Global reach, the possibility to deploy and maintain a capability for long periods and away from home bases, is a crucial element in a world of competition and contest. This broader definition of the traditional element of reach adds to the two other Air Power characteristics of persistence and speed.

Uncrewed vehicles and controlled levels of autonomous operations offer persistence and add to sustainability and resilience by creating additional combat mass acceptable for attrition.

Cyber and space capabilities will have to be developed from both defensive and offensive points of view. Cyber already is a battlespace domain; and space is at least a battlespace domain in the making, as Russia demonstrated anti-satellite capabilities.

The need for information superiority in a hostile environment requires us to invest in all technologies, sensors, effectors, and transmission systems which allow us to transform data and information into an operational advantage, thus achieving dominance over the electromagnetic spectrum. In a situation where every mobile phone can support intelligence gathering, the collection and exploitation of open-source information is relevant. Therefore, investing in those dual-use technologies for defence is paramount.

Towards a More Effective Defence Planning and Quicker Procurement

The defence budgets of NATO nations sum up to one trillion euros. Eight nations meet the 2 % of GDP defence spending goal, and other nations are getting there. For over seven consecutive years, ten nations already exceeded NATO's 20 % investment target for defence spending. Ten nations are also meeting the NATO capability targets. These are promising numbers.

In Europe, we still operate 20 different fighter planes – compared to the US with six – and 28 different types of helicopters. As long as every nation develops and buys its own systems and subsystems, we are subsequently forced to make them interoperable – what we have done for a long time. Instead of continuing that way, an approach to ensure interoperability by design should be considered. This will require precise standards, at least for the software components, that allow the industry to follow a product approach instead of a very costly system approach.

The NATO process of defence planning coordinates national developments of capabilities and offers perspectives to consider developing common capabilities. NATO Airborne Early Warning (NAEW) and Alliance Ground Surveillance (AGS) are examples where nations acquired a capability together. On the EU side, the Joint Procurement Task Force will support smarter approaches to defence spending. Unfortunately, the European Defence Agency (EDA) missed its goal of having 25 % of members' equipment procured through the agency's framework. The trend was the opposite, with figures dropping to 11 %. If this is not changing, there is a high chance that European nations will not get the required capabilities.

'…defence budgets of NATO nations sum up to one trillion euros. Eight nations meet the 2 % of GDP defence spending goal, and other nations are getting there. For over seven consecutive years, ten nations already exceeded NATO's 20 % investment target for defence spending.'

Overall, NATO has established an impressive structure that manages defence planning. However, the national defence management and planning processes are concurrent with the NATO process and the separate EU defence planning process. However, the links and connections between the EU and NATO defence planning processes are not sufficiently clear. There is an urgent need to harmonize these processes or even bind them together to enable smoother and swifter planning to assure that targets are met.

