CEPA

An Urgent Matter of Drones

ABOUT CEPA

The Center for European Policy Analysis's (CEPA) mission is to ensure a strong and democratic transatlantic alliance for future generations.

CEPA is a nonpartisan, nonprofit, public policy institution.
All opinions are those of the author(s) and do not necessarily represent the position or views of the institutions they represent or the Center for European Policy Analysis.

Cover photo credit: Illustration: Michael Newton/Center for European Policy Analysis. Photo: A soldier prepares a drone equipped with a Dummy ammunition for a simulated flight operation. Soldiers at the training camp, during the drone flight tests while wearing FPV Vision goggles. Credit: Marco Cordone/ SOPA Images/Sipa USA

An Urgent Matter of Drones

By Federico Borsari and Gordon B. “Skip” Davis Jr.

Table of Contents

Executive Summary

Uncrewed aircraft systems (UAS) have become essential elements of modern warfare and their role will expand in the future, raising the urgency of NATO and individual allies to rapidly adapt starting now.

Individual allied nations own a wide variety of UAS capabilities, and the alliance collectively owns and operates NATO's Alliance Ground Surveillance (AGS).[1] Despite NATO efforts to encourage procurement and capability development and to promote common standards and enabling capabilities, NATO has too few drones for a high-intensity fight against a peer adversary. It would be severely challenged to effectively integrate those it has in a contested environment.

Several challenges hinder the development of robust and effective UAS capabilities across the alliance. These include limited interoperability, critical capability gaps, inadequate platform survivability, deficiencies in personnel and training, limits to intelligence processing, and more.

For NATO and allies to leverage and prepare for the full potential of future drone warfare, this report recommends the following:

- First, the alliance must clearly assess UAS and counter UAS (C-UAS) capability requirements based on lessons learned from recent conflicts, technological developments underway, and expected future threats and challenges.
- Second, UAS and C-UAS capability development and policy development must be guided by the need for scale and interoperability and the imperatives of multidomain operations.
- Third, enabling capabilities such as AI tools, data architecture, communications networks, and cyber and space capabilities and services must be enhanced.
- Fourth, NATO and individual allies should leverage the significant innovation efforts underway while improving operational experimentation and procurement processes.
- Fifth, NATO should refine or establish joint allied doctrine, operational concepts, tactics, techniques, and procedures (TTPs) to cover new and expanded roles of UAS and the growing importance of C-UAS.
- Sixth, both UAS and C-UAS capability integration into NATO and national forces will require a special focus on human resource development.

Introduction

Russia's full-scale invasion of Ukraine marks not only the return of conventional war in Europe but also technological innovation on the battlefield. The conflict has become a testing ground for new military systems.

Ukraine has pioneered the use of both military and commercial off-the-shelf UAS – also known as "drones" – to perform tactical reconnaissance and surveillance, collect real-time intelligence, adjust artillery fire, provide communication relay, conduct short to long range strike and battle damage assessment (BDA), and drop repurposed munitions against enemy equipment and personnel. The net effect is that Ukrainian forces have employed drones as enablers and force multipliers, shortening and simplifying the "kill chain"[2] and enabling better and faster military decision-making.

This is the latest example in a growing list of conflicts featuring UAS, including the civil wars in Libya, Syria, and Yemen, as well as the region of Nagorno-Karabakh. UAS proliferation has empowered both state and non-state actors with new and, at times, substantial capabilities, ending the West's monopoly on UAS and threatening to erode its technological edge.

Bigger changes loom. Advancements in artificial intelligence (AI), data-related technologies and applications, quantum sensing, next-generation communications, swarming technology, and human-machine teaming capabilities promise to enhance the ubiquity, versatility, lethality, and effectiveness of UAS. This changing character of the UAS threat may potentially reshape the offense-defense balance,[3] making counter-UAS systems equally important. At the same time, increasingly contested battlespaces (air, land, and sea) pose doctrinal and operational challenges to NATO's use of medium and large UAS.

Preliminary indications in Ukraine and elsewhere already suggest that the ubiquitous presence of sensor-packed UAS on the battlefield may frustrate achieving the element of surprise and render offensive maneuver operations ever more difficult and costly.

The pervasiveness of UAS also raises serious questions about force protection and the vulnerability of forces and infrastructure to attack, including at considerable distances from the frontline. As a British Army General put it, "the use of unmanned aerial systems has created a transparent battlefield where there is no sanctuary."[4]

Indeed, UAS employment has reintroduced the threat of near-constant aerial observation and strike for conventional forces at a level not experienced since the Cold War. Cover, concealment, and protection from above are now concerns

Photo: US Air Force Academy's Drone Racing Team members, Andrew Fedora and Luke Ringe, fly small unmanned aircraft vehicles (UAVs) on Feb. 28, 2024 in the Holaday Athletic Center.
Credit: Rayna Grace/US Air Force

throughout the battlefield, not just on the front line. This ubiquitous vulnerability will have important implications for the future of land warfare and the ways in which ground forces are employed, protected, and defended in a sensor-rich environment.

However, as many experts contend, drones require a variety of complex (and expensive) systems to support their use, as well as refined TTPs, enabling capabilities, and organizational structures[5] to achieve tangible effects. This complex set of prerequisites is called the "military ecosystem," and in robust form it can leverage UAS capabilities for decisive advantage.[6]

This study aims to fill the gap in existing literature on NATO's uncrewed aerial systems, adopting a four-step approach. First, it identifies the main operational requirements and developments regarding the use of UAS in present and near-future high-intensity environments. To that end, the paper draws upon relevant lessons emerging from the war in Ukraine and other recent conflicts.

Second, it assesses NATO's capabilities in the field of UAS, looking at the three traditional operational domains of air, land, and sea as well as the enabling domains of space and cyber. This includes the analysis of current policies and upcoming policy initiatives to boost alliance UAS capabilities at the national and multinational levels.

Third, the report looks at the challenges affecting NATO's use of UAS and key enabling functions as well as C-UAS capabilities. Finally, the report concludes with considerations and recommendations for changes needed to prepare the 31 (soon 32) allies to effectively operate together and leverage the maximum potential of UAS and C-UAS capabilities for decisive advantage in an increasingly complex security environment.

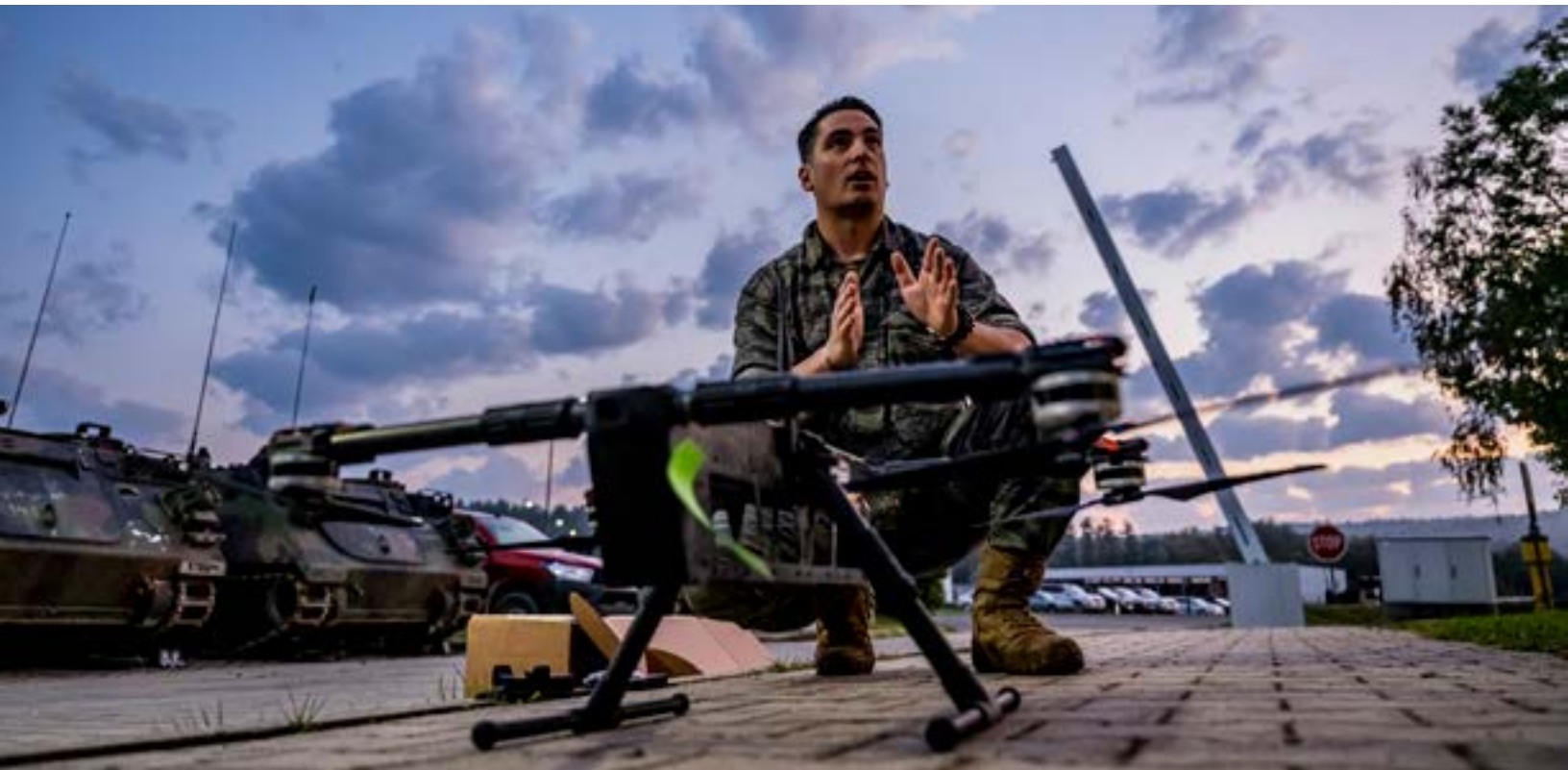
The History of Drones

The history of uncrewed aerial systems (UAS) – and technology in general – is one of continuous evolution. During the early Cold War, when the first UAS prototypes were introduced, their most common use was for intelligence, surveillance, and reconnaissance (ISR) and limited strike missions.

Fast forward to 2023, UAS' capabilities have expanded considerably, although their fundamental technologies have existed for decades, including propeller-powered aircraft, electro-optical sensors, precision munitions, and multiband data transmission. These are, in many respects, the same found in crewed aircraft. Today, UAS are a primary means of intelligence, surveillance, and reconnaissance (ISR) but they can also conduct air power missions similar to crewed aircraft - close air support, armed reconnaissance, interdiction, electronic warfare (EW) attacks, suppression of enemy air defenses (SEAD), communications relay, and resupply and refueling.

The integration at scale of both automated (deterministic) instruments as well as nondeterministic[7] AI and machine learning tools along with, advanced onboard computing, next generation communications and data technologies (e.g., cloud and edge computing) promise to push UAS capabilities to unprecedented levels and reshape their evolutionary trajectory.

Photo: US Army Sgt. Connor Piegaro, a Small Unmanned Aerial System master trainer with the 1st Battalion of the 4th Infantry Regiment, talks about the TS-M800 II drone to explain its capabilities during Saber Junction 23 at the Joint Multinational Readiness Center near Hohenfels, Germany, Sept. 11, 2023. Credit: 1st Sgt. Michel Sauret/ US Army Reserve



Part I – UAS in Ukraine and Other Recent Conflicts: What essons for NATO?

Uncrewed aircraft systems (UAS) have become essential elements of modern warfare and their role will expand in the future, raising the urgency of NATO and individual allies to rapidly adapt starting now.

Lessons Learned from UAS in the Ukraine War

Ukraine's extensive use of multiple types of UAS, from high-end Turkish-made medium altitude long endurance (MALE) TB2 combat drones to small and cheap commercial Chinese-made DJI quadcopters, has helped Kyiv to repel and stop its much stronger opponent. The number of videos showing modified DJI quadcopters that chase and strike Russian personnel and equipment by dropping fin-stabilized grenades is a telling example.[8] The cumulative kinetic and psychological effects of weaponized commercial drones deployed *en-masse* deserve further attention.

Drones achieve their full potential when used in synergy with other combined arms capabilities, ranging from direct-fire maneuver, artillery and long-range fires, air defense (including counter-UAS), mobility and counter-mobility, as well as electronic warfare (EW) and air power. UAS will never be able to seize and hold terrain, but they can provide fire and logistical support, as well as eyes and ears to any command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) architecture, the "central nervous system" of any modern military.[9]

Importance of Counter-UAS Capabilities Revealed via the Ukraine War

Second, the war in Ukraine has highlighted the critical importance of having the capacity to counter or defend against the threat from UAS – whether in the form of observation, strike, electronic warfare attack, disruption, etc. – and the urgent need to do so with more cost-effective solutions. While high-end air and missile defense systems and expensive munitions are reasonable for protecting high value assets (e.g., population areas, ships, critical military, or civilian infrastructure), intercepting a weaponized DJI quadcopter (worth a few hundred dollars) or even a ~$40,000 Iranian Shahed slow-flying munitions with a million-dollar missile is not efficient or sustainable. Overall, the costs of damaging a target versus the value of that target and the benefit of adverse effects avoided comprise the metric that should be used to determine the cost-to-benefit index for C-UAS.[10]

The challenge for future counter-UAS (C-UAS) capabilities, therefore, is twofold: 1) to turn the cost-of-intercept curve in favor of the defenders while 2) retain a high success rate in defeating different types and large numbers of UAS attacking simultaneously. Russia, for example, has employed volleys of Shaheds for deep strikes against Ukraine's civil infrastructure, and used Lancet-3 loitering munitions in large quantities to blunt the Ukrainian counteroffensive.

As NATO approaches a future where AI-enabled drone swarms are likely to play a significant role, NATO may have reached a critical point at which current air defense (AD) systems, including the most sophisticated ones, cannot neutralize large drone swarms or even volleys of uncoordinated loitering munitions. For these reasons, C-UAS requires a multi-spectrum and layered combination of different tools, both kinetic and non-kinetic, to be effective. This protection must be ensured from the forward tactical edge to the rear support area to air bases and strategic C2 nodes even further in depth.

Analysis by Capability Category

Some lessons are novel while others reinforce those learned from other recent conflicts.[11] This study begins with an analysis of the role played by UAS, C-UAS, and supporting capabilities in Ukraine and elsewhere, as well as key takeaways for the alliance.

A) Medium and large-size UAS[12]

These offer an unmatched combination of state-of-the-art sensors, strike capabilities, endurance, range, and payload. The gradual integration of more capable and sophisticated sensors alongside long-range precision munitions is paving the way for new roles and mission sets for these platforms.

Medium Altitude Long Endurance (MALE) drones are increasingly used by a wide range of nations and opposing forces as ISR and strike platforms in high-intensity scenarios. Smaller countries now have access to these capabilities after years of proliferation supported by lower prices and more liberal export policies by countries such as China and Turkey.

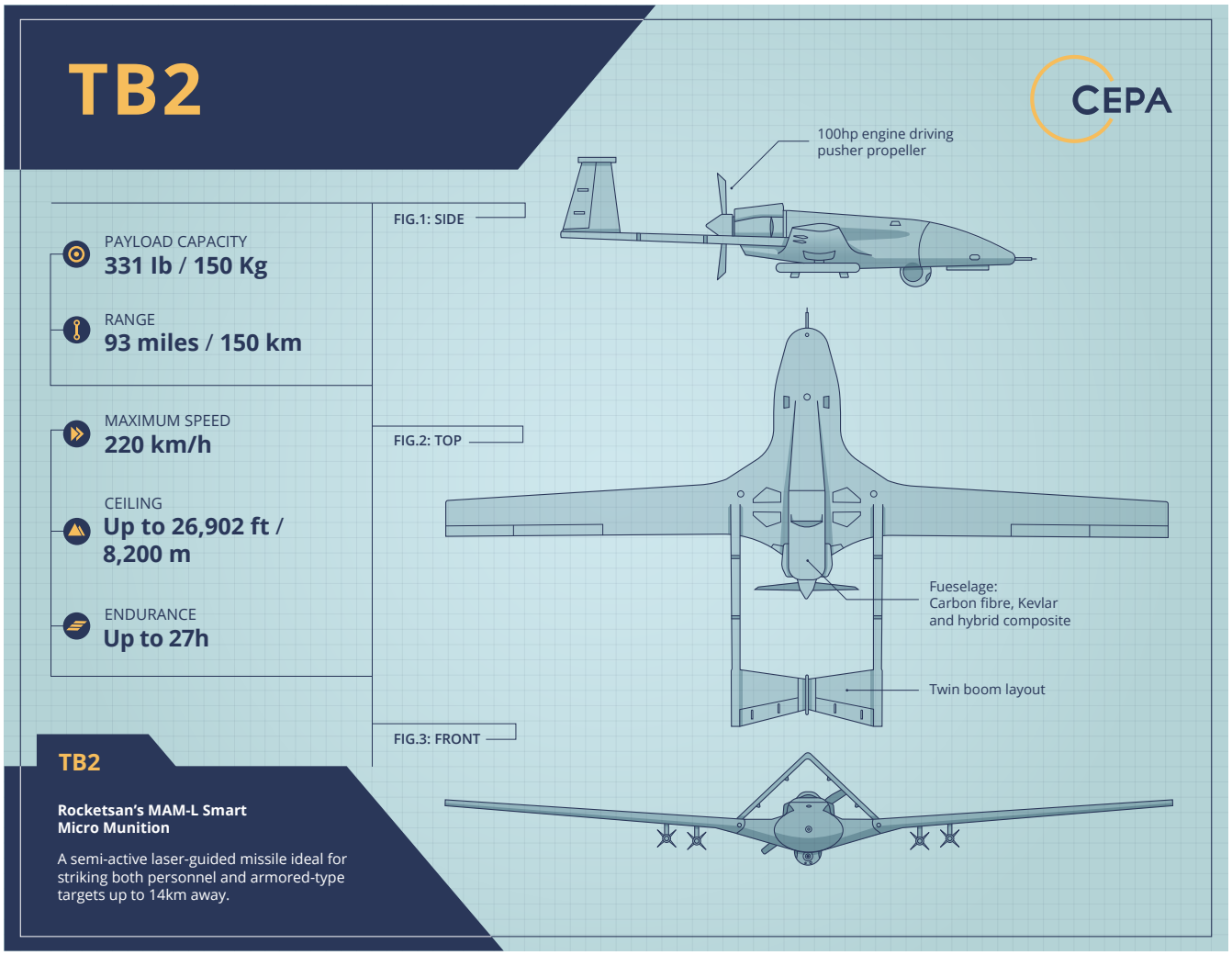
Popular models like the Turkish-made Bayraktar TB2 and Chinese Wing Loong II armed UAS are now in service in several countries[13] and have played important roles in wars across the Middle East and Africa, including in Libya, Syria, Yemen, and Ethiopia. The TB2 was also a key enabler of Azerbaijan's swift victory over Armenia in the 2020 Nagorno-Karabakh conflict. In Ukraine, both sides have deployed MALE UAS for intelligence, surveillance, target acquisition, and reconnaissance (ISTAR) and strike missions, although Kyiv has made use of its systems more extensively and proficiently than its Russian aggressor.[14]

Ukraine's Use of TB2

At the outset of the conflict, Ukrainian forces had some two dozen Turkish TB2 drones, which carry four smart laser-guided munitions and have an endurance of 27 hours.[15] The TB2 also sports a capable multi-spectral sensor payload for information collection and targeting that includes a day-night electro-optical/infrared (EO/IR) camera. Other payloads include multi-function laser targeting capabilities and a multi-purpose active electronically scanned array (AESA) radar.[16]

Thanks to its relatively small radar signature, the TB2 can be harder to detect with ground-based radars,[17] although its vulnerability increases significantly vis-à-vis multilayered integrated air defense systems that combines a variety of ground-based and airborne radars.[18] Given its versatile characteristics, the TB2 has typically been used to:

- spot and illuminate targets for artillery;
- provide long-range ISR into the Black Sea;
- attack logistic units and time-critical targets;
- conduct battle damage assessment (BDA).



Ukrainian TB2s were also instrumental in the destruction of enemy air defenses (DEAD) in the first weeks of Russia's invasion.[19] According to open-source data based on visually confirmed losses in Ukraine during the first weeks of the war, the TB2 destroyed 15 air-defense systems – including Russia's advanced Pantsir-S1 (SA-22 Greyhound) and Buk-M2 (SA-17 Grizzly) – along with several artillery pieces and logistics equipment.[20]

The TB2s' success partly stems from Russia's slow deployment of mobile short and medium-range air defenses in the initial phase of the invasion.[21] However, Russia's capacity to counter Ukraine's use of drones is improving. Just a few weeks after Russia's initial attack, Russian forces started to commit their full air defense and electronic warfare (EW) capabilities, allowing Russia to shoot down Ukrainian TB2s in large numbers, with at least 18 visually confirmed losses at the time of writing.[22]

Russia's Use of Medium and Large-Size UAS

Russia's use of MALE UAS has so far had less impact. First, Russia has a limited number of platforms. Indeed, the operational MALE UAS fleet at the onset of the 2022 offensive consisted of a handful of indigenous Korsar and Inokhodets systems, and a few more Forpost-R drones – a licensed copy of the Israeli IAI Searcher Mk II. The first Inokhodets UAS was delivered by the Kronshtadt Group in April 2020[23] after extensive trials in Syria. As of mid-2021, at least three Inokhodets operated from an airbase near Kirovskoe in occupied eastern Crimea.[24] In the second half of 2022, Russia also received an unspecified number of Mohajer-6 multirole UAS from Iran, but their operational impact remains difficult to quantify.[25]

Similar to the TB2, these Russian and Iranian platforms have a range of 200-300 km with supporting ground relay equipment. They can also carry an array of both guided and unguided ordnance, including Kab-20 and Qaem-5 light precision-guided munitions (PGM), respectively, an air-launched derivative of the Kornet 9M113FM-3 anti-aircraft missile known as the Kh-BPLA, and the heavier Kab-50 guided/unguided bomb.[26] Based on open-source data, at least three Inokhodets, one Mohajer-6, and four Forposts have been shot down in Ukraine as of the writing of this report.[27]

The second factor impeding Russia's successful use of MALE is the lack of operational experience in using medium and large UAS in high-intensity environments, which is partly a byproduct of their limited number. In fact, despite having invested substantially in drone technology since at least 2008, Russia's at-scale MALE UAS production has never materialized.[28] The resulting limited inventory of MALE UAS has meant minimal integration of these systems with the Russian military, few opportunities for troops to train and familiarize with them, and neither development of an organic doctrine nor a mature concept of operations.