Reliable Investment in Defence and Cooperative Competition

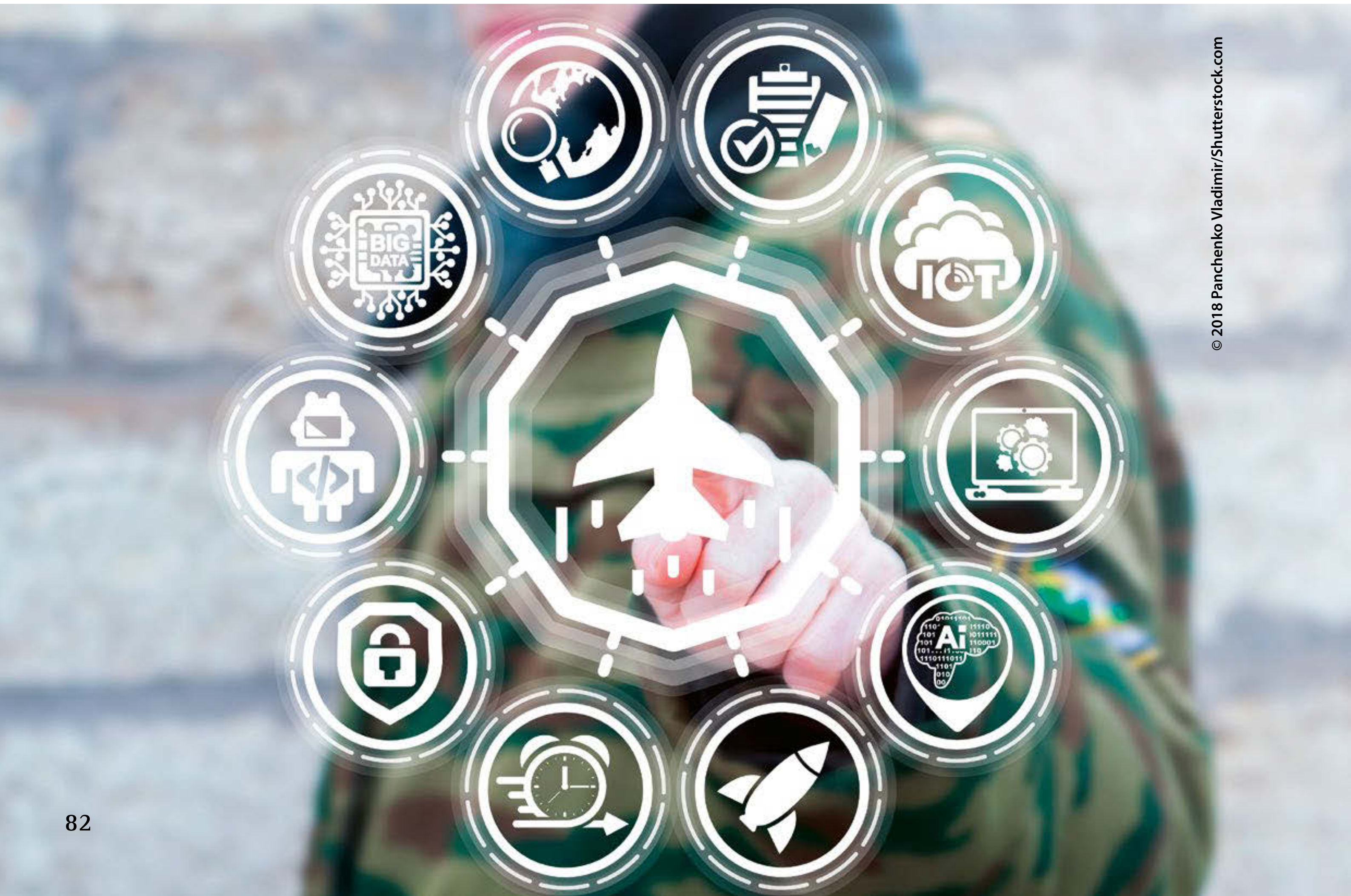
To enable faster delivery of capabilities, extant processes must be streamlined and more agile ways to contract must be identified. The defence industry needs reliability through clear signals to develop the desired capabilities. This will have to include robust and reliable planning of armaments procurement based on long-term, not short-term, demands. The industry has already proactively invested in capacities and people. Now, they need increased reliability through firm, long-term contracts to incrementally increase quantity and quality and assure tailored stock requirements.

The Western Air and Space industry is highly capable and eager to contribute to deterrence and defence. In the past, many nations have not invested robustly in defence capabilities and infrastructure. However, this is a prerequisite to making the defence industry resilient. The defence market is different from the consumer market; the necessary investments to create the required capabilities cannot be provided by industries alone. Governments have to invest their share.

A crucial point to be considered is: How much competition can we allow and afford in the defence industrial sector? A first guess proposes that competition is still the way forward to achieve high-quality results, even a cooperative competition. Industry wishes to work with their customers to simplify things and, together with defence institutions, find the right balance to get the required capabilities fast and in time. Thus, a common industrial base in Europe seems favourable for improving interoperability and adaptability while retaining sufficient competition to provide redundancy and multiple options to customers.

Setting interoperability standards has been a core issue for NATO since its inception. A combined force will only work with clear and appropriate standardization. Clear standards are also necessary for developing interoperable capabilities upfront through effective industrial cooperation. Open architecture approaches are a way to achieve a faster process than we see today.

Additionally, the safety standards for a platform should be separated from the tactical functionality. This would allow hardware changes in weeks rather than months and enable fast software updates to expedite capability development (e.g. the integration of new weapons). The benefits of digitalization also allow the creation of digital twins to transition quicker from development to testing without building several platforms. Accreditation and certification authorities will certainly have to support these approaches.