Photo: Dozor-600 at Engineering Technologies International Forum in Moscow, Russia, 2010.
Credit: Vitaly V. Kuzmin/Wikimedia Commons

Third, the skepticism over UAS among the senior ranks of the Russian military has likely hindered the integration of these strike-capable drones until very recently. The cause of this skepticism arises largely from institutional neglect rather than technological gaps.[29] As maintained by Russian military analyst Konstantin Makienko, "programs for the development of [combat] unmanned aircraft were not considered a priority in the research and development work of the Ministry of Defense."[30] As a result, the Russian military has both overemphasized ISR systems at the expense of armed UAS and more slowly adapted in light of lessons emerging from recent conflicts on the value of UAS for fires.

Turkish Medium-Size UAS

Among countries that have used or are using UAS in non-permissive combat environments, Turkey, which develops these systems indigenously, unsurprisingly seems to have the most mature and effective concept of operations, employing a "network-centric approach." For this approach, drones are deployed in conjunction with electronic warfare, long-range fires, and rapid command-and-control (C2) systems enabled by distributed sensor-fusion capabilities.

This architecture, which Turkish analyst Can Kasapoğlu defines as "drone-augmented battle networks,"[31] exploits UAS' force-multiplying role and proved particularly effective in Syria, suppressing and destroying the regime's Russian-made air defenses and other targets during Turkey's Spring Shield operation in March 2020.

Supported by electronic and signals intelligence (ELINT/SIGINT) CN-235 special mission aircraft, Turkish land-based Koral EW systems[32] and the EW suite on board the TAI Anka-I, UAS located and blinded the Syrian air-defense radars and paved the way for a strike campaign by TB2s, Anka-S drones, and long-range guided artillery. At the same time, armed UAS identified targets for Turkish artillery and provided close air support (CAS) to Turkish ground forces.[33]

Azerbaijan's quick success against Armenia later in 2020 also relied on a similar concept of operations. Baku's forces employed a mix of repurposed unmanned decoys and EW systems to deceive, saturate, and locate Armenia's Soviet-legacy air defenses, which were subsequently destroyed by long-range Israeli-made Harop loitering munitions and TB2s acquired from Turkey.[34] According to military expert and author John Antal, "the war waged in Nagorno-Karabakh was a watershed, [marking] the first conflict in history won primarily by robotic systems."[35]

Nevertheless, some of this success was due to Armenia's poor operational planning and air defense limitations—an attribute that is difficult to measure and frequently omitted from assessments. As noted by some analysts, Armenia's air defense infrastructure mostly relied on Soviet-legacy systems, including the 9K33 Osa and 9K35 Strela short range air defense systems (SHORAD) – incapable of targeting high-flying drones like the TB2 – and long-range modernized S-300PS, which are not optimized for C-UAS missions.[36] The latter S-300PS were destroyed early in the war by Harop anti-radiation loitering munitions.[37]

Furthermore, Armenia lacked enough EW capabilities to complement its air defense network and effectively disrupt Azerbaijan's drone operations. Baku's combined use of loitering munitions and small and medium UAS succeeded mostly because Armenia's anti-access/air denial (A2/AD) systems were not prepared to counter the more sophisticated Azerbaijani employment of UAS.

Survivability of Medium and Large-Size UAS

The employment of MALE UAS was less successful in other recent conflicts. The TB2 and Chinese-made Wing Loong I and II suffered high attrition in Syria[38] and Libya, even in operational contexts characterized by modest air defenses. Overall, at least 10 Wing Loong family UAS and many more TB2s used by the forces loyal to Libyan General Khalifa Haftar and the Tripoli-based Government of National Accord (GNA), respectively, were shot down in Libya between April 2019 and July 2020.[39]

The success of the GNA's TB2 against modern Russian-made Pantsir air defense systems (ADS) – which on paper can track and engage the drone before it comes close enough to launch its 14 km-range smart munitions – is likely due to the lack of supporting EW capabilities among Haftar's forces and the inadequate proficiency

and readiness of air defense operating crews. Some of the destroyed Pantsir, for example, had their radar switched on when hit.[40]

The issue of UAS survivability, including in semi-permissive scenarios, also affects high-end MALE UAS such as the US-made MQ-9 "Reaper." For example, one Italian and at least two US MQ-9 UAS were downed over Libya between 2019 and 2022, likely by Pantsir ADS operated by the Russian private military company Wagner Group.[41] Back in 2013, then-commander of the US Air Force's Air Combat Command, General Mike Hostage, candidly described MALE UAS such as the MQ-9 as being "useless in a contested environment" and vulnerable even against "countries with the most minimal air force."[42]

Although MQ-9's vulnerability may be exaggerated, the survivability of medium and large UAS in non-permissive scenarios remains a key challenge and poses major doctrinal and tactical questions for their use against peer and near-peer competitors.

B) Small Military and Commercial UAS

Cheap, small commercial UAS have become staples for both Ukraine and Russia in the ongoing conflict. The military use of these smaller systems is not new. Terrorist organizations and non-state armed actors such as the Islamic State and the PKK Kurdish separatist group have repeatedly used commercial rotary-wing drones to conduct tactical ISR and drop small munitions against military targets in Syria, Iraq, and Turkey.[43] Drug cartels and other organized armed militias around the world haven taken inspiration and developed similar low-tech, cheap "air capabilities."[44]

Both sides in Ukraine have deployed small commercial rotary-wing drones such as Chinese-made DJI's Mavic and Matrice series, most of which have been sourced from crowdfunding. These UAS have become ubiquitous along the forward line of troops (FLOT) and provide crucial real-time ISR, battle damage assessment, and fire correction for artillery units thanks to full-motion video feed and thermal vision capabilities for night operations.

Employing many small, less expensive UAS often compensates for their limited endurance and vulnerability to EW and small-arms fire. Both Russia and Ukraine have also weaponized these systems, utilizing them to drop a variety of fin-stabilized munitions[45] or flying them as improvised first-person view (FPV) kamikaze drones to strike both equipment and personnel with remarkable effect.[46]

FPV drones, which are piloted with hand controllers and a headset that shows a live video feed from the drone's nose camera, are cheaper, faster, and more maneuverable than other commercial quadcopters and allow for attacks beyond line of sight (e.g., behind cover and concealment, in trenches, in buildings).[47]

Photo: Donbas Region, Ukraine - February 14, 2023: Drone operators of Ukraine army. Credit: Kish Kim/Sipa USA/Alamy Stock Photo

The Ukraine-made Wild Hornet FPV UAS, for example, costs a fraction of the price of a DJI Mavic 3 ($400 vs $2,000), has a larger payload, and can be customized to function at different ranges and signal frequencies.[48] This means the UAS is more resilient against EW and can be equipped with more explosives, including rocket propelled grenades for specific anti-tank missions.[49] By way of their cost-effectiveness and long-range, they have rapidly become key weapons to take out even the most modern main battle tanks like the Russian T90, at the cost of a few hundred dollars.[50]

Recent months have seen a surge in attacks by Ukrainian FPV UAS against Russian units and key systems (e.g., armor, fighting vehicles, artillery), with significant results.[51] Furthermore, Ukraine is now introducing a new AI-powered FPV attack drone – called Saker Scout - that autonomously detect and pinpoints the coordinates of enemy equipment, day or night, even when concealed, and can also operate in swarms.[52] If confirmed, this development would mark a major milestone in the deployment of autonomous systems in the conflict.

Russian forces are mimicking their adversary and increasing the use and production of FPV UAS, often through crowdfunding and private donations.[53] In April, the Kremlin announced a plan to order $1 billion worth of drones by 2026, and more than double that figure ($2.2 billion) by 2030.[54] In recent months, Russia has been able to deploy more drones along the FLOT, improving situational awareness and the accuracy and speed of its artillery fire.[55]

Overall, in Ukraine, commercial drones have complemented and often replaced the work of other small military-grade UAS such as the Russian Orlan-10 and the Ukrainian Shark and Leleka-100, despite lacking key targeting capabilities like laser-marking and range-finding. Their vulnerability in heavily denied and EW-saturated environments means that the average life span of commercial drones, however, rarely exceeds a few days.[56]

The panoply of UAS used by both Ukrainian and Russian forces has created widespread capability inconsistencies among units and has complicated management of training and standardization. To address this problem, both Ukraine and Russia are focusing on the production of a few, specific military UAS that can guarantee better performance at reasonable costs.

Ukraine has recently pushed into service the domestically produced Shark UAS, which offers high-quality ISR – including a ground moving target indicator (GMTI) – at a low-entry price.[57] The Punisher produced by UA Dynamics is another domestically made, privately funded small UAS which carries a small 3 kg payload, can fly up to 30 minutes, is GPS guided, and has a reportedly high success rate against a variety of Russian targets.[58]

In a similar vein, Russia has expanded the production of the Orlan-10 multirole UAS,[59] the workhorse of its drone fleet. The Orlan-10 can be equipped with a variety of different payloads, including EO/IR, laser imaging, detection and ranging (LIDAR) sensors, and electronic warfare capabilities depending on the mission assigned.[60] Kyiv's forces also employ military UAS provided by Western partners, including US-made ScanEagle and Puma ISR drones and Vector UAS produced by the German company Quantum Systems.[61]

Ukrainian Whole-of-Society Support

Overall, Ukraine has harnessed drone technology more than its opponent. One reason for this advantage lies in Ukraine's comprehensive approach to technological innovation, whereby the private sector, civil society, academia, and the government have joined forces to exploit a fertile domestic technological ecosystem to deliver quick solutions to the military.[62]

Photo: ZAPORIZHZHIA REGION, UKRAINE - JANUARY 27, 2024 - v are seen at work, Zaporizhzhia region, southeastern Ukraine. Credit: Ukrinform / Alamy Stock Photo

A prominent example of Ukraine's innovation ecosystem is the "Army of Drones" initiative lead by the young Deputy Prime Minister for Innovation, Education, Science and Technology, Mykhailo Federov.[63] The initiative includes rapid battlefield feedback loops between drone operators and developers, leveraging public and growing private funding, and most importantly scaling production and training.

This combination of bottom-up and top-down contributions fits into a broader approach that Ukrainian expert Hanna Shelest defines as Ukraine's "third way" between the "total defense" model of Sweden, Finland, Singapore, and Switzerland, and the strongly hierarchical model of the United States, Russia, and China.[64]

Another telling example of the Ukraine model is the Iziviz startup, which before the war was making drones used for inspections in the construction sector and is now providing UAS solutions to the Ukrainian military.[65] Another case is the famous "Aerorozvidka" team, which began as a group of volunteer drone and IT enthusiasts in 2014 and is now a structured nongovernmental organization (NGO) that provides

drones and dedicated training to the Ukrainian armed forces.[66] Many more private drone schools and NGOs are training thousands of UAS pilots for the army.[67]

Through constant experimentation, rapid refinement, and exploitation of civilian quadcopters as well as other small military drones, the Ukrainian military has developed robust concepts of operations and TTPs that have been further refined against Russian troops since February 2022.

Thanks to the availability of small commercial UAS, Ukrainian forces down to the platoon level have access to persistent, tactical ISR. This means better situational awareness, improved coordination with nearby units, and more accurate artillery support, among other advantages. Better situational awareness can be leveraged to seize opportunities, while organic ISR capabilities allow small units to retain a fair degree of operational flexibility even when communications are disrupted.

Perhaps most importantly, the outsized role played by small drones has prompted unprecedented reforms in Ukrainian military force structure, including:

- the creation of a full-fledged "drone army" comprising 60 new attack-drone squadrons – at least one in every brigade – led by separate staff and commanders;[68]
- classified updates to the country's military doctrine to fully harness drones' military potential;
- the creation of new institutional bodies[69] such as a new board within the Ukrainian Ministry of Defense that will coordinate the acquisition and supply of UAS, with a budget of $540 million in 2023.[70]

Russian Experience with Commercial UAS

Russia's approach to commercial drone technology by comparison seems more reactive and hampered by the same slow adaptation that has delayed the development of its UAS sector vis-à-vis its competitors. Despite the common use of small commercial quadcopters by Russian forces[71] and measures taken to address the chronic shortage of tactical military-grade UAS among Russian units,[72] there has been limited enthusiasm and action to integrate new drones, especially among senior military ranks.[73]

Experimentation among Russian forces in combat of commercial UAS has often been hindered and considered of secondary importance.[74] A notable exception is the Sparta Battalion, a unit of the breakaway Donetsk People's Republic (DPR), which has embraced commercial drone technology and extensively used drones in its operations.[75] While Russia has significantly scaled up UAS production over the

past few months, soldiers have often resorted to buying their own drones rather than relying on military supplies.

Overall, due to their low price, user-friendliness, and large availability, commercial drones will continue to play a role in Ukraine and other future conflicts alongside military-grade systems. However, commercial UAS typically have inferior capabilities in terms of range, payload, sensor quality, etc. and entail risks in terms of encryption and vulnerability to EW.

C) Ukraine is Leveraging Other Private Sector Technologies and Support

The Ukrainian battlespace features a converging pattern of global big-tech companies, volunteer enthusiasts, NGOs, and the private sector playing a major role in developing solutions to military challenges and thus shaping military outcomes against an aggressor which enjoyed a tenfold larger defense budget on the eve of the invasion.[76] Examples abound. Kyiv's forces have exploited commercial satellite imagery provided by private firms like Maxar Technologies and Capella Space to monitor Russia's buildup and improve operational planning.[77] Google maps traffic updates have helped the Ukrainian military to track Russian movements and logistics.[78]

Thousands of Starlink low-orbit satellite-based communication terminals have enabled Ukrainian units, civil authorities, and households to communicate despite Russia's intense cyber and EW offensive.[79] Starlink has also served as a key enabler for the use of UAS in heavily GPS-denied environments. Despite limitations imposed by the holding company, Elon Musk's SpaceX, Ukrainians have been able to find workarounds.[80]

Additionally, drones have been integrated into a cloud-based comprehensive situational awareness digital map, called "Delta." [81] Developed by the Ukrainian military with seed money from a NATO trust fund, this tool delivers a detailed picture of the front line, providing the real-time position and information of both Ukrainian and Russian units, and tracking changes based on user inputs. Delta is accessible to strategic headquarters and tactical units alike and fuses information from multiple sources and distributed sensors behind and beyond the FLOT, including ISR from UAS, smartphones, radars, satellite imagery, and open-source intelligence (OSINT).

This innovative situational awareness tool, in turn, can feed specific software that assists intelligence gathering, observation, and targeting for artillery fires, tracking of enemy movements, and coordination among Ukrainian forces. Tools like GIS Arta for Artillery and the Android-based Kropyva "Nettle" App, for example, allow soldiers to quickly share the coordinates of enemy units, which are immediately engaged by the nearest artillery battery.[82]

These software applications have dramatically expedited Ukraine's targeting process, improving timeliness and effectiveness, and closing the gap in one of Russia's expected military advantages. *Kropyva*, which was developed by Ukraine's Army SOS NGO with US support in 2014, features a user-friendly interface that runs on Android tablets and can also be used by air defense and armored units at the tactical level.[83] Logically, drones represent a core component of these applications.

More recently Ukraine drone developers have been focused on mitigating another Russian advantage, numerous powerful EW jammers. Supported with government-shared battlefield technical data, manufacturers and programmers are working on AI solutions to allow small drones to strike their identified targets even after loss of communications.[84] Other enhancements include whisper quiet motors and designs to reduce visible and electronic signatures.[85]

These examples confirm that the effectiveness of UAS depends on their integration into a complex battle management architecture that leverages the synergy between different capabilities and technologies, such as:

- fused, multi-source intelligence;
- artificial intelligence tools;
- electronic warfare;
- resilient communications networks;
- tactical command and control;
- integrated fires nets.

In the case of Ukraine, the creation of this battle management architecture is the result of years of unique, field-tested lessons learned, the creation of a specialized workforce capable of guiding such developments, and a whole-of-society response to Russian aggression.

D) Loitering munitions

Loitering munitions (LM) are another prominent air capability that has emerged in Ukraine and other recent conflicts. These systems generally combine the expendability of missiles with drones' advanced targeting and sensor capabilities as well as longer endurance.

Loitering munitions can be considered smart missiles which, rather than homing in on a preselected target via a preplanned route as traditional land-attack missiles do, orbit over a wide area in search of targets leveraging their multi-spectral sensors and energy-efficient propulsion.

A key aspect of loitering munitions is their ability to condense and simplify the sensor-to-shooter cycle by incorporating sensing and striking capabilities on a single platform. This ensures the shortest time loop between target acquisition and engagement, thus making these platforms ideal assets to strike time-critical targets and targets of opportunity while providing persistent ISR.

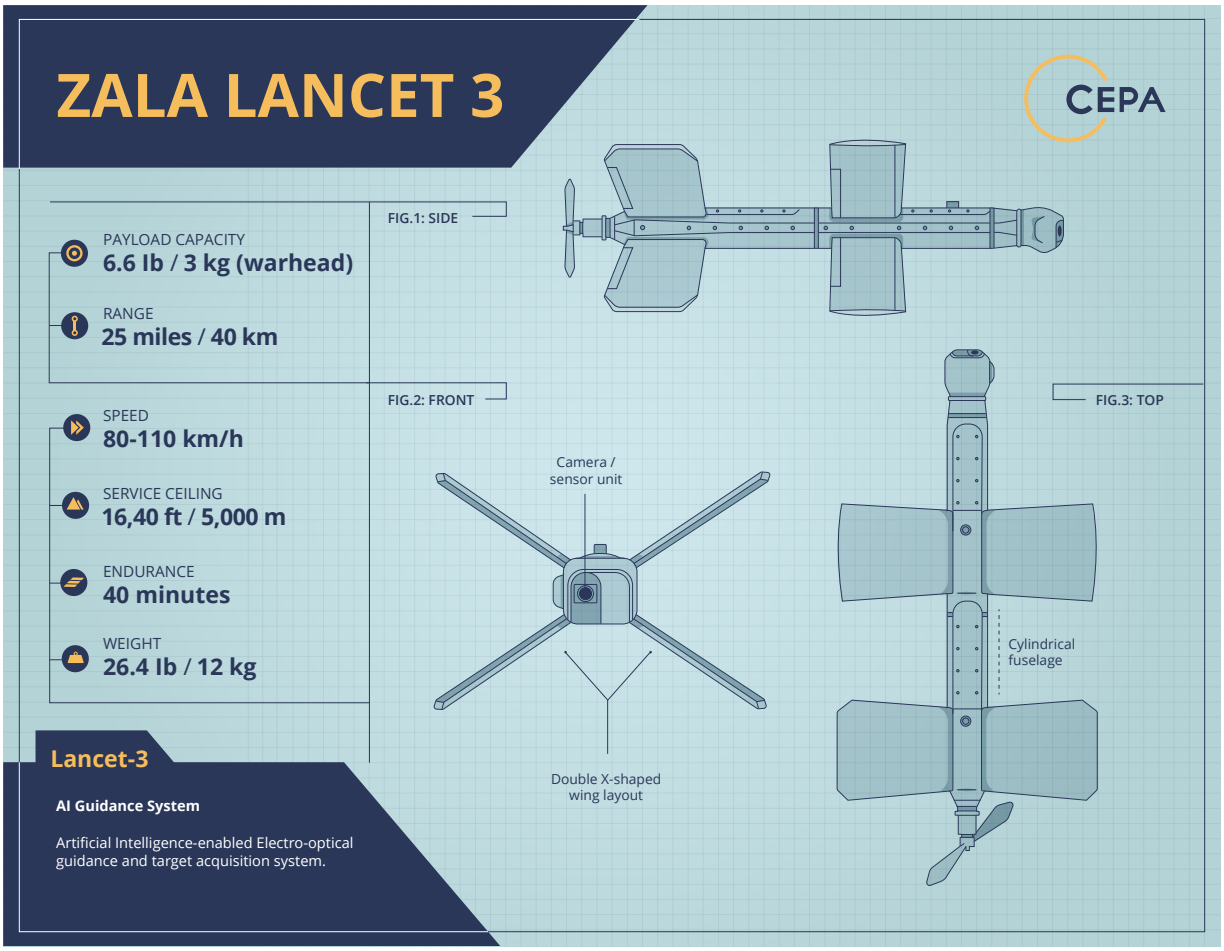
The variety of available warheads and loitering munitions' low electromagnetic and acoustic signatures allow for broad mission sets, including the suppression and destruction of enemy air defense (SEAD and DEAD, respectively). So far, available evidence suggests that these systems have been used via human-in-the-loop control, although several platforms include autonomous features like AI-enabled target selection and navigation. Autonomy – including swarming capabilities – is poised to become a more prominent characteristic of these weapons in the near future.

Russian Use of Loitering Munitions in Ukraine

Russia has so far demonstrated superior LM capabilities, employing its own Kub and Lancet-3,[86] , along with the Iranian-made Shahed 136 and 131 variants. While available evidence shows mixed results for the short-range and lightly-armed Kub, the Lancet-3 – which has a range of 40 km and an endurance of 40 minutes[87] – has become a thorn in Ukraine's side, particularly for Ukrainian artillery units.[88] Russia deploys the Lancet for counter-battery fire missions and against time-critical targets along the FLOT and at tactical depth.

Russian forces usually employ the Lancet-3 along with Orlan-10 and Zala ISR drones, despite the former's EO guidance and loitering nature, likely to maximize spotting opportunities and to have an independent, accurate battle damage assessment after the Lancet's strike.[89] According to the producer, the Lancet-3 can operate as a fully autonomous system, with AI-enabled navigation and autonomous target acquisition and engagement.[90] This reduces the need for data and navigation links with the operator and renders the Lancet-3 more resilient against certain EW techniques (e.g., jamming, spoofing), explaining the remarkable success of this weapon.

Russia has also deployed large numbers of the Iranian delta-wing Shahed-136 and lighter Shahed-131 (rebranded Geran 2 and Geran 1, respectively) systems. These platforms are more akin to slow propeller-powered missiles than loitering munitions, given their lack of EO sensors and their reliance on a combined global navigation satellite system (GNSS) and inertial navigation system (INS) guidance suite to strike preselected stationary objectives. Russian forces have used the Shaheds to target power infrastructure and military installations with good results. The Shahed's small radar cross section (RCS)[91] and slow speed make it harder to detect at long range, especially for ground-based radars. Meanwhile its affordability and the integration



of anti-jamming and anti-spoofing GNSS controlled reception pattern antennas allow its use in GNSS-denied environments.[92]

As for other Russian precision weapons,[93] both Lancet-3 and Shahed-131/136s loitering munitions recovered by Ukraine have been found to contain several commercial and dual-use electronic components produced by Western countries, with 82% of them manufactured by companies based in the United States.[94] These include US-made Nvidia Jetson TX2 AI modules, contained in Lancet-3s and specifically designed for autonomous computing.[95]

Ukraine is Closing the Loitering Munitions Gap

Ukraine is rapidly closing the gap with Russia in loitering munitions. So far Kyiv's forces have mostly relied on foreign systems, including US-made Phoenix Ghost, Altius-600, Switchblade-300s and 600s, and the Warmate from Polish company WB Group.[96] However, Ukrainian units are now receiving additional indigenous platforms like the RAM II, produced by the Ukraine company CDET, which is based on the Leleka-100 UAS, has a 30km range, and uses a 3kg multitype warhead.[97] The RAM II, which is roughly comparable to the Lancet-3, has already scored several successes against Russian mobile air-defense systems and other military equipment.[98]

Use of Loitering munitions in Other Recent Conflicts

Besides Ukraine, loitering munitions were instrumental in securing Azerbaijan's victory in Nagorno-Karabakh. Israeli-made IAI Harops were deployed *en masse* against helpless Armenian air-defense systems. One-way slow-flying munitions have also proven to be a formidable asymmetric weapon in the hands of non-state armed groups such as the Houthis in Yemen, which used Shahed-136s to repeatedly strike oil infrastructure in Saudi Arabia, defying interception from US-made Patriot air defense systems.[99] However, context-specific factors such as terrain, crew proficiency, and the specific radar frequency settings of the air defense systems also play a major role in the success or failure of drone operations.

Filling a niche between cruise missiles and armed UAS, loitering munitions provide great flexibility to accurately engage both line-of-sight and beyond-line-of-sight targets at operational depth and reduced costs compared to more expensive missiles. Furthermore, mass-deployed loitering munitions can saturate and overwhelm even the most modern air defense networks, proving ideal for SEAD and DEAD missions.[100]

E) Counter-UAS

Challenges in Defending Against the UAS Threat

Both Ukraine and Russia still experience significant challenges in defending their forces from UAS attacks. At present, there seems to be an overall lag between the UAS threat and available C-UAS solutions, especially when it comes to defeating large barrages of drones or drone swarms simultaneously converging on single or multiple objectives. Furthermore, the proliferation of cheap weaponized commercial drones as well as long-range loitering munitions and their ubiquity across the battlespace question the sustainability of traditional air defense alone and underscore the need for more cost-effective, diversified, and distributed C-UAS solutions.

While in Ukraine there is no available evidence (yet) of attack by swarming drones (i.e., large numbers of partially or fully autonomous interconnected and synchronized UAS), Russia has launched several mass-scale salvos of Iranian-made Shahed-136s munitions and different types of missiles against Ukrainian critical infrastructure, causing significant damage but failing to break Ukraine's fighting spirit and cripple its overall energy resilience.

According to a NATO C-UAS expert familiar with this issue, "the biggest challenge for Ukrainian air defenses is the detection and tracking of slow-flying and relatively small objects like the Shaheds."[101] The small radar signature and slow speed of these systems make them difficult to identify for Ukrainian air defenses, which at the

Photo: A Croatian soldier with the Croatian Air Defense Regiment uses a QR-07S3 drone jammer system to disrupt enemy drones as part of Exercise Shield 23, April 20, 2023 in Pula, Croatia. Credit: Sgt. Mariah Y. Gonzalez/ US Army

beginning of the invasion included upgraded Soviet-legacy platforms like S-300PT/PS, and a variety of short-range air defense systems not optimized against UAS and similar threats.

At the tactical level, loitering munitions and weaponized rotary-wing commercial UAS are also producing a significant cumulative impact in terms of casualties, which add to those caused by drone-corrected artillery fire.

Ukrainian Air Defense

The provision to Kyiv of highly capable Western platforms like the US-Norwegian-made NASAMS and German-made Iris-T short-to-medium range air defense system has significantly improved Ukraine's defense capabilities against the Shaheds, although at a high cost-per-interception ratio.[102]

Besides EW systems, compact C-UAS guns using high-power microwave and radio signals can be effective against rotary-wing commercial UAS at short range,[103] although their irregular distribution along the FLOT and among units on both sides has limited their effects.

Traditional anti-aircraft artillery such as Soviet-era ZU-23-2 and the German-made Gepard self-propelled radar-enabled anti-aircraft gun have offered a cheap and effective capability against slow-flying objects, including Shaheds.[104] The downside is the limited number of such systems to defend critical infrastructure, population areas, and forces over an immense territory.

The recourse to simpler, improvised methods has proven a useful C-UAS alternative to anti-aircraft artillery. Besides camouflage techniques, Ukrainian forces, for instance, have discovered the effectiveness of simple metallic nettings for protecting artillery pieces and equipment against Lancet-3 loitering munitions, which get entangled and fail to properly detonate.[105] The use of inflatable and improvised decoys, especially by Ukrainian forces, may also mitigate the threat from UAS and loitering munitions, underscoring the timeless importance of deception even on a sensor-saturated battlefield.[106]

Russian Air Defense

Russia, for its part, has deployed an effective A2/AD envelope that has degraded Ukraine's ability to deploy TB2 combat drones close to the forward line of troops. Ukraine's initial success in the first weeks of the invasion is likely due to the fact that Russian A2/AD capabilities over occupied Ukraine were not sufficiently concentrated nor fully established.

Moscow's forces have had more difficulties denying the use of airspace over the Black Sea and the nearby Ukrainian southern coast, where TB2s have continued to provide uninhibited long-range ISTAR. A combination of geographical limitations, limited A2/AD assets, and the consequences of the loss of the naval command-and-control platform Moskva in April 2022 in which the TB2 played an important role can explain Russia's less successful C-UAS efforts in the maritime domain.

Capitalizing on its stronger EW capabilities, Russia has also hindered the use of smaller UAS, including commercial platforms, by dazzling their sensors and jamming their mostly unencrypted satellite navigation systems and communications links.[107] The complementary use of different kinetic and non-kinetic interceptors like Man-Portable Air Defense Systems (MANPADS) and man-portable C-UAS guns from both sides has created a situation where, according to some estimates, 90% of drones employed are lost and their average operational life is limited to three to six sorties depending on the system in question.[108] A recent RUSI report, for instance, assesses that Ukraine may be losing up to 10,000 UAS per month, mostly to enemy EW.[109]

Nevertheless, Ukraine has repeatedly managed to fly medium-size commercial and military-grade UAS deep into Russian-occupied territory or Russia proper, striking military bases in Crimea and an oil refinery in the Rostov region.[110] A combination of

gaps in Russia's EW coverage,[111] good route planning, and optimization of Ukrainian UAS against ground-based radars may offer a plausible explanation.

More generally, these examples underscore the threat posed by slow and low-flying UAS and the inherent challenge in guaranteeing a layered C-UAS and air defense coverage over large areas. In this respect, it is worth noting that factors such as personnel experience, systems readiness, and terrain represent other important variables of the C-UAS equation.

As the next section will explore, the introduction of directed-energy weapons (DEW) (i.e., laser and high-power microwave) promises to revolutionize and make C-UAS much more cost-effective.

F) Lessons for NATO

Recent examples of UAS employment in armed conflict offer valuable lessons for NATO regarding the likely trajectory of UAS technology and the role UAS will play in future military operations.

There are challenges to survivability and the element of surprise on a transparent battlefield. The pervasive surveillance of the battlefield provided by UAS and their connection to precision fires significantly constrain the use of surprise and introduce unprecedented challenges for the survivability of personnel at all operational levels, from the FLOT to rear areas. This aspect has huge implications for maneuver operations, force survivability and design, and the overall conduct of land warfare against peer adversaries.

The dawn of a new UAS-enabled targeting network is now. The fusion of UAS and precision fires (short to long-range, surface-based, or aerial) into a fully digitalized C4ISR architecture combines real-time situational awareness with precision-fire capabilities and drastically accelerates the targeting cycle, allowing for quick and accurate engagement of targets with devastating effects. As previously described, in Ukraine small commercial and military-grade UAS feeding into user-friendly situational awareness software such as GIS Arta and Kropyva ("Nettle") have reduced the time between target identification and engagement by the nearest artillery units to a few minutes. A distributed, resilient, and scalable C4ISR architecture that fuses multiple ISR sources with C2 and fires platforms is essential for preserving information dominance and expediting the kill chain.

Ubiquitous small military and commercial UAS pose a serious threat. UAS employment extends beyond the traditional ISTAR mission set and includes strikes with smaller munitions, loitering munitions, battle damage assessment, and kamikaze missions at tactical range. The pervasive threat small UAS pose increases the stress for frontline units (requiring an unprecedented degree of vigilance and

Photo: German Rheinmetall KZO drone being launched during Iron Wolf II exercise in Lithuania. Credit: NATO

protection from the threat above or from any exposed flank) and degrades combat effectiveness of the less prepared units over time. As the conflict in Ukraine shows, the cumulative and extremely cost-effective impact of weaponized COTS drones in terms of casualties and destroyed equipment can be substantial and should not be underestimated.

Quantity has a quality of its own. The high attrition rate suffered by UAS of all classes in contested environments underscores the need to incorporate large numbers of UAS (cheap and expendable when possible) for tactical and operational ISR at all echelons, and to have the industrial capacity and resources to replace them at scale. Self-protection capabilities for UAS to mitigate kinetic and non-kinetic threats are a recent development and will be likely introduced to enable survivability for more expensive and capable UAS. Investing in a balanced mix of expendable small and medium UAS and high-end MALE and HALE UAS will be important to account for their vulnerability to modern, layered air defenses.

The private sector has become an essential player and a key stakeholder in matters of defense and national security, with an increasing spillover of civilian technology and innovation in the military realm. The ability to harness innovation and quickly acquire, integrate, and proficiently employ novel technologies at scale are keys to success in modern warfare. Besides adequate resources, this ability

and agility will depend on flexible institutional and bureaucratic arrangements to experiment and rapidly adapt, acquire and integrate new technologies.

Drones are not game changers by themselves. Despite the hype surrounding UAS, their effectiveness depends on their integration into a wider military ecosystem centered on mutually supporting and enabling capabilities, including combined arms formations; EW, cyber, and space capabilities; C4ISR (including multidisciplinary intelligence); and naval and air power capabilities (depending on type of UAS in question).

As the role of UAS in defense capabilities increases, other considerations for their successful integration include the recruitment and training of qualified human resources, ranging from operators to analysts and support personnel to leaders of UAS formations and other supported forces. Additionally, doctrine and concept development; material, digital, and operational standards; organizational structures; and dynamic civil-military cooperation will be needed. Establishing such a military ecosystem will not be easy, especially in a multinational environment like NATO, and will require investments, political leadership, and joint defense planning involving all military branches.

UAS pose a greater threat when deployed in groups, including with other types of UAS and crewed systems. By employing sheer mass, collaborative or swarm tactics, UAS can overwhelm and quickly change the cost-benefit ratio of traditional air defense systems, reveal their positions, and pave the way for the use of additional weapons and assets. Defense against drone groups and swarms requires not only cost-effective countermeasures but also the computational and processing capacity to rapidly detect, track, and intercept myriads of threats simultaneously.

While employing UAS with crewed systems has not yet been tested in combat, militaries are widely experimenting with human-machine teams in concept and capability development. Human-machine teams promise to significantly enhance both offensive and defensive capabilities of the forces that employ them, but will also require data and network architectures, training, and leader development to exploit the human-machine potential.

C-UAS is essential across all domains and at all echelons. As drones (including loitering munitions) become cheaper, expendable, more capable, and more numerous on the battlefield, the use of traditional air defenses to counter them becomes technically less viable and less and less cost-effective. As such, a combination of passive (concealment, electromagnetic discipline, dispersion, nets) and active countermeasures becomes essential against UAS and other smart munitions. Active countermeasures must ideally include a layered combination of traditional kinetic effectors, including anti-aircraft guns, and non-kinetic means like EW, directed-energy weapons, and other drones.[112]

The roles and missions of drones are expanding. Combat UAS have expanded options for SEAD/DEAD missions, close air support, air to air engagement, and even air combat[113] besides their traditional ISR, targeting, and strike functions. Stealthier next-generation UAS equipped with long-range air-to-air and air-to-surface munitions will be able to penetrate hostile airspace and conduct counter-air missions, electronic warfare support, escort, and in-depth interdiction, alone and in close cooperation with crewed aircraft.[114] Furthermore, UAS will perform resupplying and air refueling missions, provide advanced tactical data link relay, improve anti-submarine warfare, and release other drones and loitering munitions. Finally, other technological improvements, such as in sensing, computing (onboard and cloud), AI, lasers, and next generation networks, will further expand the roles of drones in C4ISR, air and missile defense, and targeting in general.

Photo: A Portuguese Unmanned Aerial System (UAS) Ogassa OGS 42 drone stands ready for takeoff during NATO Exercise REPMUS 22. Credit: NATO

Part II - Assessing NATO's Current UAS Capabilities

Individual allies own a wide variety of UAS capabilities, and the alliance collectively owns and operates NATO's Alliance Ground Surveillance (AGS). Despite NATO efforts to encourage procurement and capability development and to promote common standards and enabling capabilities, NATO has too few drones for a high-intensity fight against a peer adversary. It would be severely challenged to effectively integrate those it has in a contested environment.[115]

NATO's drone capabilities are diverse and vary among allies. Many countries possess advanced drone systems ranging from small rotary-wing UAS to large fixed-wing platforms that can be used for a variety of military operations. While the quantity and quality of UAS contributions from member states to meet NATO's intelligence collection needs are increasing,[116] allied efforts to transfer capabilities under NATO control or to promote multinational capability development are often constrained by national concerns including limited availability, loss of control, or intellectual property rights and fear of market share loss.[117]

Equally important, NATO does not have an allied joint doctrine covering the employment of UAS in contested scenarios, although allies are working to develop one.[118] The lack of NATO doctrine has inevitable implications for the definition of capability requirements, concept of operations (CONOPs), common TTPs across the alliance, and ultimately achieving interoperability.

Indeed, a shared doctrinal document is necessary to steer the alliance's development of its drone capabilities, at a time when new operational requirements call for a shift from remotely operated, single-mission platforms to more complex, autonomous, multi-mission systems, and crewed-uncrewed platform integration.[119]

A) Air and Land Domains

This section delves into the major UAS capabilities of NATO nations in the air and land domains, which have substantial overlap in terms of platforms, sensors, and mission sets. While large UAS tend to be operated by national air forces for traditional air power tasks, small and medium UAS may be operated by air, land, or special forces for a variety of air and land power tasks.

Thus, for this report's purpose, examining UAS capabilities by size is more useful than attempting to do so by an artificial division between their employment in air and land domains. More specifically, the section examines UAS capabilities in each of the three NATO UAS classes – from larger Class III UAS down to mini and micro systems in Class I. The NATO UAS classification is illustrated in the table next page.

NATO UAS Classification

Class	Category	Normal Employment	Normal Operating Altitude	Normal Mission Radius	Primary Supported	Example Platform
Class III (>600 KG)	Strike/Combat	Strategic/ National	Up to 65,000 ft Mean Sea Level (ft MSL)	Unlimited (Beyond Line Of Sight)	Theater	MQ-9 Reaper
	HALE	Strategic/ National	Up to 65,000 ft MSL	Unlimited (BLOS)	Theater	RQ-4D
	MALE	Operational/ Theater	Up to 45,000 ft MSL	Unlimited (BLOS)	Joint Task Force	Heron, Bayraktar TB2
Class II (150-600 KG)	Tactical	Tactical Formation	Up to 18,000 ft Above Ground Level (AGL)	200 KM (Line Of Sight)	Division, Brigade,	Watchkeeper
Class I (<150 KG)	Small (>15 KG)	Tactical Unit	Up to 5,000 ft AGL	50 KM (LOS)	Battalion, Regiment	Scan Eagle
	Mini (<15 KG)	Tactical Sub-Unit (Manual or Hand Launch)	Up to 3,000 ft AGL	Up to 25 KM (LOS)	Company, Platoon, Squad	Skylark
	Micro (<66 J*)	Tactical Sub-Unit (Manual or Hand Launch)	Up to 200 ft AGL	Up to 5 KM (LOS)	Platoon, Squad	Black Hornet

Source: "NATO Standard AJP-3.3 - Allied Joint Doctrine for Air and Space Operations. Edition B Version 1," NATO, April 2016, p. 2-2, https://www.japcc.org/wp-content/uploads/AJP-3.3-EDB-V1-E.pdf.
*J stands for Joule.

Alliance Ground Surveillance

Program Overview

The Alliance Ground Surveillance program represents the sole UAS capability directly owned and operated by NATO which provides critical and long duration Joint ISR (JISR) platforms to the alliance. The AGS fleet, which comprises five RQ-4D "Phoenix" UAS, fixed and mobile ground and support segments, and advanced sensors, is stationed at the Sigonella Main Operating Base in eastern Sicily, Italy.

The AGS fleet is operated by the NATO AGS Force (NAGSF), which is under the operational command of NATO's Air Command stationed in Ramstein, Germany. From Italy the UAS deploy along the alliance's borders to perform all-weather, long duration, wide-area terrestrial and maritime surveillance, collecting vast amounts of data and providing in-theatre, near real-time situational awareness to allied commanders.[120]

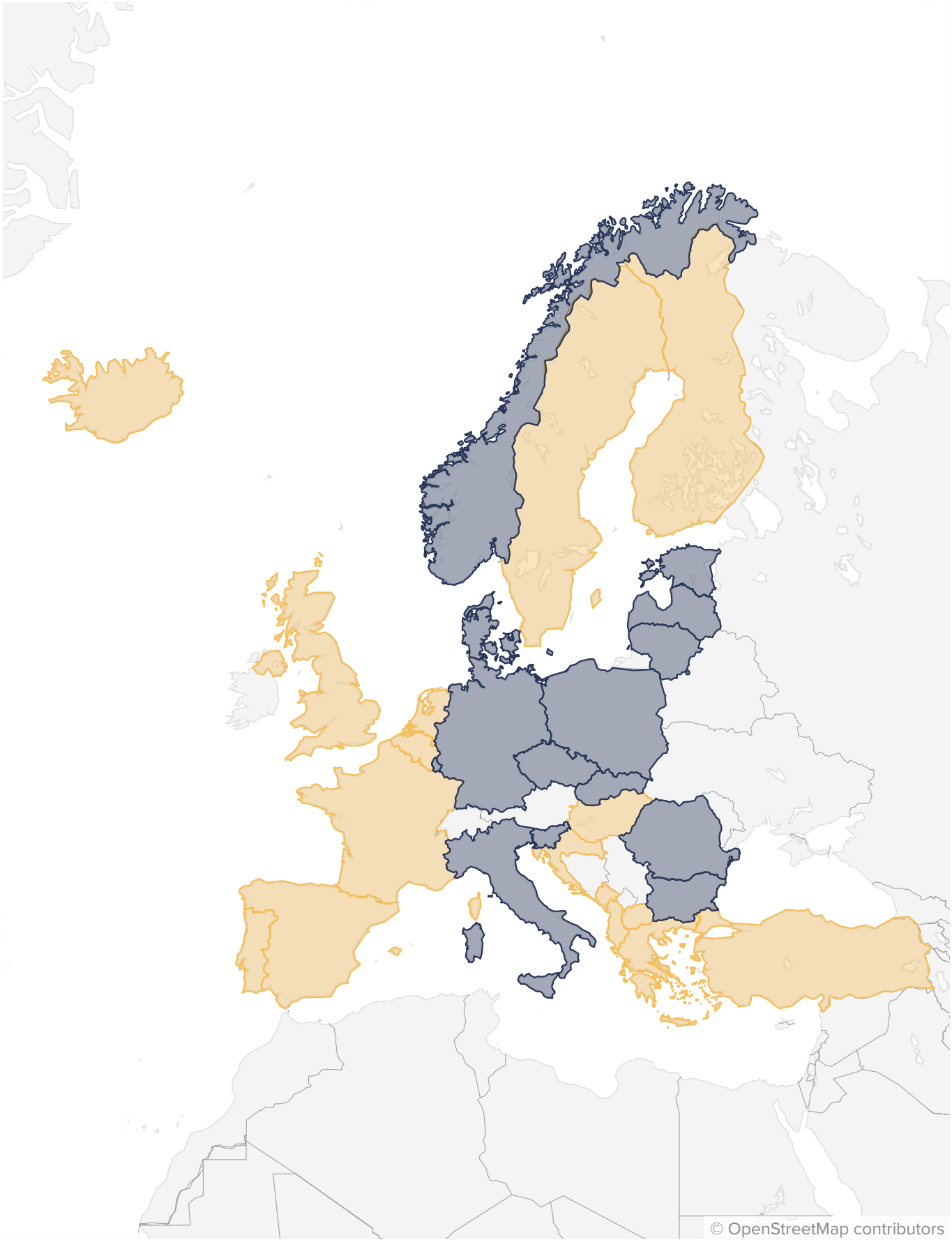
AGS' origins date back to 2009 when the program memorandum of understanding was signed by fifteen participating member states and the NATO Alliance Ground Surveillance Management Agency (NAGSMA) was established.[121] In 2012, the North Atlantic Council decided to collectively cover the costs for operating AGS for the benefit of the alliance, paving the way for the AGS acquisition contract with the RQ-4D's manufacturer Northrop Grumman. In 2021 the AGS achieved initial operational capability (IOC).[122]

The alliance needed the AGS capability "to fill a critical intelligence gap" that had been previously addressed by the contributions of single countries, resulting in inevitable lags and dissemination issues.[123] The RQ-4D Block 40 platform was selected because of its state-of-the-art sensor package, particularly the synthetic aperture radar (SAR) and ground moving target indicator (GMTI) functionalities provided by a multifrequency active electronically scanned array (AESA) radar, which allow NATO to monitor vast areas and track potential threats in near real-time.[124]

The AGS's sensor suite derives from the advanced multi-platform radar technology insertion program (MP-RTIP) on board the US RQ-4 Global Hawk UAS, but has been modified to meet the specific requirements of the alliance.

The "Phoenix" UAS, which according to NATO has a maximum ceiling of 18.2 km and a range of more than 16,113 km, provides near-instantaneous data transfer to NATO's commanders through an extensive suite of line-of-sight and beyond-line-of-sight, long-range, wideband data links. Its impressive ceiling and standoff ISR capabilities allow the AGS system to collect critical intelligence while remaining outside the engagement zone of most air defenses, although this advantage

NATO Allied Ground Surveillance (AGS) Member and Non-Member States



NATO AGS Member

NATO Non-AGS Member

The United States is also a member of the NATO AGS System.