© 2018 Panchenko Vladimir/Shutterstock.com

© JAPCC

The JAPCC Director, General Hecker's opening conference remarks, focusing on the demands of a challenging security environment, the necessary development of capabilities, and the ways to deliver them.

Investing in People

The conference focused on the demands of a challenging security environment, the necessary development of capabilities and the ways to deliver them. It emphasized the need for deterrence, defence, and the related resolve and resilience. Capability development and procurement processes will have to be adjusted and better aligned to ensure quicker availability of platforms and systems.

Beneath our technology, capabilities, and infrastructure investments, we should remember to invest in people. Dealing responsibly with the newest emergent technological software and devices, enhanced by artificial intelligence and automation, will require smart, educated personnel. In the end, equipment by itself does not fight. The Ukrainians demonstrate that will, imagination, and commitment can take you an awfully long way, in a manner that pure mass often does not. We should, therefore, always remember the importance of the conceptual and the moral components.

As NATO's Centre of Excellence for Air Power, the JAPCC relies on the mastery, experience, and innovative capacities of its personnel. We thank everybody who participated in the 2022 Joint Air and Space Power Conference. We look forward to meeting you again in Essen from 10 to 12 October 2023, where we will examine the near-term imperatives to achieve deterrence and defence. ●

Colonel (GS) Thomas Schroll

started his military career in 1989 and was trained as a ground-based air defence officer. He went through general staff training at the German Armed Forces Command and Staff College and the UK's Joint Services Command and Staff College and has subsequently served in national and international positions at various levels of command, including in the German CHOD's office and for the SACEUR. He earned master-level degrees in Economics and in Defence Studies. Until December 2022, he was the Assessment, Coordination and Engagement Branch Head in the JAPCC and served as the Conference Director for the annual Joint Air & Space Power Conference.

Pilot: © Suchat tepruang/Shutterstock.com; Fighter Jet: © Pixabay/WikiImages; Space Background: © 1xpert – stock.adobe.com; Sky: © Katy – stock.adobe.com; Clouds (partially): © taira42 – stock.adobe.com

© JAPCC

JAPCC Hosts the 9th Joint Air and Space Power Network Meeting

In Light of the New Security Environment

On 23 November 2022, the NATO Joint Air Power Competence Centre hosted the 9th edition of the annual Joint Air and Space Power Network Meeting (JASPN) in Kalkar, Germany. The JASPN Meeting is organized by the JAPCC since 2014 with the intent of stepping-up joint efforts to make better use of limited resources and utilize common insights to enhance synergy within the Air and Space Power community.

This year the JASPN included representatives from the NATO HQ, HQ Allied Air Command, European Union Military Staff, Movement Coordination Centre Europe, European Air Transport Command, European Defence Agency, European Air Group, Competence Centre for Surface-Based Air and Missile Defence, Command and Control Centre of Excellence, Air Operations Centre of Excellence, and FR Air Force.

The one-day event focused on presenting current programmes of work to identify and discuss those areas of common interest for either the potential for collaboration or to avoid duplication of effort. Furthermore, the meeting indicated again the possibilities of cooperation in many areas such as: Multi-Domain Operations and Command and Control, Cyberspace Integration, Logistic Support to Air Operations (AAR, AT), Countering UAS, Red Forces Delivery, Emerging Technologies (Hypersonic, AI), IAMD, Joint ISR, Education & Training, Force Protection, Alliance Future Surveillance and Control, and Resilient Basing.

The group also recognized new opportunities to mitigate limited human resources by avoiding unnecessary effort duplication and fostering knowledge in order to accelerate the transformation of Joint Air and Space Power, with the intention of preparing NATO for the new realities, which include substantial changes to world security in light of the Ukrainian war and a changed security environment in Europe.

The upshot of the meeting was the updated collaboration matrix with twelve focus areas to depict the identified lines of effort with common interests and serve as a platform for fostering collaboration among participating organizations. Once again, the JAPSN has proved to be an inestimable value for the exchange of insights and experiences. In March this year, the JAPCC looks forward to hosting the annual Think Tank Forum, which takes a similar approach to finding collaboration within nations. ●

© Crown Copyright

Air platforms remain extremely vulnerable on the ground.