Map: Center for European Policy Analysis • Source: NATO

significantly drops against peer adversaries such as Russia and China. However, as the force commander US Air Force Brigadier General Andrew Clark, NATO AGS Force Commander, has pointed out, "the NAGSF is much more than a flying unit"[125] and comprises a critical ground and support infrastructure, with a multinational team of analysts that conducts the processing, exploitation, and dissemination (PED) of the raw data and information received from the UAS.[126]

NAGSF provides an "organic collection capability for ground radar imagery and moving target patterns," in-depth analysis, and dissemination of intelligence products across the NATO enterprise, relying on mobile ground control stations and tactical C2 workstations for deployed forces.[127]

AGS' operating system is "platform agnostic" and thus designed to be interoperable with other NATO assets and platforms, allowing for seamless integration with other intelligence-gathering capabilities.[128] For example, NAGSF analysts "can combine the [high-resolution 2D] radar imagery provided by the RQ-4D Phoenix with other types of imagery intelligence (IMINT) like full-motion video (FMV) and ELINT/SIGINT products received from other high-altitude platforms such as the US U2 aircraft," to obtain a comprehensive picture of the operational environment.[129]

The Russian invasion of Ukraine has given new impetus to the cultivation of this capability as Russia's attack "accelerated the need for persistent ISR for the alliance," prompting NAGSF "to fly twice the amount envisioned upon reaching initial operational capability and delivering over 11 thousand intelligence products since February 24, 2022."[130] This intelligence output includes the integration of other intelligence-gathering capabilities, with only 25% of intelligence products originating from NAGSF organic collection and the remaining 75% deriving from external sources, including allied nations' platforms and open-source intelligence.[131]

NATO AGS Force should reach full operational capability (FOC) in 2024. With a total authorized force of around 600 personnel NAGSF is set to become the "clearinghouse of NATO's ISR."[132] However, this NATO capability also faces several challenges to achieving its full potential.

Challenges for NATO's AGS

The first problem lies in a lack of institutional knowledge concerning the organization's role and the system's capabilities, which could result in inappropriate or insufficient tasking."[133] This indicates the need for more effective coordination among NAGSF, Allied Command Operations, and other NATO bodies, including NATO Headquarters and the Joint Force Commands, in defining the intelligence requirements which shape the tasking of NAGSF's assets.

The need to better define taskings overlaps with the constraints in the federated PED process caused by the lack of human resources and the exponentially increasing amount of data to be analyzed and disseminated. AI-based analytical tools, along with more contributing analysts, can help reduce the burden on personnel and expedite the entire PED cycle. At present, specific AI tools provide automatic target identification during NAGSF PED process, but on a limited scale.[134]

The second challenge concerns NAGSF's future and its relevance in the medium to long-term. The RQ-4 is an aging platform without an active industrial production line. This raises the issue of diminishing manufacturing sources (DMS), with inevitable implications in terms of spare parts and life-cycle sustainment. In September 2022, Northrop Grumman was awarded a $13 million contract for sustainment of the AGS's radar and mission management computer, to be completed by September 2023.[135]

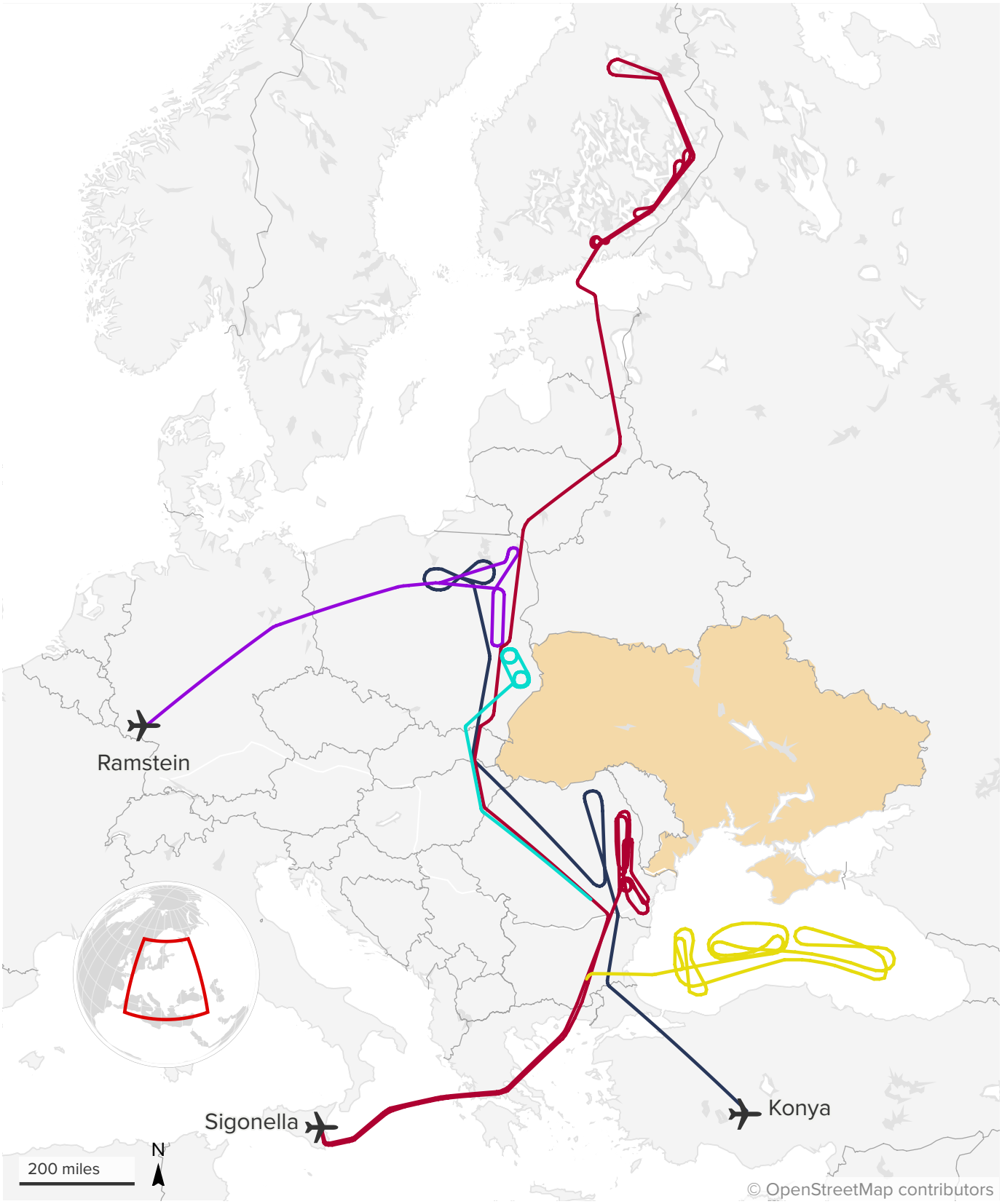
At the same time, reengineering options appear unfeasible. While the NATO Support and Procurement Agency (NSPA), which works to facilitate and harmonize the procurement of UAS across NATO, has encouraged industry partners to provide an assessment of the RQ-4 product line's future, discussions within the alliance on medium to long-term sustainability through substitution or replacement have not yet started.[136]

Further delays to decision-making stand to increase the likelihood of an ISR capability gap in the long term. Apart from addressing an aging platform, NAGSF's future relevance could also be enhanced by leveraging NAGSF's potential to command and control additional national contributions of JISR systems and units, or by leveraging its training cadre and analytic capacity to train analysts from across the alliance on a rotational or temporary basis. Sensor gaps exacerbate this limitation. According to the NAGSF commander, the NATO AGS Force would greatly benefit from SIGINT and long-range EO/IR payloads, which are currently missing and whose contribution must be provided by other platforms with inevitable implications for the TCPED process.[137]

The third challenge involves the RQ-4D's survivability, which many US military sources have acknowledged as being limited against modern air defenses.[138] For instance, in 2019, a US RQ-4A Global Hawk was shot down by an Iranian surface-to-air missile (SAM) when it was flying at a relatively high-altitude (~6.7 km) in international airspace over the Strait of Hormuz.[139] According to US Air Force Chief of Staff, General Charles Q. Brown, the RQ-4 operates very well "in uncontested and low-threat [contexts] where the United States and its allies enjoy superiority across all domains of warfare [but] cannot compete in a contested environment."[140]

Indeed, the RQ-4D does not have self-protection capabilities. As the AGS remains NATO's primary organic JISR asset, the alliance may soon need to assess possible solutions to increase its survivability and medium to long-term viability. Near-term upgrades may be possible, but eventually substitution or replacement will be necessary.

NATO UAS Intelligence, Surveillance, and Reconnaissance (ISR) Flight Paths



US Air Force RQ-4 Global Hawk

NATO Boeing E-3A Airborne Warning and Control System (AWACS)

Boeing E-8C Joint Surveillance Target Attack Radar System (STARS)

Boeing E-7T Airborne Early Warning Control Aircraft (AEW&C)

NATO AGS RQ-4D

Map: Center for European Policy Analysis • Source: Flight Radar 24

Class III UAS

A Limited, but Growing Allied Inventory

Excluding the AGS program, NATO's UAS capabilities are based on the systems allies possess and make available to the alliance. While the war in Ukraine has accelerated the development and acquisition of UAS among NATO nations, the speed and level of commitment varies across member states.[141] MALE UAS represent one of the categories where such disparities are most tangible. Only ten countries currently operate these large UASs. Of these ten, seven – including the US – employ the MQ-9.[142] Germany and Greece (and soon the Czech Republic)[143] use the Israeli-built IAI Heron TP.

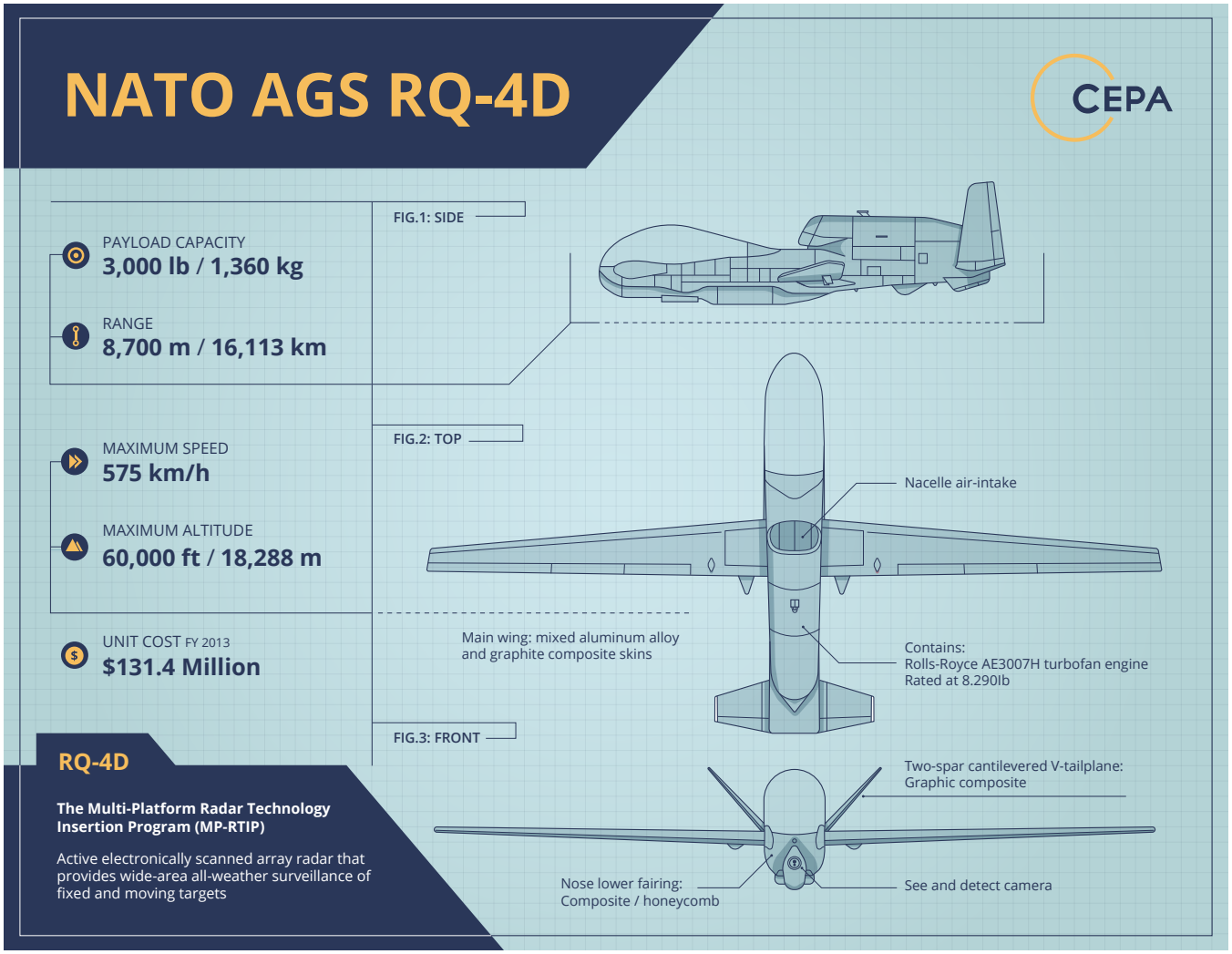
Turkey operates several domestically manufactured MALE drones like the TB2, the Anka, and the more advanced Akinci. Turkey recently introduced a maritime version of the TB2, the TB3,[144] which is capable of take-off and landing aboard Turkey's recently commissioned amphibious ship the TCG Anadolu (more on this will be in the maritime domain section that follows).[145] At the same time, Belgium, Canada, Germany, Greece, Norway, and prospective NATO member Sweden may have reached preliminary agreements or started discussions to purchase the MQ-9's upgraded version.[146]

Other member states such as Albania, Poland (already operating MQ-9As), and Romania have inked deals with the Turkish company Baykar for the acquisition of Bayraktar TB2 UAS.[147] The TB2 has also been the focus of discussions between Baykar and NATO members Hungary, Portugal, and Slovakia.[148]

France, which already operates the MQ-9A, will soon receive fourteen new Patroller MALE UAS produced by the French multinational Safran.[149] The NSPA is increasing its focus on the MALE category and will soon provide sustainment support for the TB2 to one ally.[150] The Agency does not currently deal with multinational UAS procurement but is trying to incentivize this option among allies. At the moment, though, most countries continue to favor national acquisitions.[151]

France, Germany, Italy, Spain, and their respective industries are collaborating on the "Eurodrone program," an ambitious EU-funded initiative that should deliver an initial batch of 20 MALE multi-mission UAS systems to the four countries starting in 2028.[152]

This mixed but fluid picture of Class III UAS operated by allies derives from a combination of factors, including fluctuating and diverse defense budgets, capabilities duplication and industrial competition, and different priorities vis-à-vis drone technology across the alliance. As a result, bringing consistent MALE UAS capabilities to bear will most likely require years, considering the various systems' production and delivery times and their later integration into national militaries and NATO force structures.



More and Higher Quality Assets Needed

While better-equipped allies can provisionally compensate for NATO's collective UAS capability gaps – as already done with other capabilities – the increasingly complex threat scenarios the alliance will face require a much larger number of interoperable UAS capable of integration in NATO command or force structure than currently available. In the words of NATO's Assistant Secretary-General for Intelligence and Security David Cattler, the war in Ukraine shows that "if you haven't invested in sufficient UAS capabilities, you're likely to have serious deficiencies against someone who has made the investment."[153]

To meet this need, it is vital that NATO countries increase their respective defense budgets to meet at least the 2% of gross domestic product (GDP) target. For those NATO countries unable to allocate additional resources and purchase more expensive UAS, stopgap options, including leasing, can fill capability gaps in the short term. Leasing is often disregarded but is a valid solution because it also comes with training and maintenance, thus laying the groundwork for a smoother integration of disparate systems.

As an example, General Atomics Aeronautical Systems has leased MQ-9As to Poland pending the arrival of the system's upgraded version purchase by Warsaw.[154] Furthermore, the same company offers a lower-cost service, contractor-owned, contractor operated (CO-CO), whereby General Atomics owns and operates the UAS while the ISR data is controlled by the customer.[155] Hence, a joint, multinational CO-CO scheme may represent an advantageous option for smaller member states with budget constraints to deploy key high-end UAS capabilities.

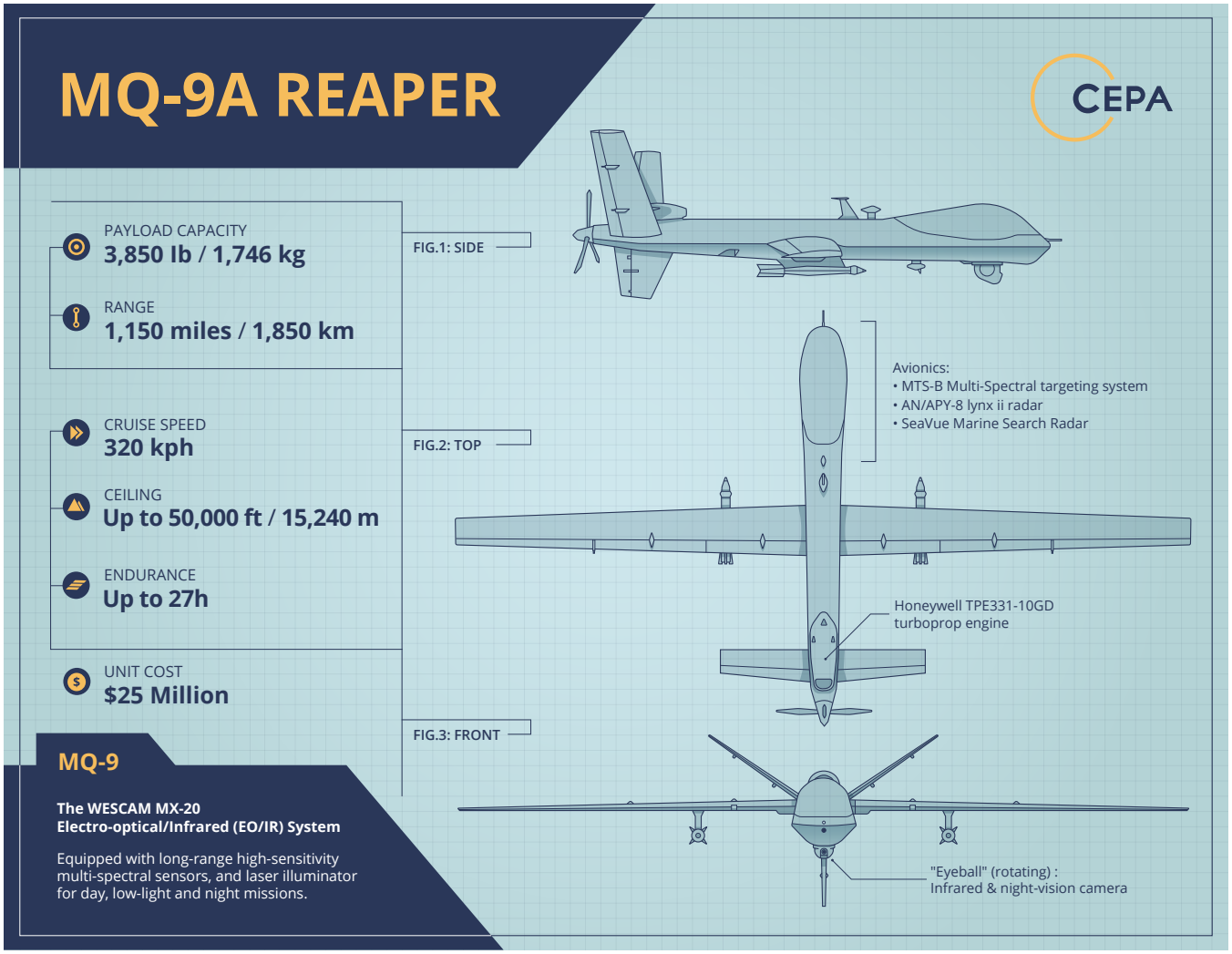
MALE drones provide not only persistent, high-quality standoff ISR but also EW and strike options, enhancing the warfighting utility and flexibility of allied UAS. Over the past few years, the US has deployed a limited number of MQ-9 UAS along NATO's eastern flank on a rotational basis, including in Estonia, Poland, and Romania. In the case of a full-fledged confrontation with Russia, however, a handful of MQ-9 would hardly be sufficient, considering the likely high attrition from hostile surface-to-air missiles and intense offensive EW and cyber operations.

Russian threat capabilities underscore the importance of robust and homogeneous MALE UAS capabilities across the alliance. The threat also highlights the need for a combination of high-end yet cheaper, more expendable systems (i.e., TB2, TB3) and next-generation autonomous "wingman" platforms able to conduct collaborative operations with crewed aircraft. The mission set for this class of drones will vary to include deep strike and reconnaissance into enemy territory, air combat and close air support, and interdiction in support of ground or maritime operations, among others.

Equally important, the possibility of equipping MALE UAS such as the MQ-9 and the Turkish-made Akinci with air-to-air missiles[156] and AI capabilities for advanced onboard computing and rapid target processing and engagement also expands their mission sets. MALE UAS so equipped could be used in counter-air, combat air patrol (CAP), and air combat roles in the future. At the same time, the integration of next-generation EW suites and standoff precision-guided munitions can pave the way for a more prominent use of these UAS in SEAD and/or DEAD missions.

Class II and Class I UAS

While MALE class UAS primarily support missions at the strategic and operational levels, medium and small drones, which have both comparatively limited duration and range, have become the most common tools for situational awareness and ISTAR at the tactical level. Capabilities in these classes of UAS are consistent across the alliance and revolve around multiple platforms. Examples range from the ubiquitous US-made RQ-11B Raven, RQ-20 Puma, and ScanEagle tactical UAS to the hand-launched Israeli-built Skylark to a variety of other national or foreign systems.



The “Support Partnership” initiative, a legal framework coordinated by the NSPA, offers cooperative support arrangements for ten countries for the acquisition and sustainment of military off-the-shelf UAS from nano/micro to tactical types and more.[157] According to Doug Heintz of NSPA, the Agency’s portfolio mainly covers platforms from the US and Israel, and a few from Europe, but it will soon include Turkish systems as well.[158]

Class I and II UAS usually have an endurance of approximately 60 minutes and a range of roughly 30-40 km, and trade payload for portability. As such, they are used for ISTAR purposes up to brigade-level units. Medium-size UAS such as Portugal’s Ogassa OGS 42 and Norway’s FX-450 provide greater capabilities, with ranges varying between 100 km and 250 km, an endurance of several hours, and the ability to fulfill the ISTAR needs of brigade-size units.

Several NATO countries have also expanded their UAS fleets with mini and micro UAS such as the 100 Black Hornet personal reconnaissance system (PRS), which provides squad-level immediate and covert situational awareness and has an

endurance of 25 minutes.[159] Mini and micro UAS are typically employed by special operations forces (SOF) and specialist units for very short-range ISR purposes.[160]

Certain member states are also investing in small bomber drones and loitering munitions. France, for example, has recently launched several projects to equip its armed forces with different remotely controlled munitions and attack drones, including a multi-rotor UAS capable of dropping up to twenty 40mm grenades.[161]

Italian special forces will soon receive Hero-30 loitering munitions, which are produced by the Israeli firm UVision and have a range of 15 km, to meet an "urgent mission requirement."[162] Other countries like Poland are betting on domestically designed loitering munitions such as the Warmate, while Estonia and Lithuania have placed orders for US-built Switchblade-300 and 600 loitering munitions.[163]

As a means for target acquisition, medium and small UAS have become essential tools for improving artillery accuracy and shortening the sensor-to-shooter cycle. At the same time, the battle damage assessment role of UAS tends to be underestimated, despite its critical importance for evaluating operational effects and avoiding wasted time and additional resources to obtain the desired effects on a target.