Force Protection Decision Support Tool

'It is easier and more effective to destroy the enemy's aerial power by destroying his nests and eggs on the ground than to hunt his flying birds in the air.'
General Giulio Douhet,
The Command of the Air, 1921

On 8 December 2022, the JAPCC and Cunning Running Software Limited concluded a highly successful 'Proof of Concept' presentation, marking the completion of the JAPCC's Force Protection Decision Support Tool (FPDST) project. The project was initiated by a Request for Support (RfS) from NATO Air Command (AIRCOM) to explore the feasibility of automating the process of analysing the Force Protection (FP) challenges facing the Air Component, often referred to as 'The FP Estimate'. The estimate is a structured way to analyse all aspects of a base's defence and determine appropriate measures. However, it requires trained and experienced individuals and is a time-consuming process, especially when dealing with multiple locations. Of note, although the initial RfS was air-centric, the FPDST just delivered has joint applicability.

The RfS was prompted by a simulated incident during a NATO exercise, which resulted in catastrophic losses due to flawed FP decisions based on inaccurate information. This incident highlighted the importance of FP decision-making, as seen in the 2012 Taliban attack on Camp Bastion in Afghanistan, where subsequent reports cited failings in FP decision-making as a major cause of the incident. The Air Component's high-value, low-density assets are so significant that any losses, even at the tactical level, are increasingly likely to have strategic consequences.

AIRCOM is responsible for a vast geographical area with numerous locations, each with its own unique characteristics. With limited staff resources to conduct FP Estimates, the challenge is to understand the FP requirements of the entire area of responsibility in a dynamic and ever-changing environment, in order to best protect troops and materiel and inform commanders' decision-making. Having rapid access to accurate, standardized information for all required locations is a key part of the solution. The fielded version of the FPDST already provides this, and the current 'Proof of Concept' promises to reduce staff effort in creating the FP Estimate by up to 60 %.

The FPDST concept is based on software that has been in existence for over two decades, originally known as Surface to Air Missile Prediction Rating and Analysis Software (SAMPRAS). Initially, this software was used to predict adversary air defence systems, but has since been enhanced to include threat prediction for rockets, mortars, artillery, and small arms. Further software developments have enabled wider FP planning applications, as well as a module for siting sensor systems and Counter-Unmanned Air System (C-UAS) functionality.

FPDST utilizes digital mapping with locations uploaded from a database, or user defined, and generic or platform-specific flight paths. This data is then used to generate a Surface to Air Fire or Man-Portable Air Defence System threat footprint. Additionally, alternative flight paths incorporating intelligence-led tactical exclusions can also be modelled, allowing platform operators to define defensive, evasive manoeuvres that can further reduce the threat footprint.

The software also allows for the definition of other threats to identify targets for adversary direct and indirect fires. Threat templates are produced based on individual weapon characteristics, while target visibility and tactical restrictions can be user selected. Unmanned Aircraft System restrictions based on national rules can be applied, visualized, and modelled if necessary.

Furthermore, the software can be used to analyze friendly sensor locations, define sensor/effector range based on real terrain data, and evaluate friendly sensor system's coverage holistically. This capability is not limited to C-UAS sensors, but can be used for a wide variety of friendly sensor applications.

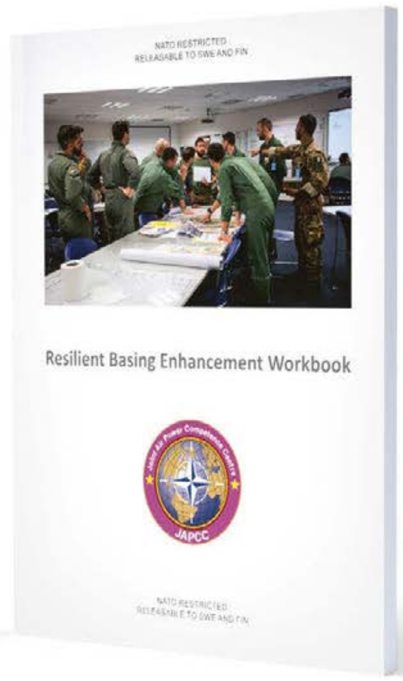
The software also provides the ability to create three-dimensional visualizations that can be overlaid with all of the other features and footprints produced by the software. This allows for a comprehensive analysis of the threat landscape, enabling platform operators to make informed decisions and optimize their defensive strategies.