In light of the extremely high attrition rate these systems suffer in Ukraine and the open-source data regarding their availability among member states, **the alliance has nowhere near the minimum number that would be required in near-peer or peer adversary scenarios.** This means that allies should stockpile hundreds of medium UAS and several thousand small UAS – at the very least – along with the capacity to rapidly replace them if necessary. The war in Ukraine should be a wake-up call for NATO allies to significantly expand their medium and small UAS inventories and corresponding manufacturing capacity, with a balance between expendable and reusable systems.

B) Maritime Domain

Increasingly, the alliance is focusing on the role and use of UAS in the maritime domain. Maritime unmanned systems (MUS) include UAS, along with uncrewed surface and underwater vehicles (USV/UUV), and represent ideal assets which can operate in challenging sea conditions while offering several advantages.

First, they allow allies to conduct persistent, long-range maritime ISR and engagement over larger areas and with lower electromagnetic signature assets.

Second, they diminish the need to deploy sailors or marines into harm's way, thus reducing the risk of casualties.

Third, they tend to be cheaper to field than crewed platforms and are less logistically intensive, integrating seamlessly with other systems with less personnel.[164]

Furthermore, they allow for greater modularity and scalability in terms of payload integration compared to crewed aircraft.

Improving Communications and Interoperability

While large UAS have been a regular component of NATO Unified Vision exercises, these events have focused on the interoperability of JISR tools and systems in general. For the maritime domain, allies have embarked on a multinational effort focused on MUS specifically, including capabilities, concepts, and interoperability.

The Maritime Unmanned Systems Initiative, a multinational framework launched in 2018, now includes sixteen member countries and supports the introduction of flexible and more interoperable maritime unmanned vehicles into allied navies.[165] This initiative revolves around seven main areas of cooperation, including integration of MUS into NATO policies, technical standardization to enhance interoperability, doctrine development, joint training and support, and engagement with industry.

Interoperability and doctrine development deserve special attention at a time when technology is evolving fast and the threats to the alliance are multiplying. To consolidate these two areas, the MUS Initiative (MUSI) countries participate annually in operational experimentation conducted by NATO and NATO nations like the Robotic Experimentation and Prototyping augmented by Maritime Uncrewed Systems (REPMUS). In September 2022, MUSI nations participated in NATO's Dynamic Messenger operational experimentation (OPEX) exercise series. The REPMUS experimentation, hosted by Portugal, focuses on capability development and technical interoperability with MUS in military maritime operations.[166]

The Dynamic Messenger (OPEX) co-hosted by NATO's Maritime Command (MARCOM) and Allied Command Transformation (ACT), expanded REPMUS achievements in MUS integration in NATO naval operations, and added the enhancement of TTPs in detecting and clearing mines, conducting anti-submarine warfare (ASW), and monitoring sea lines of communication, among other tasks.[167]

The Dynamic Messenger exercise was the first NATO exercise solely focused on MUS and their integration with crewed platforms. The exercise allowed for unhindered experimentation with MUS by NATO maritime commanders and operators (including Standing NATO Maritime Group 1) and the integration of dual use emerging and disruptive technologies in cooperation with academic and industry partners.[168]

Beyond the trials of more than 120 different multi-domain uncrewed assets, these exercises provided a unique opportunity to test sensor and communication fusion

Photo: Technicians do final checks of an underwater drone aboard FGS Homburg (SNMCMG1) October 26, 2018 before launch during Trident Juncture 18 night mine countermeasures operations.
Credit: NATO MARCOM

between different systems within C2 architectures whereby drones can "speak the same language," autonomously cooperate, and interact with the headquarters.[169]

The value of the Portuguese Navy's innovation in MUS development and experimentation was recently confirmed by NATO. "The Portuguese Navy's Maritime Operational Experimentation Centre – located at Troia, the facility that hosts 'REPMUS' and 'Dynamic Messenger' – has been assigned as a Defense Innovation Accelerator for the North Atlantic (DIANA) test center, including being tasked with developing AI, autonomy, data, and new materials technologies."[170]

The NATO Centre for Maritime Research and Experimentation (CMRE) collaborated with partners in the NATO Science and Technology Organization research project aimed at standardizing communications among different C2 systems and uncrewed systems operating in communications limited environments. This team developed the Collaborative Autonomy Tasking Layer (CATL), a set of languages for enabling multi-domain autonomous tasking and data sharing. The CATL developments help inform the on-going STANAG 4817 effort, which aims to standardize multi-domain command and control.[171]

According to the CMRE's Director Catherine Warner, these federated, multi-domain C2 architectures "will allow human command and machine control."[172] This has enormous implications for interoperability and the role of autonomy in improving both human-machine interaction during operations and the utilization of uncrewed systems – including UAS – in communications-denied environments.

Maritime Tasks for UAS

Amongst the UAS that were tested during Dynamic Messenger, the Austrian S-100 Camcopter was employed in an anti-submarine role, using a dedicated data relay payload to transmit information from various sonobuoys to the command center ashore and then facilitate the detection and classification of possible enemy submarines.[173] In recent years the anti-submarine task has regained prominence in the alliance's military agenda due to Russia's increased submarine capabilities and activities in both the North Atlantic and the Mediterranean Seas.

Against this backdrop, specialized long-endurance UAS with tailored ASW sensors and autonomous features can carry out some of the traditional ASW tasks of crewed maritime patrol aircraft such as protracted submarine detection and tracking missions, expanding NATO's ASW options and capabilities.[174]

More generally, UAS can leverage their endurance and long-range multi-type sensors to provide unmatched maritime ISR and engagement over vast areas at cheaper costs compared to crewed aircraft. Other tasks may also include extended-range early warning and detection of incoming anti-ship missiles, including maneuvering sea-skimming missiles that are more difficult to counter.

For maritime forces to employ UAS in maritime air defense tasks, they require a rapid TCPED process as well as autonomous capabilities. According to naval warfare expert Steven Horrell, the alliance will not be able to capitalize on the advantages offered by drones in the maritime domain "without the creation of a dedicated joint fusion architecture – to be organized in regional fusion nodes – that improves intelligence sharing and makes critical information available to all allies in the shortest possible time."[175]

Another area of experimentation is the use of UAS for maritime resupply and refueling purposes (including ship-to-shore). For example, both the Royal Navy and the US Navy have recently tested UAS systems in heavy lifting and transport missions over medium and long distances.[176]

The US Navy is also at the advanced trial phase of the Boeing MQ-25 Stingray, an air-to-air refueling (AAR) UAS that will significantly extend the operational range of US carriers' crewed aircraft fleet, including F/A-18 Super Hornet and F-35C fighter jets.[177] Once in service, the MQ-25 will also provide key support for the air wings of allied navies.

National Maritime UAS Capabilities

At the national level, the US remains the major actor in terms of maritime UAS capabilities, though several NATO countries are expanding their UAS fleet in

this domain, including France, Italy, the United Kingdom, and Turkey. The French Navy has started the integration of the fixed-wing Aliaca UAS aboard its future offshore patrol vessels and surveillance frigates. The Aliaca drone has a three-hour endurance and provides high-quality, all-weather ISR up to a range of 50 km thanks to its gyro stabilized EO/IR payload.[178]

The French *Marine Nationale* is also in the final testing phase of its "Système de Drone Aérien pour la Marine" (SDAM) program, which is based on the Airbus VSR-700 Naval vertical take-off and landing (VTOL) UAS. This program aims to deliver a VTOL UAS capability for future frigates of the French Navy. The VRS-700 has an impressive range of 150 km and is outfitted with a maritime surveillance radar, an Automated Identification System (AIS) receiver (transponder-based ship location system), and an optronic payload optimized for use in the marine environment.[179]

Turkey is one of the NATO countries investing most in UAS capabilities, including in the maritime domain. The Turkish Navy commissioned the amphibious assault ship TCG Anadolu – the country's largest military ship and the first of its kind to provide a Class III maritime UAS unit afloat. The TCG Anadolu should become fully operational in 2025 and will host an improved and folding-wing version of the combat-proven TB2 UAS, called TB3.[180] The TB3 will give Ankara a BLOS offensive drone capability thanks to a satellite communication link and a heavier payload (280 kg) compared to its land-based brethren.[181]

The TCG Anadolu is also set to carry the Bayraktar Kizilelma uncrewed fighter jet, a highly maneuverable stealth UAS capable of conducting offensive offshore and onshore missions, including SEAD and DEAD. The landing-helicopter-deck (LHD) class Anadolu will pave the way for new concepts and operational uses of UAS in maritime operations, making Turkey the first country and NATO ally to deploy a full-fledged drone strike group along with an amphibious assault force.

The United Kingdom and Italy are also currently improving their maritime UAS capabilities. Earlier this year, a contract was signed with the Austrian company Schiebel for the acquisition of S-100 Camcopter rotary-wing UAS that will operate from the Royal Navy's Type 23 frigates and provide long-range high-performance ISTAR[182] along with a capable multi-sensor fusion software. The Royal Navy will also trial General Atomics' "Project Mojave" short takeoff and landing (STOL) UAS onboard its aircraft carriers, which could pave the way for the future integration of a STOL version of the MQ-9B UAS developed by the same US company.[183]

Italy, a NATO member strategically located in the Mediterranean and itself an operator of the S-100 UAS, will bolster its naval UAS capabilities with new acquisitions over the next few years, according to its 2022-2024 Defense Planning Document, although the specifics of these capabilities remain unclear.[184] The Italian

Navy has also commissioned a feasibility study for a drone carrier ship, following in the footsteps of its Turkish counterpart.[185]

Overall, however, there continues to be a tangible imbalance in the distribution of UAS maritime capabilities across the alliance, with repercussions for ISR coverage in key areas such as the Black Sea. While the rotational deployment of US MQ-9s and NATO RQ-4D AGS is partially filling the maritime ISR gap in the region, coastal countries such as Romania and Bulgaria lack long-range UAS assets to conduct persistent maritime ISR and engagement in their territorial waters and beyond.[186]

As a result of this maritime capability gap, NATO may have difficulties in detecting and tracking the movements and activities of the Russian Black Sea fleet in case of confrontation. Despite the loss of the Slava-class Cruiser *Moskva* in April 2022, Russia remains the dominating naval power in the Black Sea region and continues to pose a credible threat to NATO along its southeastern flank.

C) Cyber and Space Domains[187]

Cyber and space represent both enabling domains for UAS as well as avenues for attack. Cyberspace (along with the electromagnetic spectrum) enables connectivity between UAS and command modules (ground, afloat, or airborne), operators, analysts, and other C2 nodes, sensors, and effectors, including other UAS (for coordinated or collaborative operations). Space provides data and multiple services such as positioning, navigation, and timing (PNT), information (e.g., meteorological, environmental) and satellite-based communications and guidance.

The fast-paced integration of UAS into military operations into the physical domains of land, air, and sea requires support from the cyber and space domains. UAS are interdependent with space and cyber, including from a security perspective[188] as they rely on satellite navigation, the use of wireless communication, onboard sensing technology, and remote control. These conditions make them vulnerable to cyber and electronic warfare attack.

Cyber Domain

UAS systems are extremely vulnerable to cyberattack. In the cyber domain, attacks can target all components of the UAS, including supporting satellites, the ground control station (GCS), and the communication signal between the GCS and the drone itself. Attacks can include the interception of downlink data and information from the UAS to the operator in order to obtain intelligence, the disruption of the drone through malicious code to impair its functions or capabilities, the intrusion in or disablement of the GCS operating system, and the jamming or spoofing of

the navigation and communication signals. These are the most frequent types of attacks, though others are possible.

An example is the hacking of a stealthy US RQ-170 Sentinel UAS by Iran in December 2011[189] while it was conducting an ISR mission deep in Iranian airspace. Although it remains unclear what method Iranian forces used, they managed to disrupt the communication and navigation signals between the operator and the UAS, bringing down the system largely intact onto Iranian territory.

Navigational spoofing — which falls between cyber and EW techniques — could have been a plausible cause. In another case from 2009, Iranian-backed Shiite insurgents in Iraq were able to breach the operating system of a US MQ-1 "Predator" UAS and view its live feeds using a mass-market software program.[190]

However, the cyber domain is also essential for enabling drone operations. For example, well-prepared cyberattacks can be launched ahead of SEAD and DEAD missions, disrupting the opponent's C2 network and degrading the functionality and readiness of its air defenses, paving the way for UAS kinetic strikes or close air support missions in hostile territory.

Robust cybersecurity protocols ensure the resilience and protection of C2 and navigation links between the UAS, the operator, and the broader military ecosystem into which drones are integrated. As NATO's reliance on UAS grows, the alliance's cyber capabilities must keep pace with evolving and increasingly advanced hacking techniques to effectively safeguard allied C4 networks while providing the necessary support to military operations.

Space Domain

As with cyberspace, space is a critical operational domain for the alliance's security and military operations, playing a key role in the following areas:[191]

- **positioning, navigation, and timing**, which enables precision strikes, tracking of forces, and search and rescue missions;
- **early warning**, which helps to ensure force protection and provides vital information on missile launches;
- **environmental monitoring**, which enables meteorological forecasting and mission planning;
- **secure satellite communications**, which are essential for consultation, and command and control;
- **intelligence, surveillance, and reconnaissance**, which are crucial for situational awareness, planning, and decision-making.

Photo: A SpaceX Falcon Heavy rocket with the Psyche spacecraft onboard is launched from Launch Complex 39A, Friday, Oct. 13, 2023, at NASA's Kennedy Space Center in Florida.
Credit: Aubrey Gemignani/NASA

As UAS across the alliance become more and more integrated into a complex military ecosystem, they inevitably need space support and services, not least in terms of resilient navigation, secure communication, and accurate intelligence for better operational planning and execution.

In denied environments, onboard autonomy can effectively obviate the jamming of satellite navigation by exploiting sensor fusion capabilities. However, the disruption of satellite communication links by enemy EW, for example, hampers the operator's control of the drone and risks compromising the mission. While a communication and data link are not required in fully autonomous systems, its interruption represents a major challenge as long as UAS are employed with a human-in-the-loop or human-on-the-loop approach (more on that later).

As noted by NATO's Assistant Secretary General for Intelligence David Cattler, space assets also provide critical ELINT, IMINT, and SIGINT resources for the effective use of UAS.[192] Exploiting space-based intelligence can enhance and better focus drone employment with positive implications for the overall military effort.[193]

Leveraging Allies' Space Capabilities

At present, NATO countries operate an estimated total of 1,809 satellites, inclusive of civilian (national or multinational), commercial, military, or intelligence

assets.[194] In February 2023, NATO announced plans to establish the alliance Persistent Surveillance from Space (APSS) initiative, a multi-year, multi-domain, and multinational effort to boost space-based surveillance and intelligence for the alliance, thus improving its situational awareness and collective decision-making.[195]

Two characteristics of the APSS initiative stand out:

- Its multinational and cooperative nature leverages existing and future space assets in allied countries and connects them in a NATO virtual constellation called "Aquila."
- Its data-centric approach will allow the APSS to integrate data from both government-owned and commercial space contributions.[196]

This multinational and collaborative approach will allow NATO allies lacking space capabilities – 15 countries – to access space-based intelligence and communications, while improving and expanding information sharing across the alliance. Moreover, this approach will enhance interoperability by pushing allies toward the use of common platforms (i.e., sensors, software, etc.) and standardized TTPs.

The Growing Importance of LEO Satellites to UAS Operations

At the same time, the direct involvement of private space companies with Low Earth Orbit (LEO) satellites enhances the resilience and effectiveness of the alliance's activities and operations, especially in terms of services and signal availability. Compared to geostationary orbit (GEO) and medium-earth orbit (MEO) satellites, LEO satellites are smaller, operate at lower altitudes (500-2,000 km), and provide signals with increased bandwidth and at low latency rates thanks to their shorter distance from the earth's surface and constant non-stationary orbit.

These features make LEO satellites ideal for communications applications, including military ones. While LEO satellite-based communications (SATCOM) are vulnerable to jamming and other EW methods,[197] the use of vast networks of satellites — also known as constellations — ensures greater resiliency against EW compared to fewer GEO satellites.[198]

As discussed in the first part of this study, Starlink's LEO SATCOM have allowed Ukrainian drone operators to elude the bulk of Russian jamming attacks and continue drone operations, although Russia forces have adapted and had some successes in limiting the use of Starlink terminals by Ukrainian units.[199] The increasing military role of LEO satellites will also impact complex BLOS drone operations. In December 2022, the US company General Atomics flight-tested an MQ-9A equipped with a LEO satellite communications C2 system, which will enable high-latitude pole-to-pole operations — otherwise constrained via GEO SATCOM — and provide resilient connectivity to and from the aircraft."[200]

Photo: U.S. Air Force Tech. Sgt. Joshua Werho, 55th Combat Communication Squadron radio frequency transmission systems technician, and Senior Airman Jesse Severns, 35th CBCS cyber security technician, check operations on a Ranger 2400 Flyaway Multi-Band Terminal during EXERCISE AGILE BLIZZARD-UNIFIED VISION 2023 near Comox, British Columbia, Canada, June 19, 2023. Credit: Tech. Sgt. Betty R. Chevalier/US Air Force

According to the same company, LEO SATCOM should "decrease operational costs" and allow for cheaper payload integration in the future thanks to a smaller and more modular hardware footprint.[201] This development is especially important for the alliance considering the increasing role the MQ-9 will play in the UAS fleets of NATO allies in the medium term.

Additional advantages of LEO SATCOM include:

- the provision of a backup data and C2 link — set on a different frequency — in case the main satellite connection is jammed or lost, ensuring robust redundancy during BLOS operations;[202]
- faster and larger data transmission by virtue of high-throughput, low-latency communications.

A higher order of data transmission would facilitate the use of UAS in a multi-domain sensor-C2-shooter architecture, shortening the kill-chain cycle during BLOS missions, and possibly enabling cross-cueing detection as well as the sharing of tracking information between space-based and airborne sensors to improve long-range ISR and strike.

Against this backdrop, the NATO APSS or a future similar NATO initiative could eventually include a component modeled after the US Space Force's Transport Layer, a novel LEO constellation that "will provide assured, resilient, low-latency military data and connectivity worldwide," exploiting the unprecedented connection performances provided by Optical Inter-Satellite Links (OISLs).[203]

However, the reliance on LEO SATCOM is not without risks. Various EW techniques like jamming and spoofing against the signal transmission, and cyberattacks against both the ground infrastructure and the satellite add to challenges emanating from the complex logistics and network infrastructure required by LEO constellations.[204] These issues underscore the need for more robust and resilient protection standards for space assets that are used for military purposes, both in terms of hardware and software with built-in security protocols.

Based on the above considerations, space is now more than a mere enabling domain for UAS operations in contested environments, and NATO countries that seek exquisite UAS capabilities should consider the critical role played by space in UAS development and employment.

D) Enabling efforts

Enabling Policies and Standardization

NATO has agreed to an impressive number of policies covering UAS development and employment. These policies include:

- NATO's Total System Approach to Aviation (addresses both crewed and uncrewed systems);
- NATO policy for unmanned aircraft systems;
- NATO policy for civil/military aircraft operating in support of NATO or NATO-led missions and operations;
- NATO Remote Piloted Aircraft Readiness Initiative (R2i).[205] NATO R2i includes a strategy and implementation plan and focuses on UAS piloted by remote control.

In addition to NATO policies, NATO nations have agreed to an array of standardization agreements (STANAGs) regarding UAS (more on this later).[206] Yet, in spite of NATO policy and standardization efforts to harmonize NATO UAS development and operations, diverse national approaches to capability development and acquisition, along with a multitude of proprietary UAS, associated payloads, and data-exchange protocols in use by NATO nations, significantly complicate interoperability.

Photo: German Air Force A400M pilot conducts manoeuvres on the A400M during Air Defender 23. Credit: NATO

NATO STANAGs and policies represent a foundation for alliance interoperability, but implementation and follow through by individual allies is often lacking. Exacerbating a lack of implementation is the absence of a verification process to assure NATO military authorities of overall UAS interoperability, readiness, and responsiveness.

Digital Transformation

Digital transformation is a broad endeavor launched by the alliance that focuses on the enabling technologies, technical infrastructure, and people needed to "increase the speed, security, and effectiveness of NATO critical processes, from C2 and communications to data and intelligence analysis and dissemination, in order to enhance interoperability and decision-making."[207]

Digital transformation will shape the over-arching C4ISR architecture as well as sensor-C2-shooter networks in which UAS will operate in the future. Digital transformation will be the enabling foundation for future alliance Multi-Domain Operations. Security and interoperability standards will enable rapid integration of various national and NATO UAS systems into forces, networks (i.e., an internet of military things) and operations, as well as dynamic tasking and synchronization of cross-domain or multi-domain effects.

While this critical endeavor aims to prepare NATO for future demands, including multi-domain operations against a peer adversary, its ambitious and comprehensive nature may be a challenge for NATO to fund, implement, and sustain.

Achieving digital transformation's goals will be essential for the use of UAS in collaborative roles and human-machine teaming, but also a challenge, considering the latency associated with increased encryption in data links, among other issues.[208] More generally, NATO must be able to protect and transmit information in a coalition environment, such as multi-domain operations, where data is stored in a cloud architecture, leveraged at the tactical edge, and shared at the speed of relevance.

Autonomy, AI, Data, and Other Emerging and Disruptive Technologies (EDTs)[209]

Autonomy, AI, data, and other EDTs stand to further enable UAS capabilities. When it comes to autonomy, NATO distinguishes between autonomous, automated, and automatic (all of which may feature AI capabilities). While both governmental bodies and international organizations have provided multiple classifications of these concepts,[210] this study uses the official NATO definitions.[211]

Autonomous, Automated, and Automatic

According to NATO, "autonomous pertains to a system that decides and acts to accomplish desired goals, within defined parameters, based on acquired knowledge and evolving situational awareness, following an optimal but potentially unpredictable course of action.

Automated characteristics describe a system that, in response to inputs, follows a predetermined set of rules to provide a predictable outcome.

Automatic pertains to a process or equipment that, under specified conditions, functions without human intervention."

At present, the integration of autonomy in drones remains largely confined to specific functions, such as AI-enabled target detection and tracking. The human-out-of-the-loop (HOOL) scenario — whereby the UAS decides and acts to accomplish desired goals without human input — has not materialized. This means that current UAS have a degree of human control (technically defined as human-in-the-loop and human-on-the-loop) in every action they execute.