The Force Protection Decision Support Tool is a revolutionary software that enables headquarters and their subordinate units to better understand the FP challenge specific to their locations, as well as the FP capabilities necessary to mitigate them. This is achieved by incorporating known or user-defined enemy capabilities, deducing friendly force requirements, generating the FP Order of Battle, building a FP Estimate, and creating a report together with a supporting presentation. The process is guided by NATO standards and is underpinned by fully configurable databases, allowing the software to handle dependencies between force elements and automatically identify their support requirements. Outputs are then automatically generated in standard, but editable, formats.

The FPDST provides a comprehensive 'library' of individual locations that, once consolidated, will provide the FP overview necessary to allow proper senior-level FP decision-making. Interested nations or headquarters can express their interest by contacting the JAPCC FP team, in order to move from the 'Proof of Concept' to an in-service capability. ●

New Release: Resilient Basing Enhancement Workbook

An Approach to Base Resilience Assessment


NATO RESTRICTED
RELEASABLE TO SWE AND FIN
Resilient Basing Enhancement Workbook
JAPCC
NATO RESTRICTED
RELEASABLE TO SWE AND FIN

© JAPCC

Many of our Alliance members are focusing on introducing new capabilities in an era where the operational environment is in a constant state of change with technology evolving at an ever-increasing pace. If not done correctly, the employment of new technologies in a dynamic operational setting will lead to new vulnerabilities, possibly new threats, and certainly greater risks as our adversaries will seek to exploit any weaknesses. Sudden interruptions of Air and Space Power activities either at home stations or at deployed locations will have an immediate impact on joint force operations. We must be proactive in preventing and mitigating such man-made risks in addition to natural hazards.

Resilience is a national responsibility and simultaneously a collective commitment anchored in Article 3 of the NATO Treaty. During the Madrid Summit in June 2022, the North Atlantic Council reemphasized the need to boost NATO's resilience to current and projected threats and strengthen overall interoperability. Fortunately, the JAPCC had already responded to a Dutch Request for Support (RfS) to better analyse the current resilience status of Alliance members against a full spectrum of threats. Supporting both objectives, the JAPCC recently published the Resilient Basing Enhancement Workbook.

This workbook provides a description of a virtual airbase ('Base X') placed in several fictitious scenarios – based on existing NATO Force Protection doctrines and experiences, as well as current developments in Ukraine. To enable nations to self-evaluate their airbases' resilience, over a hundred 'Issues to Consider' followed by a series of questions have been incorporated in a questionnaire. By completing the workbook and returning the questionnaire, nations can both improve their resilience and contribute to a better understanding of the issue across NATO.

The workbook is designed for the national entities responsible for contingency planning and evaluation. It is up to each nation to determine the appropriate headquarters responsible to formulate a comprehensive response. The workbook can be obtained via NSWAN by contacting us at JAPCC.Registry@japcc.nato.int. In return, JAPCC appreciates your findings, including mitigating strategies, before 1 June 2023, via the Response Collection Sheet included with the workbook. Subsequently, the JAPCC will assess the received inputs and inform nations about the results via a whitepaper currently planned for fall 2023.

We thank you in advance for your support in enhancing the Alliance's resilience. ●

New Release: Freedom of Manoeuvre in Cyberspace White Paper

Inextricably Linked to Freedom of Manoeuvre in the Air Domain

© JAPCC

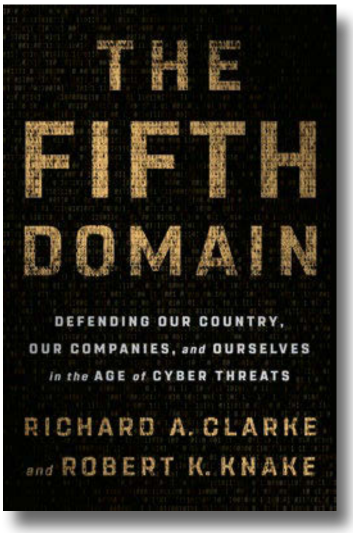
Today's highly computerized world owes a great debt to the investments made by military organizations of decades past. For example, Alan Turing, employed by the British War Office, made significant contributions to the development of the computers that deciphered the German codes during the Second World War, earning him the title of 'Father of Theoretical Computer Science and Artificial Intelligence' for his work on the theory of computing. In addition, the Internet rose from the ARPANET, a military network built in the 1970s by the US Defense Advanced Research Projects Agency (DARPA). Gradually, computing technologies have been increasingly employed in demanding and intricate roles in the conduct and support of military operations. In fact, cyberspace has evolved so drastically that it has developed its own distinct vocabulary. Now, it is widely recognized as an independent warfighting domain.

The computing technologies have evolved to such an extent that cyberspace has become an integral part of civil society and the traditional warfighting domains, particularly in the air domain, which relies on highly advanced technologies to effectively dominate that battlespace. Therefore, it behoves air domain operators and commanders to broaden their sphere of expertise into the edges of the cyberspace domain to ensure success in air operations. To assist this endeavour, the JAPCC has published a White Paper (WP) on Freedom of Manoeuvre (FoM) in Cyberspace. This paper takes the approach of defining and applying the concept of FoM, which is essential in the physical domains, to the cyberspace domain.

The WP introduces the fundamentals of cybersecurity and cyber defence before delving into the primary uses of cyberspace capabilities as manoeuvre elements. It also examines the role and potential impact of cyber-related emerging and disruptive technologies. Finally, it emphasizes the interdependencies between traditional warfighting domains and cyberspace. Within the Multi-Domain Operations concept, data-centricity is the lynchpin, making the need to maintain FoM in cyberspace a top priority. This WP is invaluable for warfighters and decision-makers, providing them an understanding of their role, as well as the level of effort and investment necessary to maintain an acceptable degree of FoM in cyberspace and, by extension, FoM in the air domain, which is heavily reliant on cutting-edge technologies.

You can find the FoM in Cyberspace White Paper, along with other subject matters' White Papers, by following the link to our website https://www.japcc.org/white-papers. Hardcopies are available upon request. ●

‘The Fifth Domain’



Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats

Drawing from extensive experience and careers in top governmental and civilian positions, the authors depict the current landscape and potential futures of cyber warfare. The book addresses the most current cyberspace topics affecting governments, corporations, and individuals. Many relevant examples, some of which were in the news, like the Stuxnet, WannaCry, and NotPetya viruses, illustrate the cyber threats we face while describing how the affected industries coped with them. It also looks into the future concerning near-term technologies, such as 5G, quantum computing, and AI, and analyses their impact on the security landscape. Promoting the idea that we constantly need to implement new measures to secure the cyber domain and mitigate its inherent risks, it includes a host of good policy options and recommendations, from a potential ‘Schengen accord for the internet’ to developing resilient systems. Clarke and Knake pragmatically emphasize that most Americans have been victims of identity theft, and provide practical advice and user solutions, like multifactor authentication and biometric-enhanced passwords.

A must-read for anyone working in the broader cybersecurity enterprises, the book concludes with the authors voicing an optimistic view: ‘Securing our countries, our businesses, and ourselves in cyberspace is far from hopeless.’ ●

By Richard A. Clarke and
Robert K. Knake;
Penguin Press; 2019
Reviewed by:
Lt Col Ciprian Teletin,
RO AF, JAPCC

‘War in Space’

The Science and Technology Behind Our Next Theater of Conflict

War in Space is a technological and doctrinal analysis of the current use of space, especially by the military. Providing first impressions on the dependencies we take for granted, Linda Dawson details deep insights into the leading space powers: the US, China, and Russia. The use of space and counter-space developments are comprehensively addressed and analysed. The author offers a broad technical perspective on space, focusing on the impact of the hostile and non-cooperative environment of space on materials. This thorough background information on material degradation helps the reader understand the limiting factors in operating systems in space. Dawson discusses today’s paradigm change in space users, from nations to commercial actors, which will cause challenges in the future, including the required adjustments of space-related laws, norms, and practices. She summarizes different methods to prevent a future war in space and addresses and, also, discusses options available to mitigate or deter attacks on space-based assets.

This book is focused on the US use of space and well-fitted into the historical context and can be an accessible entry point to this complicated topic for non-expert readers. The technical explanations are far above the level of popular literature and offer a firm basis for further research, even for educated readers. ●

By Linda Dawson;
Springer Nature; 2018
Reviewed by:
Lt Col Tim Vasen,
GE AF, German Air Force Headquarters

airbus.com
DEFENCE
IS
A
FORCE
FOR
GOOD