Equally important, the vast majority of UAS fielded today, including those seen in Ukraine, typically do not process information on-board at scale and they are not

networked together. In general, collected data and information are usually relayed to the ground control station in real time, or stored in the UAS for later examination, based on the system's specifications.

For example, the Shahed-136/131 slow-flying munitions analyzed in the first chapter are launched in large numbers simultaneously, but do not communicate with each other and cannot autonomously replace those that are shot down. This has significant implications in terms of target prioritization. However, some systems like the Russian Lancet LM and Ukrainian FPV drones have AI-powered software that allow for automatic target detection and engagement even if the connection with the operator is lost due to hostile jamming or environmental factors.[212]

One automated function involves the ability of most commercial drones to return to the launch coordinates if the navigation signal is lost. This ability is not an autonomous feature but rather automated based on a preprogrammed set of commands from which the UAS cannot deviate.

Up until now, NATO and Western militaries have generally operated under full-spectrum dominance, where the operator can communicate with the UAS at any given time and in most environmental conditions. However, things are rapidly changing and today's operational environments present increasing levels of threat that mitigate or even deny Western technological supremacy.

Hence, for NATO to preserve its technological edge, it is crucial to leverage EDTs such as AI, Big Data, quantum technologies, and advanced propulsion solutions, among others. According to a subject expert from a private company focused on autonomous UAS, "the war in Ukraine has become a catalyst for experimenting AI-enabled UAS in a non-permissive environment, achieving greater results in one year than in the past decade."[213]

The Importance of AI-Enabled Autonomy for UAS

Simply put, autonomous UAS are akin to flying computers with their own C2 capabilities. This allows for the detection, tracking, and potential engagement of multiple targets simultaneously and at an unprecedented pace. Further, autonomous flying and maneuvering functions reduce the mission load on the operator while allowing the latter to control multiple drones. AI and advanced onboard computing can also reduce or eliminate the need for external communications, limiting vulnerability to jamming and spoofing and allowing for operations in a communications-denied environment. Yet, total dependence on AI (software) is a double-edged sword, for it can render fully autonomous UAS more exposed to cyberattacks.

Moreover, AI-enabled autonomy is also the gateway to both swarming capabilities, whereby multiple networked UAS coordinate and adapt to achieve complex

Photo: As part of NATO's Unified Vision 2014 Trial, members of the Italian Air Force launch a surveillance drone (STRIX, a multi-purpose, man-portable, totally autonomous TUAS) over Oerland, Norway. Credit: NATO

objectives, and teaming operations with crewed aircraft in which UAS enhance the former's situational awareness, survivability, and capacity to deliver effects.[214] Overall, in future UAS development, autonomy needs to be integrated along with quantum sensing and new propulsion capabilities for maximum effectiveness.

Autonomy will have a huge impact on future UAS's ground control and support as well. AI-aided software and machine learning tools can dramatically improve the PED cycle by quickly analyzing massive amounts of data and extracting only the information that is relevant to a specific intelligence task, mission, or area of operations.

AI-enabled PED has enormous implications for the NATO enterprise, considering the challenges of cross-domain Joint ISR data in a multinational environment. This is especially important considering the likely multiplication of intelligence sources and increase of raw data collected, human resources constraints, and the need for speed of intelligence dissemination during conflict and crisis.

Leveraging Data Architecture for UAS Operations

The effectiveness of UAS operations as well as the intelligence they produce depend on the integration of UAS into a data-centric military ecosystem that connects different capabilities and fuses data and information from multiple sources within a joint C4ISR architecture for better situational awareness and faster decision-making. Uninhibited access to information and the ability to process, exploit, and disseminate it quicker than the adversary is key to success.

As noted by ASG Cattler, "plugging in new sensors — no matter how powerful they are — is useless if you don't have the capabilities and resources to exploit the data you collect."[215] At the same time, archiving data for later exploitation is becoming less functional considering the growing demand for real-time or near-real-time intelligence to inform decision-making.[216]

For a collective organization like NATO, the abovementioned ecosystem requires a unified approach to data governance that includes:

- common data formats and protocols;
- shared storage policies;
- standardized data management tools

This approach will enable better information sharing as well as big data exploitation.[217]

For example, an Air Force officer of a NATO member state underlines the lack of alignment and standardization between NATO datasets, the limited connectivity among them, and the absence of an optimized processing criterion in the overall exploitation process.[218] More broadly, the key challenge is to make data and information available at scale, and promptly, across the alliance.

To this end, in October 2021 NATO ministers adopted a Data Exploitation Framework (DEF) policy. The ensuing DEF Strategic Plan revolves around several lines of effort, including common data governance, an open and scalable data architecture, AI integration, and a standardized data management process.[219] These measures aim to facilitate and expedite data visualization, sharing, and exploitation across the alliance, but it will take time to achieve these goals.

Likewise, NATO priorities for UAS include efforts to streamline and accelerate the flow and management of information at the tactical level, where time is of the essence, in order to avoid "ISR bottlenecks" and shorten the kill chain. The CATL architecture is a related NATO tactical data effort (supporting development of STANAG 4817) and meant to enable multi-domain autonomous tasking and data sharing, as well as reduce the volume and frequency of UAS external communications.

Leveraging Quantum Technology to Protect and Enhance UAS Capabilities

Given the reliance of UAS on wireless communications and data links, it will be essential to increase the bandwidth, speed, and encryption level of data and signals across the entire C4ISR architecture. In this respect, NATO has recently tested different quantum technologies that have the potential to make communications virtually impossible to intercept and hack.[220]

Indeed, AI-enabled autonomy, along with quantum sensing,[221] can ensure persistent positioning and improved situational awareness in electromagnetic-denied situations, thanks to onboard multi-sensor fusion capability (inertial, optical, magnetic, etc.) capable of overcoming the lack of satellite signals. At the same time, autonomy offers onboard processing capabilities to exploit data, allowing the UAS to choose among multiple courses of action at warp speed without human input and a data link with the operator.

Other NATO EDT Policy Efforts Relevant to UAS

The alliance is developing the necessary policy framework for supporting the adoption of EDTs, prioritizing AI, data, and autonomy policies due to their broad application to current and future military capabilities. Along the same lines as the NATO data policies covered previously, NATO's AI Strategy and Autonomy Implementation Plan were approved in 2021 and 2022, respectively, and aim to provide clear policy guidance for the responsible and sustainable development of innovative AI-enabled and autonomous technologies by all allies.[222]

Also in October 2022, NATO established the Data and Artificial Intelligence Review Board, tasked with implementing the technical standards and principles governing responsible use.[223] Other EDT policy efforts that may impact future allied UAS development include:

an EDT strategy for quantum technologies;

a NATO taxonomy for autonomous systems;

an interoperability fund to help nations develop NATO material standards.[224]

Multinational Cooperation

NATO enables UAS capability development and NATO-wide integration[225] through armaments cooperation (including industry and private sector engagement), cooperation in scientific and technological research and development, operational experimentation, and a variety of recent NATO innovation initiatives focused on adoption and protection of (NATO prioritized) emerging and disruptive technologies.

NATO agencies (NSPA, NCIA), CMRE, and the Strategic Commands (especially ACT) play a significant role in capability development and innovation. Despite structured efforts across the NATO enterprise, more can and must be done specifically to adapt lessons learned from recent conflict and upscale the development and acquisition of UAS and related capabilities. Improvement and acceleration of NATO and national procurement processes are also necessary.

Recent NATO Initiatives Important for UAS Capability Development

NATO efforts to promote innovation are part of the alliance's overall effort to adopt and protect EDTs to maintain NATO's technical edge and decisive military advantage vis-à-vis potential adversaries. In support of advanced technology integration and to develop a vibrant innovation ecosystem, NATO has launched DIANA[226] and the NATO Innovation Fund (NIF).[227] The alliance has made considerable progress in terms of defense modernization, and investment and UAS are firmly in the mix. New initiatives prioritize expanding and improving existing capabilities for use against near-peer adversaries.

Broadly, the DIANA and NIF initiatives are meant to bring allied nations and their industries and research communities into a closer partnership to fund, develop, and deploy dual-use EDTs. Both initiatives aim to leverage commercial technological breakthroughs to create solutions that can bridge key capability gaps and offer good prospects of commercialization at scale.

DIANA consists of a board of directors, a management director, and staff, as well as two regional hubs, and a wide network of research and test centers across North America and Europe. The initiative is intended to work directly with leading scientists, engineers, and entrepreneurs through a bottom-up and learn-by-doing approach.[228] DIANA will launch regular challenge programs based on its biennial Strategic Direction.[229] The first challenge was announced in June 2023, and focuses on three priority EDT areas as identified by DIANA's board: sensing and surveillance, energy resilience, and secure information sharing.[230]

UAS technologies fall clearly in the first area, may be relevant to the second, and will certainly leverage outcomes of the third area.

Unlike DIANA, the NIF is an opt-in initiative with currently 22 allies participating as limited partners.[231] [232] The "fund" in NIF is actually the first of its kind €1 billion ($1.1 billion) multi-sovereign venture capital fund designed to provide strategic investments for start-ups developing dual-use emerging and disruptive technologies to support NATO capabilities.[233]

Photo: NATO Deputy Secretary General opens DIANA's European Regional Office. NATO's Assistant Secretary General for Emerging Security Challenges and DIANA's interim Managing Director David Van Weel symbolically passed the baton on to the incoming Managing Director, Professor Deeph Chana. Credit: NATO

That NIF capital used to expand and upscale DIANA programs increases the possibility that UAS technologies may benefit from such investment. The NIF has a charter, a Limited Partnership Committee (LPC), and an independent supervisory board of directors[234] that will manage and execute the NIF. While the NIF is not expected to be at full operational capacity until fall 2023, its governance, investment strategy, and venture capital focus are clear. NIF will focus investment on "early-stage deep tech startups" involved in emerging and disruptive technologies.[235] UAS or related enabling technologies certainly present promising areas for investment.

The abovementioned capabilities and enabling efforts demonstrate the considerable progress made by the alliance in terms of defense modernization and investment. While the use of UAS is not new and centers on mature and battle-tested technologies, the priority is now to expand and improve their capabilities for use against near-peer adversaries, including in high-intensity combat.

The next and last part of this study identifies and analyzes the main challenges for NATO UAS operations in high-intensity scenarios.

Part III – Challenges

Several challenges hinder the development of robust and effective UAS capabilities across the alliance. These include limited interoperability, critical capability gaps, inadequate platform survivability, deficiencies in personnel and training, limits to intelligence processing, and more.

Interoperability

From a military standpoint, **interoperability is arguably the biggest challenge for NATO**. Interoperability affects the entire UAS architecture including personnel training, communication protocols, data-exchange formats, CONOPs, and, eventually, the rapid dissemination of intelligence and targeting data across a multinational joint force. Predictably, NATO's collective nature renders such a layered undertaking even more complex.

While the work of NATO's Joint Capability Group-UAS[236] has contributed to streamlining and condensing different efforts and discussions on UAS from across the alliance, according to Ross McKenzie and Michael Callender, NATO still suffers from the "lack of a structured Joint Staff focused on harmonizing and bringing together UAS capabilities in a comprehensive way."[237]

The predominance of domestic development and procurement initiatives — to a large extent driven by industrial competition — represents a major hinderance for interoperability.[238] Industrial competition has led to a variety of data links, communication protocols, and message formats between the uncrewed aircraft, the ground control station, and external command, control, communications, computers, and intelligence (C4I) nodes.[239] As a result, "the dissemination of sensor data is mostly via indirect means," despite the need for near real-time tasking/re-tasking of UAS assets, payload employment, and dissemination of intelligence at different echelons.[240]

To address these specific issues, NATO has approved the standardization agreement (STANAG) 4586, now in its fourth edition, which aims to enable interoperability between the ground segments (i.e., the ground control station) the air segments (the uncrewed vehicle), and the C4I segments of legacy and future UAS operating in a NATO Combined/Joint environment.[241]

STANAG 4586 also identifies the different levels of interoperability (LOI) between the UAS and the operator(s) (see footnote) and specifies the parts of the UAS that need to comply with specific requirements to interact with various uncrewed aircraft, their payloads, and different C4I systems.[242]

Photo: US Army Sgt. Zachary Pacetti, assigned to 2nd Cavalry Regiment, Regimental Engineering Squadron, makes repairs to an AAI RQ-7 Shadow unmanned aerial drone as part of ORION 23, April 19, 2023. ORION 23 is a French-led interoperability campaign that is designed to develop partnerships with allies and assess the ability to operate within a coalition.
Credit: Sgt. Khalan Moore/US Army

While essential, compliance with this STANAG alone does not ensure full interoperability between different UAS, for it "does not address platform and/or sensor operators' proficiency levels, nor does it define the [necessary] CONOPs."[243] Indeed, the use of different patented platforms and sensors across NATO implies tailored training and specific personnel skills that further complicate the alliance's efforts to harmonize UAS capabilities and increase interoperability. In this respect, different approaches to, and investments in UAS entail a lack of UAS crew and specialized personnel in some NATO countries.

At the current stage, the lack of full interoperability has huge implications for the use of UAS in joint NATO operations. Operators and specific uncrewed aircraft of different member states are not able to mutually interact and communicate with C4I nodes with the necessary speed and proficiency required in high-intensity environments.

Technology can obviate this issue. For example, General Atomics and the Spanish firm Sener Aerospacial have developed a customizable and internationally exportable "NATO Pod" that allows operating countries to plug-and-play sovereign,

cross-domain sensors and payloads on the MQ-9 family of UAS, which will likely become the workhorse of allies' national MALE UAS fleets in the mid-term.[244]

STANAG 4586 is just one of many standards agreed upon by member states to improve interoperability and integration between a plethora of UAS. These standards cover most UAS-related elements and aspects, including airworthiness requirements for different types of UAS,[245] minimum training benchmarks for UAS operators and pilots,[246] weapons integration,[247] and C2 data links.[248]

Importantly, the NATO JCG-UAS is currently developing a new standard (STANAG 4817) for the data link between a GCS and multiple uncrewed systems in other domains to enable multi-domain operations.[249] Furthermore, the JCG-UAS is supporting the implementation of the Remotely Piloted Aircraft Readiness Initiative (R2i), an operationally focused strategy that aims to foster the integration and operational effectiveness of national and NATO common-owned uncrewed aircraft across the alliance in line with NATO's UAS policy.[250]

Another key factor is operational experimentation (OPEX), which plays a critical role in improving the development and adoption of EDTs, tailoring them to the capability needs of the alliance, incorporating feedback from industry and academia, improving interoperability, and allowing for a smoother elaboration of doctrine, concepts and TTPs. Examples of this bottom-up and multi-stakeholder approach include:

NATO's Project X, a short-term endeavor (2022) between NATO, Boeing, the government of the Netherlands, Designing with Delft, and the Unmanned Valley field lab focused on the development of autonomous systems that can remotely access and evaluate situations inaccessible to human life;[251]

The US Central Command's Task Force 99, a recently established unit of the US Air Force headquartered in Qatar that conducts innovative work on uncrewed systems and digital integration, with a focus on commercial UAS.[252]

Finally, operational interoperability relies on common doctrine and concepts. There are no NATO joint allied publications dedicated wholly to UAS and C-UAS employment and very few nations have such joint doctrinal publications. There is mention of UAS in joint allied air doctrine, but references do not capture the expansion of UAS capabilities, roles, and missions in recent conflict or employment concepts being put into national defense plans (i.e., collaborative crewed-uncrewed operations, swarms, cooperative or collaborative groups, advanced sensor/effector payloads, autonomous air to air combat, etc.).[253]

As the technology of UAS matures and NATO's focus shifts toward multidomain operations, more efforts are needed to define joint allied UAS and C-UAS doctrine and concepts (e.g., of operations or of employment, TTPs).

UAS Capability Gaps

Efforts by NATO allies to expand and improve their UAS capabilities predate the Russian full-scale invasion of Ukraine but have accelerated since. Despite a NATO focus on autonomy as a priority emerging and disruptive technology, efforts to improve UAS capabilities vary significantly across the alliance and are mostly driven by national priorities.

The NATO Alliance Ground Surveillance and the EU-sponsored Eurodrone are notable exceptions in terms of collective Class III UAS capability definition and procurement. While the NATO AGS Force represents a critical JISR capability for the alliance, RQ-4D will soon have obsolescence issues and would be severely challenged to satisfy even a portion of collective JISR requirements in a potential confrontation against peer adversaries.

While uncrewed technology is now at the top of most allies' defense agenda, more coordination is needed in terms of investments and the most effective types of capability to acquire to address current shortfalls.

This study has found both qualitative and quantitative deficits, which must be assessed against the backdrop of high-intensity conflict rather than the permissive counterinsurgency and counterterrorism environments in which NATO UAS have operated over the past 20 years. These deficits span across all three classes of NATO UAS, though the nature and extent of shortfalls vary significantly among allies.

Quantitative deficits mainly refer to the insufficient number of UAS, especially with regard to classes I and II, currently available across the alliance. Qualitative shortfalls concern the lack of specific UAS capabilities, in particular combat capable systems, long-range all-weather ISTAR sensors, and EW payloads.

Quantitative Deficits

From a quantitative standpoint, Class III UAS capabilities of NATO allies are increasing, though their distribution remains structurally unbalanced. While the US and Turkey operate a large number of Class III UAS,[254] most allies only possess a limited number of MALE and HALE UAS — mostly MQ-9 systems. Many countries such as Bulgaria, Hungary Romania, the Baltics, Slovakia, Finland, and Norway have no capability in this category. Should NATO be involved in a conflict in the foreseeable future, these countries could not provide Class III UAS to the alliance and would have to rely on either collective assets or other nations' platforms.

Considering the vulnerability of most large UAS currently in service to modern air defenses and their potentially high attrition rate, the current number in service with NATO allies falls short of a realistic baseline for high-intensity conflict.

Photo: An MQ-9 Reaper remotely piloted aircraft piloted by Airmen from the 556 Test and Evaluation Squadron flies over the Nevada Test and Training Range and performs live-fire exercises with Air-to-Ground Missile-114 Hellfire missiles and Guided Bomb Unit-12 Paveway IIs, Aug. 30, 2023. Credit: Airman 1st Class Victoria Nuzzi/US Air Force

Quantitative issues are particularly relevant with regard to Class I and Class II UAS. Indeed, the availability requirements and high attrition rate imposed by high-intensity scenarios in terms of small and medium UAS used for ISR — as proven by the war in Ukraine — suggest that most NATO allies' inventories are not sufficient. Several thousands of Class-I and hundreds of Class-II UAS appear to be a minimum baseline for sustaining even a few weeks of fighting characterized by a high demand for ISR assets in a limited regional scenario involving a few Multinational Land Corps.

Furthermore, any assessment of required numbers should include the ability to replenish losses either via rapid industrial production or acquisition at scale, both of which require resilient and efficient supply chains. Another key aspect regards the importance of military-grade systems, which provide better performance and resilience in denied environments compared to commercial UAS. Integrating commercial drones is certainly cheaper but entails serious risks in terms of unencrypted communication and data links, along with less capable payloads.

Qualitative Deficits

In terms of qualitative gaps, there is a structural lack of armed UAS across the alliance. The few exceptions are the US, UK, France, Italy, and Turkey. Other countries such as Germany, Poland, and the Netherlands are set to weaponize their MALE UAS soon. More allies are likely to follow suit. As many recent conflicts have shown, armed UAS provide substantial flexibility in augmenting or complementing direct and indirect fires. As UAS capabilities improve, their mission sets will likely expand as well (i.e., beyond the close to deep battle, to air and maritime interdiction, etc.).

For NATO, armed UAS represent an essential asset that will acquire further operational relevance as the alliance embraces a multidomain approach centered around data and information dominance and characterized by shorter kill chains and very high-tempo operations.

In similar scenarios, key capabilities will include very long endurance and low-observable UAS platforms equipped with BLOS redundant communication and data links, as well as a comprehensive sensor and capability mix. Specifically, this would comprise:

- long-range ISTAR payloads, including SAR, maritime wide area search radars, and GMTI functions to provide high-quality, real-time intelligence and surveillance;
- standoff EW;
- precision strike munitions for both air and ground targets.

At present, for example, NATO AGS does not include an EO/IR sensor capability. The addition of such features would be a significant boost to mission versatility and collection capabilities.[255] Considering the characteristics of comprehensive sensor payloads in terms of dimensions, weight, and performance, medium and large UAS remain the platforms of choice for their integration. Therefore, the lack of Class II and III UAS significantly narrows the options to field similar capabilities in high-intensity scenarios.

Autonomy

The incorporation of onboard autonomy, which can offset the problems caused by hostile EW to communication and data transmission, among other issues, represents another critical challenge for NATO. While the alliance works to further refine its recently published policy framework for embracing and developing autonomous technologies,[256] not all allies are convinced of the advantages or urgency of doing so. According to NATO UAS experts Ross McKenzie and Michael Callender, “allies are not able yet to integrate autonomy in a comprehensive way.”[257]

Ethical as well as legal implications have impacted discussions about armed UAS in countries like Germany and the Netherlands and heavily influence allies’ approaches to autonomy. This factor has made systematic testing and operational experimentation of autonomous technologies more difficult, thus slowing their incorporation.[258]

Indeed, the key challenge with autonomy — and EDTs more generally — is not just about technology per se but also having the necessary mechanisms in place that would allow NATO to test, adopt, and push out new solutions faster than competitors. In this respect, horizontal diffusion of new technologies can benefit enormously from

Photo: US Army Sgt. Nicholas Sutton, an infantryman assigned to 1st Battalion, 5th Infantry Regiment, 1st Infantry Brigade Combat Team, 11th Airborne Division, releases a Black Hornet 3 drone at a remote fighting position during Joint Pacific Multinational Readiness Center-Alaska 23-02 at Yukon Training Area, April 3, 2023. Credit: Senior Airman Patrick Sullivan/US Air Force

bottom-up initiatives, including from the civilian sector, but requires a permeable and flexible structure at the top to allow for such innovation to be assimilated and shared across all alliance forces.

Sense and Avoid

Besides autonomy, the integration of standardized Sense and Avoid (SAA) technology on UAS at scale is another crucial challenge for NATO. Given the absence of a pilot in the cockpit, drones must satisfy SAA regulations and requirements during flights. The disparate UAS and proprietary sensors used across the alliance complicates this goal.

As Ross McKenzie and Michael Callender note, the systematic incorporation of common SAA features represents a critical inflection point in the short term regarding the widespread employment of UAS.[259] Indeed, SAA capabilities, along with complementary technologies like Airborne Collision Avoidance Systems (ACAS), are essential for employing UAS all over NATO members' airspace and areas of responsibility.

In 2018, NATO approved the first standard document for UAS Sense and Avoid. This document set the stage for a common approach toward the development of SAA technologies to further improve the integration of military UAS into civilian airspace and achieve the NATO goal of unfettered UAS operations across multinational, non-segregated airspace on par with existing manned aircraft operations.[260]

Space Domain

Critical shortfalls in the space domain are also worth noting. Given the advanced and cost-prohibitive nature of space technology, only a few NATO countries possess their own space capabilities. This means that space-based intelligence products — from GEOINT to COMINT — that provide essential support for drone operations are not inherently available to all member states. At present, for example, 11 NATO countries do not have dedicated on-orbit military assets, namely satellites.[261]

Ancillary to space-based intelligence is the need for high-speed and secure connectivity to enable space-derived ISR to promptly feed UAS operations. The lack of such connectivity can limit the overall effectiveness of UAS operations, especially in contested environments where intelligence that is quickly delivered and comprehensive is critical for success.

The alliance Persistent Surveillance from Space initiative is a crucial step that will allow member states to access and share space-based intelligence, vastly improving NATO space capabilities and the entire C4ISR architecture. However, collective gaps in the space domain also require concerted efforts by single nations in terms of policy reforms to remove national barriers to intelligence sharing and implement the necessary infrastructure to digest new intelligence products made available by the alliance while effectively contributing to NATO's federated PED process.

C-UAS capabilities

With respect to NATO C-UAS policy, concept, and capability development, the scale of effort has focused on countering small UAS (Class I mini and micro) in low-intensity conflict. While C-UAS is a recognized component of IAMD, NATO policy efforts have long concentrated on C-UAS as a key counter terrorism or defense against terrorism capability to protect people, assets, and critical infrastructure.[262]

NATO innovation efforts related to C-UAS by Allied Command Transformation (operational experimentation) [263] and NCIA (technical interoperability)[264] have until now focused on small UAS. As the scale (in numbers and all sizes) of UAS employed in recent conflict has grown (including in Ukraine, Nagorno-Karabakh, and the Arabian Peninsula), and the advancements in drone technology of potential competitors like

Photo: Pfc. Mariah Davis, assigned to the 89th Military Police Brigade, operates the Drone Buster during a Counter-Unmanned Aircraft Systems class with Soldiers from 3rd Battalion, 265th Air Defense Artillery Regiment, supporting 4th Infantry Division, at Camp Taurus, Lithuania, on March 17th, 2023. Credit: Staff Sgt. Cesar Rivas/164th Air Defense Artillery Brigade

China, NATO recognition of the need for improved defense capabilities against UAS must rise.

Despite the focus on countering small UAS, NATO's approach to the problem has been fairly comprehensive and holds promise if scaled up to include the growing threat of UAS employed in greater numbers (including as collaborative groups or swarms) and with greater capabilities (longer range sensors, kinetic and non-kinetic effects, combined payloads).[265]

There are several challenges related to C-UAS that NATO must tackle:

1. **The alliance has not yet approved a joint doctrine on C-UAS operations**, although it plans to do so by the end of this year.[266] C-UAS doctrine would provide guidance and more clarity for a discipline that has overlapping applications in other areas, including air defense and force protection, which already have their own specific doctrinal publications.

   Since 2019, NATO has had a governance framework for C-UAS, with a C-UAS working group focused on Class I UAS, including commercial drones, and looking at both conventional and unconventional types of threats.[267] Yet, C-UAS capabilities and readiness vary significantly across the alliance.

   The US created the US Joint C-small UAS Office (JCO) in 2020. The JCO has taken a leadership and coordination role also within NATO. Other countries such as the UK, Italy, and the Netherlands have taken inspiration from this governance approach and established dedicated C-UAS centers at the national level. At the same time, several member states, including Belgium, Denmark, Norway, and Romania, have begun to acquire C-UAS capabilities. However, other countries are lagging.

Photo: Master-at-Arms 2nd Class Leonard Gallegos, from Reno, Nevada, operates Drone Restricted Access using Known Electronic Warfare (DRAKE) module in a counter Unmanned Ariel System (UAS) security drill aboard the Nimitz-class aircraft carrier USS Dwight D. Eisenhower (CVN 69). Credit: Mass Communication Specialist 3rd Class Zachary Elmore/ US Navy

While national efforts have stimulated the drafting process of the C-UAS doctrine, according to NATO C-UAS expert Claudio Palestini "different governance models among the Allies remain an open question."[268] For example, the US JCO is under the US Army while the corresponding body in the UK is managed by the Royal Air Force.

2. **Cumbersome procurement processes have hindered the acquisition of C-UAS capabilities** by NATO and individual allies, with delays of up to two years between the definition of requirements and contract execution.[269] The layered nature of C-UAS – with the combination of different technologies, including legacy and next-generation high-end sensors -- complicates the procurement, maintenance, and logistics compared to other capabilities.

   As a solution, several industries are now offering a "C-UAS as a service" model, whereby a government or military pays for the service rather than the equipment.[270] This option eliminates potential obsolescence problems, as the service provider owns the equipment and takes care of its upgrade or replacement, allowing for potential budget savings in the long term. For example, the US defense company Anduril, which collaborates with NATO on C-UAS, offers this contract model.[271]

3. **Technological and operational issues hinder a common C-UAS architecture**. Technical issues include the gap between C-UAS technology and a faster-evolving threat, especially large-scale swarming attacks. During exercises, large-scale coordinated attacks have proven very difficult if not impossible to defeat. Operational issues include the integration of C-UAS into the air defense ecosystem and the definition of proper CONOPs and Rules of Engagement (RoE), and a clear definition of the C-UAS discipline, which addresses its dual function in air defense and force protection.[272]

   NATO is working to define a common C-UAS architecture, which aims to provide clear guidelines regarding the communication between C2, sensors, and effectors, and an effective integration of this information into both the broader air and missile defense network of the alliance and the civilian air traffic management system. [273]

   To this end, at least one nationally established communication standard may offer a solution to NATO. The UK-developed SAPIENT interface is used for intra-C-UAS communications (i.e., between C2, sensors, and effectors) and other encrypted systems like Link-16 and Asterix to interact with air defense and civilian air traffic management, respectively. This architecture has already been tested during NATO's technical interoperability exercises (TIE), which involved the private sector and aimed "to reach time-zero integration" through the creation of a local integrated air picture that incorporated different C-UAS solutions.[274]

4. **Integrating automated and autonomous capabilities at scale are currently limited by allied members' abilities to sort, share, store, and analyze data**. AI-enabled multi-sensor fusion capabilities can combine and analyze massive amounts of data and allow for autonomous detection, thus eliminating the burden on human operator reaction time and availability. AI could be a game-changer, especially against swarming attacks. For example, the US company Anduril has pioneered a layered, AI-powered C-UAS capability that combines multiple sensors and effectors into a scalable, open operating system for autonomous detection, tracking, and threat indication at edge speed. Recently, the US Army Task Force 39 has tested an AI-powered phone app called "CARPE Dronvm" that uses pictures to identify drones at short range and determine their flight path, sending real time notifications to friendly troops nearby and improving their situational awareness.[275] Overall, however, the incorporation of these technologies across NATO remains slow due to responsible use concerns, diverse national approaches to autonomous systems, and different levels of investments.[276]

5. **The cost-per-interception curve is arguably one of the major challenges for C-UAS**, given the proliferation of cheap, expendable UAS and LMs. This unfavorable cost curve is compounded by the increased resilience of drones against EW attack, which often makes it necessary to resort to relatively expensive kinetic interceptors.

   The progressive introduction of directed-energy weapons (DEW) (i.e., laser and high-power microwaves) promises to revolutionize C-UAS and make it much more cost-effective. DEW systems provide a deeper magazine with a lower cost per shot and a cheaper system lifecycle due to their minimal logistical needs.[277]

   A major challenge regarding DEW is making them mobile. The US Army is currently testing the Directed Energy Maneuver-Short Range Air Defense (DE M-SHORAD) system, based on a Striker family vehicle outfitted with a 50-kilowatt class laser weapon able to detect and defeat small and medium UAS as well as rockets, artillery, and mortars.[278] This program includes a first platoon of four Striker systems already delivered to the Army for testing and goes hand in hand with the so-called Army Multi-Purpose High Energy Laser (AMP-HEL), an initiative to install a 20-kilowatt laser weapon system on infantry squad vehicles to provide short range C-UAS capabilities for small units.[279] Recently, Raytheon has delivered to the US Air Force a palletized 10-kilowatt laser weapon known as "H4", installed on a pick-up truck in a stand-alone configuration, "allowing it to be moved and mounted wherever needed".[280]

   However, directed energy weapons are only part of the C-UAS solution. DEW remain embryonic in maturity and challenged by atmospheric factors. Further, their considerable cooling needs impose tradeoffs between power and compactness.[281]

Survivability

Because of their design — which sacrifices maneuverability and speed for maximum endurance, range, and energy efficiency — most large and medium UAS currently in service with NATO countries are easily detectable and trackable by air defenses. Novel engineering solutions and materials will increasingly reduce radar and IR signature, but at present such solutions and materials are in use by only a few high-end platforms. In addition, the lack of onboard self-protection capabilities makes most MALE and HALE UAS easy targets for modern air defenses.

As such, NATO and allies' medium and large UAS would likely suffer high, and thus hardly sustainable, losses against peer and near-peer adversaries. The incorporation of threat warning systems and passive and active countermeasures

is already possible, although it comes at the expense of other payload options. This tradeoff impacts the drone's final suite of capabilities for specific missions.

The Self Protection Pod (SPP) developed by General Atomics for the MQ-9 family includes both radar and IR missile threat detection and a chaff and flares dispenser, providing full-spectrum awareness and countermeasures that will increase the system's survivability in contested environments.[282] However, the SPP technology falls under the US International Traffic in Arms Regulations (ITAR) regime and, for the moment, is not available to NATO allies.[283] However, a similar technology that is export-ready, or ready for a relaxation of the ITAR restrictions, should be considered as the MQ-9 becomes the centerpiece of many NATO members' UAS fleets.[284]

When it comes to smaller UAS, the limited payload capacity partially frustrates the advantage of reduced acoustic as well as radar detectability. Like in larger systems, the data link and the operator of small UAS are vulnerable to EW and kinetic attacks, respectively. Small drones are typically operated at tactical and operational ranges and their self-protection capabilities are limited to anti-jamming and EW-resistant components, without anti-missile countermeasures. Less restricted quantity and expendability due to lower cost offset these limitations.

Overall, modular and built-in self-protection capabilities will be essential to allow present and future UAS to operate in high-intensity scenarios. These comprise integral cyber security solutions against cyber threats, and layers of redundancy to ensure reliability and protection against potentially altered components from corrupted supply chains.[285] Reliability and availability deserve particular attention considering the complexity and vulnerability of today's supply chains and the increasing number of dual-use components used in military-grade systems.

Equally important, vulnerability applies to the ground segment and control elements as well. Network nodes, different transmission links, and software components are exposed to EW and attacks in the cyber domain while ground control stations and support infrastructure close to or in the area of operation are also potential targets for kinetic strikes.[286] These vulnerabilities require adequate countermeasures in terms of redundant and secure communication protocols, discipline across the electromagnetic spectrum, force dispersion, and concealment.

Personnel and Training

Conventional wisdom stating that UAS require less personnel because of their uncrewed nature does not always reflect reality. While a two-member team can be sufficient for small tactical UAS, larger platforms such as MALE and HALE UAS require a variable number of skilled professionals:[287] pilots, sensor and C2 operators,

weapons system officers, analysts, and support personnel. The actual figure may be equal to or even greater than the total required for crewed aircraft.

For example, a typical US Air Force UAS combat squadron consisting of four MQ-9 UAS of which at least one is airborne 24 hours per day, seven days per week could require up to 192 personnel. This number covers the mission control element (49), the forward-deployed launch and recovery element (59), and the PED element (84), depending on the mission and operational environment.[288] In comparison, an AC-130H gunship has 14 crew members, and an E-8C Joint Surveillance Target Attack Radar System (JSTARS) requires between 21 and 34 personnel, depending on the mission's nature.[289]

Larger platforms such as the NATO-owned RQ-4D are even more personnel-intensive, with the crew to aircraft ratio for the pilot and sensor operator positions estimated at 15:1.[290] Indeed, due to the RQ-4D's sophistication, unique data collection capabilities, and complex support infrastructure, the NATO AGS Force (NAGSF) requires more people than a similar organization of crewed aircraft. NAGSF's relatively larger manning is primarily due to its self-contained nature with organic PED capabilities and training cadre (for pilots, analysts, and support personnel).[291]

According to the NAGSF commander, personnel is the most important issue that prevents or slows progress on the attainment of full operational capability whose criteria "is predicated on flying multiple aircraft at once and delivering a certain number of intelligence products with specific response times".[292] This issue has been exacerbated by the increasing demand in terms of sorties and ISR output prompted by the war in Ukraine. At present, the NAGSF's available personnel are around 60% of the overall target quota, making the goal of achieving FOC by 2024 very difficult.[293]

More broadly, western militaries' already insatiable appetite for ISR products including full-motion imagery[294] and the need to exploit them around the clock could skyrocket in high-intensity scenarios. In the short term, the need for multiple sensor and strike capabilities will expand the demand for personnel at a time when many Western militaries are experiencing rising manpower shortages, including UAS crew members, analysts, instructors, and specialized staff.[295]

Shortfalls in UAS units' personnel can reduce operational readiness and flexibility, flight time, and analytical output, as well as have negative impacts in terms of fatigue due to increased workloads and irregular leave periods, among other factors.[296] Manning shortfalls in UAS units can exacerbate personnel management issues and the effectiveness of UAS operations. AI tools may help in numerous areas but will not completely replace the need for people.

Photo: Capt. Brian Maggi, Head of Civil Engineering at the Coast Guard Academy, holds up a drone during a training course at the Coast Guard Academy, New London, Conn, Feb 21, 2023. Credit: Petty Officer 3rd Class Matt Thieme/US Coast Guard

At the same time, the quality of personnel also deserves attention. Indeed, dealing with increasingly sophisticated sensors, munitions, and complex data packages requires highly qualified staff — including in the maintenance role — and the analytical capacity to fuse, process, and disseminate information from multiple sources rapidly and in a multi-domain environment. The same holds for advancements in C-UAS technology and novel approaches to how C-UAS is integrated and how C-UAS operations are conducted across joint forces.[297]

As such, traditional training models may fall short of the cross-cutting skills and expertise levels needed to master these new technologies, from operations to logistics to maintenance to PED. The high operational tempo that typically characterizes UAS missions can limit the time available to complete training requirements on weapons employment and emergency operations.[298] Training simulators can tackle some of these challenges, providing standardized yet flexible plug-in training scenarios while removing physical, time, and logistical obstacles typical of a multinational military alliance like NATO. The US Army, for example, has recently conducted virtual exercises in a “synthetic training environment” in which several Army branches used drones to coordinate massive artillery strikes against fictional soldiers, in a Ukraine-like situation.[299]

Additionally, effectiveness in joint and multi-domain operations requires close training between UAS crews and PED teams, which is more often conducted separately reducing the synergy and efficiency needed for successful operations.[300]

The NAGSF was designed to provide in-house "organic training" covering all the roles and responsibilities required for AGS employment and currently involves troops from most allied nations.[301] At the moment, NAGSF employs a number of contracted instructors. As an assigned training cadre increases, NAGSF will gradually shift from contractor-based to NATO-led instruction.[302]

NATO holds regular exercises that include the use of MALE UAS, in particular the MQ-9. These exercises hone the skills of UAS pilots and operators to effectively conduct a variety of missions, including close air support and combat search and rescue in multiple scenarios.[303] As more member states receive the Reaper platform or its upgraded MQ-9B version, the frequency and scale of joint training and exercises should increase, but the lack of training facilities may be an obstacle for some countries. The NATO Flight Training Europe (NFTE) initiative aims to overcome this challenge by establishing a network of multinational training facilities for pilots of different types of aircraft, including UAS.[304] The introduction of training simulators at scale offers another valid and cheaper solution.

Finally, as combat experience in Ukraine has proven, an overemphasis on technology alone is dangerous, as technology never works in isolation and is hardly the sole cause of victory.[305] Common doctrine and concepts constitute key ingredients to maximizing the potential for UAS and C-UAS to achieve desired battlefield effects, but talented, trained, and educated leaders, operators, and other contributors (e.g. data, cyber, and network specialists, analysts, software writers, maintainers, etc.) may be as or even more decisive.

NATO has recognized the importance of training and education of leaders and staff in its policies on emerging and disruptive technologies.[306] As a result, people are a key focus of NATO's digital transformation efforts.[307] In a similar vein, human resource and leader development must be a key element of UAS and C-UAS capability integration into NATO and individual allies' forces.

The Tasking, Collection, Processing, Exploitation & Dissemination (TCPED) Cycle

As noted by former US Air Force Chief of Staff General David Goldfein, "data is the currency of future warfare, and we must be able to fight at the speed the future will demand."[308] With both the amount and complexity of data steadily on the rise, allies must be able to collect, analyze, exploit, and share federated intelligence rapidly and at scale through a joint TCPED process. However, such a process "is [currently] operating at a level below its potential and short of strategic and operational need."[309]

Reaching the full potential of the alliance's TCPED relative to UAS national and NATO contributions will require a more robust, federated, multi-domain approach. Elements of such an approach are in place or in development, but many challenges remain. Meanwhile the importance of timely and quality intelligence has only grown in NATO's view of its threats and challenges.

The alliance's new strategic concept envisions a strengthened deterrence and defense with more forward-based defense capable of achieving deterrence by denial.[310] Deterrence by denial and effective defense against a peer adversary require persistent surveillance and situational awareness before and during conflict. National and NATO UAS capabilities will be a necessary component to achieving persistent surveillance and effective situational awareness from the theater to tactical levels.

Assuming a likely increase of future UAS capabilities (across all domains) and contributions to NATO (e.g., early warning and intelligence pre- and post-crisis or conflict) there are several challenges or limitations that need to be addressed in order to reach full potential of NATO TCPED.

These include:

- the willingness of individual allied states to share intelligence;
- NATO's capacity to process and exploit, the latter related to expected increases in UAS sensor data on the one hand and manning and technical limitations on the other.

At the most basic level, sharing of national intelligence remains the most important limiting factor. Crises and operations tend to lead to an increase in national sharing within NATO as has been the case for the Russian war on Ukraine.[311] Extensive intelligence sharing, however, continues to be practiced by just a few key allies and concerns persist over the security of information or intelligence shared with NATO.[312] That said, the upward trend of national UAS inventories will inevitably lead to an increased quantity of raw data and processed intelligence that nations may contribute to NATO.[313]

On a positive note, the NATO AGS Force is intensifying its collaboration with national ISR entities, including the US Air Force Distributed Ground System-4 based in Ramstein, Germany and the UK Royal Air Force's N.1 ISR Wing, to develop a robust joint data-sharing and communication network that can bridge the intelligence gaps of single allies.[314]

Still, increased quantity in terms of UAS intelligence sharing will only contribute to quality if there is sufficient analytical and dissemination capability to ensure

timeliness and delivery of the right data to the right people within the time limit of intelligence value.

The ability to fuse a variety of UAS sensor data with other multi-domain intelligence will also be critical to higher levels of confidence in analysis as well as the quality of data needed for timely identification, targeting, and engagement of threats.

Analytical capability is currently limited by the number of both trained and available analysts as well as the relatively limited use of AI tools.[315] While the NATO Intelligence Fusion Center (NIFC) has several imagery analysts, NAGSF has by far the largest concentration of sensor analysts in NATO.[316] NAGSF also has an organic analyst training capacity and thus offers a valuable, but underutilized potential to train national intel analysts from across NATO to process UAS intelligence. Despite the large number of authorized sensor analysts, the training slots are not filled.[317] NAGSF's personnel shortfall represents a self-imposed limitation that nations could easily address.

The importance of AI as a combat multiplier in data-centric processes is recognized by NATO and the object of use cases envisioned by NATO's AI Strategy.[318] Initial use cases are underway. For example, AI tools have begun to be introduced into NIFC and NAGSF for limited tasks (i.e., for NIFC sorting large amounts of open-source imagery to verify aircraft status and for NAGSF identifying targets during post-operation imagery analysis).[319]

AI has great potential in enabling NATO analysts to sift through and sort relevant UAS data in real or near-real time for cueing, fusing, and processing depending on how that UAS data is fed or shared and where the AI tools are located in the data architecture. AI could also be introduced into NATO or national UAS to improve real time situational awareness, decision-making, and action at the tactical edge.

Technical shortfalls related to digitalization,[320] network bandwidth, and latency also limit the speed and capacity of NATO and national TCPED processes. These issues are inevitably tied to digitalization efforts — or lack thereof — by single allies and the alliance as a whole. NATO's Digital Transformation campaign is underway and will tackle these technical shortfalls and others (i.e., people and process aspects as well), but success will take time, resources, and sustained political commitment.

In the case of the NAGSF, real time transmission of operational data from the RQ-4D's sensors to the PED element is another technical limitation. The communications capability and security are not in place. Imagery is analyzed once downloaded post-operation. The intake of ISR products from other platforms can also be slow.

For example, in a recent NATO exercise, it took two and a half hours for the NAGSF PED element to receive an image from a U2 spy plane and identify potential targets,

while the goal is to do so in 45 minutes.[321] According to the NAGSF commander this time has now dropped to 30 minutes.[322] In a peer-adversary conflict, a much more compressed, if not near-real time situation, TCPED process will be needed to retain a decisive advantage over adversaries from strategic to tactical levels.

While the AGS has the potential "to become the data-manager for ISR for NATO" and provide federated PED products, it needs constant access to additional intelligence disciplines like SIGINT and ELINT in order to succeed.[323] Moreover, the need for a multi-source, multi-discipline federated intelligence requires an increasing number of specialized analysts, not only in NATO ISR structures but also at the national level, along with a scalable, modular and interoperable training system. These aspects confirm that an effective PED process depends on manpower, which, in turn, is a function of training.

Recommendations for NATO and Allies to Enhance UAS and C-UAS Capabilities

For NATO and allies to leverage and prepare for the full potential of future drone warfare this report recommends the following:

- First, the alliance must clearly assess UAS and C-UAS capability requirements based on lessons learned from recent conflict, technological developments underway, and expected future threats and challenges. (Recommendations 1, 7)
- Second, UAS and C-UAS capability development and policy development must be guided by the need for scale and interoperability and the imperatives of multidomain operations. (Recommendations 2, 3)
- Third, enabling capabilities such as AI tools, data architecture, communications networks, and cyber and space capabilities and services must be enhanced. (Recommendation 4)
- Fourth, NATO and individual allies should leverage the significant innovation efforts underway while improving operational experimentation and procurement processes. (Recommendation 5)
- Fifth, NATO should refine or establish joint allied doctrine, operational concepts, and TTPs to cover new and expanded roles of UAS and the growing importance of C-UAS. (Recommendation 6)
- Sixth, both UAS and C-UAS capability integration into NATO and national forces will require a special focus on human resource development. (Recommendation 8)

The following detailed recommendations are intended to assist NATO and NATO nations in building on positive momentum already achieved by leveraging new concepts and approaches and considering new or revised efforts:

1) Define Clear UAS Capability Requirements and strike the Right Balance Between Quality and Quantity

As a first step, given the expanding roles and missions for UAS, NATO should assess the UAS capabilities that would be most important for the alliance and allies to acquire and/or develop in order to meet security and defense needs. Lessons learned from recent conflicts, ongoing national force modernization initiatives, as well as science and technology trends should feed this assessment.

Photo: A US Air Force Explosive Ordnance Disposal (EOD) technician prepares a Mk. II Talon bomb disposal robot for work during exercise Northern Challenge. Credit: NATO

NATO assessment should be clear on what UAS capabilities allies need as compared to the capabilities NATO needs for itself. Military authorities could already begin to address the expanding potential for UAS in the Minimum Capabilities Requirements (MCR) process currently underway (Step 2 of NATO's five step defense planning process).

NATO and member states should adopt a balanced approach towards UAS, consistent with the ultimate purpose of UAS technology: to provide more flexibility and risk-tolerance in military operations through uncrewed systems that are cheaper, more expendable, and that minimize the risk of personnel losses. Even the loss of more expensive UAS may be balanced against the likely gain in intelligence or battlefield effects achieved. As such, NATO ought to prioritize a mix of high-end UAS and cheaper but expendable and mass-deployable systems, without losing sight of the capacity to replenish losses over time.[324] Achieving scale in manufacturing of small UAS, assisted by private investment, will be necessary to meet the numbers likely needed for high-intensity conflict.

As NATO is adopting a plans-based capability process for the first time in decades,[325] allies should consider requirements for UAS of all classes (large to micro) for strategic and regional plans and include them in force generation for the NATO Force Model. As Class II and III UAS are currently low-density, high-demand assets and likely to remain so, NATO will need to be flexible on how it integrates national contributions for different plans or force structures. National contributions may range from forces to systems, and include flight hours, targets serviced, and PED.

NATO and NATO nations should:

- Assess NATO's UAS requirements holistically in light of recent conflicts, scientific and technological trends, and NATO's family of plans;
- Invite input from relevant NATO armaments communities and NATO's Science and Technology Organization (STO), as well as nations to assist NATO Military Authorities in the UAS assessment;
- Incorporate the expanding roles of UAS (or as much of the NATO UAS assessment as possible) in the ongoing MCR process for 2024;
- (If not already a component) incorporate a flexible approach to national UAS contributions in NATO plans and the NATO Force Model;
- Incorporate a flexible approach to UAS contributions for national UAS capability targets in the apportionment process of 2025.

2) Continue to Enhance UAS Interoperability

Interoperability is essential for NATO. Interoperability enables a multinational and diverse group of forces to achieve common understanding, to execute decisions, and to act and react with greater speed and effect. Interoperability allows the alliance to fight with a common purpose and to execute missions that are only possible through forces and capabilities unified by common or compatible means of communications, command and control, doctrine, and standards.

As NATO gears up for operations in contested environments, it should increase the interoperability of its UAS (and C-UAS) capabilities, from forces to platforms to payloads, to the human element and enabling infrastructure. Shortfalls in the implementation of agreed air traffic management regulations are hindering operations, responsiveness, and readiness. These in turn limit the benefit UAS capabilities can provide allies in terms of intelligence and deterrence effect.[326] In particular, the alliance and individual allies should:

Issue air traffic management regulations and directives agreed by NATO to enable responsive NATO AGS and other allied UAS operations in civilian airspace, including for basic overflight/diplomatic clearance, dynamic flight route planning, and diversion for emergencies;[327]

Verify implementation of existing NATO agreed standards (i.e., for airworthiness, flight safety, airspace integration, sense and avoid, operator and pilot training, human systems interface, interface of unmanned control systems for UAV, and TTPs for unmanned aircraft);[328]

Invest in modularity, specifically payload-agnostic UAS and platform-agnostic payloads that can be configured, reconfigured, and integrated across the alliance;

Advance and improve standardization in all areas relevant to the development and use of UAS, with a focus on:

- Training and certification, airworthiness, airspace integration, airfield access, etc. (especially Class III given future impact of increasing numbers of MALE, HALE, Combat UAS);
- Communication protocols, data storage, and data sharing formats, including for cross-cueing information from UAS to other assets and vice versa;[329]
- Payloads (i.e., sensors, effectors, etc.);
- C2 interfaces and operating systems;
- Detect/Sense and Avoid technology;
- Increase UAS access to national airspace for training, exercises, and experimentation;
- Enable UAS and C-UAS access to the regulated electromagnetic spectrum for training, experimentation, and operations;
- Increase the quality (scale and scope) and frequency of NATO exercises focused on or incorporating UAS and C-UAS to improve interoperability, concept/TTP development, and operational effectiveness;
- Expand the scope of NATO Unified Vision exercises to include C-UAS and other UAS threats;
- Establish a NATO UAS Center of Excellence;
- Consider establishing a NATO UAS Center of Research and Experimentation focused on UAS and C-UAS integration, interoperability, and expanding UAS / C-UAS roles in C4ISR, IAMD, and targeting
- For allies operating the same UAS platforms, consider multinational cooperation schemes similar to the MQ-9B International Cooperation Program to share best practices and further refine interoperability.

3) Prepare to Employ UAS in Multidomain Operations

Both NATO and individual allies should develop and acquire UAS capabilities for multidomain operations against near-peer adversaries. Such operations are likely to be characterized by data-centricity, speed (of decision and action or operational tempo), employment at scale of sensors and effectors (including uncrewed systems), communications-degraded and/or denied environments, and decentralized and/or disaggregated forces.

UAS of all classes are likely to support operations in all physical domains with increasing capabilities and have an increased need for interconnectivity (to operate

Photo: One of five NATO RQ-4D aircrafts called “Phoenix” presented in the hangar on Sigonella airbase in Italy. The remotely piloted aircrafts are part of the Alliance Ground Surveillance System that 15 NATO Allies have acquired together. Credit: OR7 Pia Dunkel/German Army/NATO

in C4ISR, targeting, and IAMD networks). They also have an increased need for enablement from the cyber and space domains. UAS offer advantages in agility, versatility (multi-mission capabilities), resilience (e.g., expendability for Class I UAS or avoidance of human casualties for crewed missions that UAS can undertake), and creativity (new roles and missions resulting from collaborative, swarm, and combat capabilities).

Given lessons learned from recent conflict, trends in UAS and related technologies, and ongoing research, development and experimentation, NATO and NATO nations should:

- Develop a NATO UAS capability development strategy (perhaps by expanding upon the expertise and experience gained through NATO’s R2i);
- Consider maintaining a current database of UAS systems developed and employed by NATO and non-NATO nations organized in accordance with the NATO UAS classification system;
- Incorporate UAS at scale and at all echelons to ensure each level of command has the appropriate drone capabilities for the assigned tasks. This includes a careful assessment of quantitative requirements for Class I UAS, given the likelihood of high attrition rates;

- Prioritize UAS with both short and vertical takeoff and landing (STOL and VTOL) capabilities, all weather capabilities, modular payloads, multi-sensors, multi-purpose medium-to-long-range loitering munitions, one-way attack drones, and logistic functions (e.g., transport for resupply or evacuation);
- Given the associated costs, consider multinational acquisition schemes and investments in BLOS stealth and/or survivable combat UAS with long-range weapons for threat air-defense penetration, counterair, interdiction, and standoff anti-ship missions, among others;
- Consider more investment in UAS for communications relay and air-to-air refueling of crewed aircraft;
- Invest in self-protection capabilities for larger Class II or III UAS (both legacy and next generation);
- Invest in human-machine teaming capabilities to improve situational awareness and multiply the effects of crewed systems;
- Develop specific operational concepts and TTPs addressing the use of UAS in contested environments (including collaborative groups or swarms, human-machine teaming, expanded land, maritime, and joint air power missions).

4) Expand and Enhance UAS Enabling Capabilities

Effective employment of UAS and C-UAS rely on supporting capabilities, even more so when employed at scale, when operating collaboratively with other uncrewed or crewed systems, and in support of multidomain operations. Supporting capabilities include robust and secure communications networks and data architecture as well as cyber, space, and AI technologies in general. Cyber security and defense are critical to networks and data architecture, and space support can enhance both.

Cyber security is essential for all on-board components of UAS, for electromagnetic communications used in supporting networks, as well as for software and hardware of communications equipment and command and control stations. Space-based communications can enable UAS and C-UAS operations in remote or contested environments. Space-based navigation and MET data enable both remote and autonomous flight as well as targeting and engagement. Space-based intelligence can also enable on-board or remote data fusion for threat identification, avoidance, and engagement.

AI capabilities can enhance communications networks through functions such as dynamic routing and frequency management. AI capabilities can enhance data architecture through functions such as sorting, fusion, and cueing. AI can also enable single platform functions such as sense and avoid, target identification, and engagement, as well as group functions such as collaboration and swarming.

NATO's 2021 AI strategy is a very good starting point as it has both established principles of responsible use, the importance of alliance expertise in AI, and the need to develop use cases to demonstrate the value of AI applications and build trust.[330] NATO has also established a Data and AI Review Board to build trust in AI, guide responsible AI adoption, and provide a NATO forum for sharing developments and views on AI.[331] The alliance should leverage this foundation to ensure AI is applied to NATO and national level programs involving UAS and enabling capabilities.

Integration of UAS and C-UAS into tactical or operational level C4ISR networks, targeting or fires networks, and IAMD also rely on supporting capabilities such as robust and secure communications networks and data architecture (ideally AI and space enabled). Integration of UAS and C-UAS into C4ISR, targeting, and IAMD networks is also essential to achieve multidomain effects.

Finally, alliance efforts to implement digital transformation,[332] enhance data exploitation,[333] and implement related interoperability standards will greatly contribute to establishing the foundations for robust and secure NATO networks and data architecture. Collective and national political will to follow through on NATO commitments, to implement NATO standards, and to ensure adequate investment will all be necessary as well.

Given these considerations, NATO and allied nations should:

- Ensure specific requirements for enabling UAS and C-UAS operations figure prominently in NATO's digital transformation implementation efforts and in implementation of the alliance Multidomain Operations Concept;
- Prioritize NATO AI use cases for enabling NATO AGS Force capabilities (e.g., sense and avoid, friend and foe/threat identification, multi-sensor/intelligence fusion), operations, TCPED, and sustainment; and follow successful AI use cases with prompt modifications or upgrades;
- Prioritize NATO digital transformation and data exploitation efforts to enable NATO AGS Force capabilities, supporting data architecture, and TCPED process;
- Ensure secure, accredited, and redundant communications and real-time data flow to enable NATO AGS Force operations and enable real-time sharing of AGS data/intelligence with other crewed and uncrewed aircraft/aerial systems;
- At a minimum, ensure national UAS fleets can communicate and share data among like systems as well as compatible classes of UAS (including their ground stations) across the alliance;
- Establish the concepts and standards (communications, tactical data links, data, and interface protocols) to integrate UAS in relevant NATO tactical and operational networks (i.e., C4ISR, targeting or fires, IAMD); and follow through with testing and experimentation (see next bullet), implementation, and verification;

Photo: Members of the 163d Attack Wing pilot an MQ-9 Reaper taxing down the runway after returning home from a milestone mission to Shaw Air Force Base, South Carolina, February 15th, 2024. Credit: Tech. Sgt. Paul Duquette/US Air Force

- Ensure future NATO interoperability trials and operational experimentation includes real-time networked UAS and C-UAS from across the alliance, and include testing of UAS and C-UAS as integral parts of NATO tactical and operational networks (i.e., C4ISR, targeting or fires, IAMD);
- Share national developments related to UAS capability and enabling capability development (e.g., US DARPA UAS programs,[334] US CENTCOM's TF 99,[335] UK Army Warfighting Experiment and UK Army, Research, Innovation and Experimentation Laboratory UAS activities[336]) and incorporate lessons in both NATO and national UAS or C-UAS capability development;
- Invest in AI-enabled UAS, redundant, secure, and next generation communications, supporting data architecture, 3D printing and advanced manufacturing, and quantum technology;
- Ensure sufficient resident expertise in national and NATO forces and staffs to leverage AI, data science, computer science, communications network science, autonomy, and space for UAS and C-UAS capability development and employment;
- Contribute national cyber and space capabilities to enhance NATO UAS and C-UAS operations, including nationally owned LEO satellite constellations that can enhance secure, resilient connectivity such as the US Space Force's Transport Layer.

5) Leverage NATO Innovation and Improve Agility in Procurement Processes

The increasing pace of technological innovation has a direct impact on warfare and the ability to harness and integrate technological breakthroughs quicker than adversaries. This will be a decisive factor.

NATO policies and initiatives on innovation and the promotion and protection of emerging and disruptive technologies offer opportunities to exploit collaborative allied efforts in research and development (R&D), investment, and acquisition. NATO's Science and Technology Organization (STO) promotes collaborative science and technology activities and regularly publishes documents on trends related to UAS and enabling technologies.[337]

NATO's DIANA,[338] as mentioned previously, includes a multitude of test centers focused on enabling technologies relevant to UAS (e.g., AI, autonomy, data, space)[339] and is currently focused on rapidly developing solutions to military challenges in the areas of energy resilience, secure information sharing, and sensing and surveillance.[340] All of these are relevant to UAS and could lead to improved capabilities. The NATO Innovation Fund is the first multinational sovereign venture fund of its kind, and could also be leveraged by allies to scale up promising UAS capabilities or solutions to meet allies' defense needs.[341]

Speed, agility, and effectiveness are at the heart of NATO policy on Achieving and Accelerating Capability Development and Delivery (A2CD2).[342] The policy aims to identify opportunities for accelerated delivery, to pursue approaches with highest potential payoffs, and to deliver results through enhanced collaboration between NATO military and industry, and between NATO military, armaments, and science and technology activities.

A2CD2 policy promotes increased multinational cooperation and leveraging testing and experimentation within NATO exercises to enable warfighter interaction with the private sector, and wargaming and tabletop exercising of capability solutions.[343] While UAS are not a priority focus of A2CD2 policy, NATO and NATO nations could leverage the policy to expand operational experimentation and enhance private sector collaboration in key technologies to improve UAS capabilities.

NATO common-funded procurement and most NATO nations' procurement processes remain slow and maladapted to rapidly adopt and scale promising UAS technologies. Adjusting bureaucratic and regulatory processes for risk tolerance, joint industry-end user design teams, rapid prototyping, iterative operational experimentation, multi-year funding, in-year budget reallocations, and multinational procurement are all aspects of improved agility in acquisition that would benefit allies seeking to accelerate UAS development and acquisition.

Photo: US Air Force Airmen 1st Class Anika Manabat, 432nd Maintenance Squadron avionics journeyman, examines an MQ-9 Reaper after landing at Marine Corps Air-Ground Combat Center, Twentynine Palms, California, July 25, 2023. Credit: Senior Airman Kristal Munguia/US Air Force

NATO and individual allies should consider alternative acquisition models to overcome budget constraints and access high-end capabilities like MALE and HALE UAS through leasing or multinational procurement. Typically, leasing also allows customers to get comfortable with the platform, while keeping open the option of full acquisition.[344]

Finally, given the increasing reliance on the US-made MQ-9 family of UAS by several NATO nations, the US should consider a reassessment of, and/or targeted exemptions from ITAR and other export restrictions on specific UAS technologies and components (e.g., sensors, self-protection capabilities, low-observable features, payloads, etc.) that limit access to UAS capabilities across the alliance and risk unnecessarily limiting the effectiveness of NATO missions, activities, and operations. This would require close coordination between US Government departments (e.g., Commerce, Defense, State, etc.), Congress and the related industry.

U.S. Marine Corps Marine Unmanned Aerial Vehicle Squadron (VMU) 3, Marine Aircraft Group 24, begins the assembly phase of the MQ-9A, Marine Corps Air Station Kaneohe Bay, May 10, 2023. Credit: Cpl. Christian Tofteroo/US Marine Corps

NATO and NATO nations should:

- Leverage DIANA 2023 priority areas to develop promising technologies relevant to UAS (e.g., multi-mission payloads, self-protection capabilities, AI tools for collaborative control and data exploitation, cyber security, green power, and propulsion solutions);
- Leverage the NATO Innovation Fund to scale up UAS technologies that will help allies meet UAS-related capability targets and leverage UAS capabilities for multi-domain operations;
- Promote frequent NATO operational experimentation of maturing UAS technologies to allow for operator/commander interface with industry developers and accelerate UAS capability development and delivery;
- Promote wargaming and tabletop exercising of UAS capability solutions to identify cost-effective capabilities, employment concepts, and TTPs;
- Adopt agile capability development and resourcing principles for UAS capabilities and services;
- Leverage NATO agencies (especially NSPA for UAS acquisition and NCIA for cyber, data, and space related capabilities enabling UAS operations) for multinational procurement of common UAS and enabling capabilities;
- Consider lease agreements (including bi-lateral or multinational) for UAS fleets or more expensive UAS platforms and payloads. Lease agreements come in multiple forms, such as for life cycle maintenance, operations, or fully company-owned/company-operated (COCO). Lease agreements may allow for quick capability fielding and long-term cost savings.

The US should:

- Review the ITAR and other export control regulations affecting specific UAS and associated technologies, avoiding unnecessary restrictions that could weaken the UAS capabilities of NATO allies, limit research and development in the UAS segment, and potentially undermine the use of UAS in NATO mission, activities, and operations.
- Encourage the joint development and production of UAS and/or associated technologies alongside allied or partner nations' industries in order to promote cost-sharing, enhance interoperability, and minimize the vulnerability of the Transatlantic defense industry community to export restrictions.

6) Develop Joint Allied UAS Doctrine

The definition of a specific UAS joint allied doctrine would provide NATO forces and nations with a clear framework regarding the use of UAS in deterrence and defense, including high-intensity, contested environments. The NATO Joint Air Power Competence Centre's (JAPCC) 2010 white paper on a Strategic Concept of Employment for UAS in NATO is a great foundation for a joint allied doctrinal document.[345] However, many developments have occurred since JAPCC's white paper was published (e.g., advancements in AI, autonomy, communications, cyber, data management, and space) that have expanded UAS capabilities, roles, missions, and employment techniques.

Unmanned aircraft and unmanned aerial systems are mentioned in NATO's 2016 publication on Allied Joint Doctrine for Air and Space Operations.[346] References, however, are limited to the persistent presence of UAS, a UAS classification table, the generic need to counter UAS threats, and the need to plan apportionment of unmanned aircraft in operations.

If not already in development, NATO military authorities should provide the appropriate direction and guidance to rapidly develop joint allied UAS doctrine, taking advantage of existing national doctrine where appropriate.[347] Joint allied UAS doctrine would be instrumental in NATO defense planning, identifying common UAS capability and force requirements, promoting UAS capability development and integration, promoting related concept development (e.g. TTPs), enhancing operational experimentation and interoperability trials, and enhancing training and exercises, etc.

As a minimum joint allied UAS doctrine should address:

- UAS contributions to land, sea, and air power (e.g., C4ISR, targeting/fires, IAMD, and logistics);

- UAS classification and common types in service;
- UAS organizations and structures;
- NATO principles of responsible use as applicable to UAS;[348]
- Mission sets (e.g., JISR, ISTAR, strike, EW, SEAD/DEAD, transport, relay, and decoy);
- Collaborative crewed-uncrewed operations (fixed and rotary wing);
- Collaborative group and swarm operations;
- Employment considerations (e.g., payloads, combined arms integration, and airspace management);
- Enabling capabilities (e.g., digitalization and data / network architectures, PED, cyber, and space);
- Interoperability (e.g., material and data standards, operational TTPs, testing, and verification).

7) Invest in and Scale up C-UAS Capabilities

The proliferation of low-cost, expendable UAS and loitering munitions is revolutionizing the sensor-to-shooter cycle and challenges the survivability of forces and systems across the depth and breadth of the battlefield. Furthermore, as one NATO military commentator put it, "peer competitors to NATO can be expected to employ UAS at the same level of technology, and under comparable operational principles, as the alliance."[349] Hence, C-UAS should be at top of NATO's priorities with UAS.

In general, the previous recommendations with respect to UAS doctrine development, capability and concept development for MDO, innovation and procurement, and interoperability apply to C-UAS capabilities. NATO and allied nations should:

- Invest in C-UAS capabilities and adopt them at scale across the military based on a comprehensive and cost-effectiveness distributed approach that ensures both air defense of forces and areas and single vehicle/platform/system protection.
- Ensure C-UAS capabilities available to NATO include a layered mix of kinetic and non-kinetic effectors, i.e.:
  - EW and directed energy weapons, including portable C-UAS guns;
  - Mobile short-range air defense systems (e.g., M-SHORAD), counter-rocket, artillery and mortar (C-RAM) systems, and anti-aircraft direct fire systems;
  - Cyber warfare against UAS ground terminals and control stations;

  - Air-to-air weapons for short range air defense and longer-range air interdiction.
- Expedite the development of joint allied C-UAS doctrine, currently in the drafting phase. An approved C-UAS doctrine would help streamline and add coherence to other C-UAS work strands, including the definition of common capability requirements, concepts of operation and employment, and TTPs;[350]
- Ensure harmonization of C-UAS-related policies across the NATO enterprise;
- Develop, implement, and verify C-UAS material and operational standards;
- Expand the role and scale of C-UAS into NATO Integrated Air and Missile Defense (IAMD) policy based on recent developments, including lessons learned from recent conflicts. In particular, consider the establishment of a robust C-UAS architecture (sensors, C2 nodes, effectors, data fabric) to expedite the kill chain and improve the coordination between C-UAS, other IAMD components. and civilian air traffic control authorities;
- Increase the number and frequency of technical exercises and experimentations;
- Ensure C-UAS capabilities and concepts are incorporated as part of IAMD into collective and joint training at all levels;
- In light of technological developments and lessons learned from recent conflicts, ensure C-UAS are addressed at scaled within the NATO Defense Planning Process (especially 2024 MCR and 2025 capability apportionment steps);
- Include C-UAS training, concepts, doctrine, and development in a NATO UAS center of excellence;
- Review military organizations and force structure in parallel with C-UAS doctrine and concept development to ensure the right C-UAS systems and capabilities at scale for air defense and force protection in light of the emerging challenges to survivability posed by UAS, including persistent observation connected to lethal fires.

8) Mind the Human Element

Training of personnel as well as leader development and education are integral aspects of capability integration. To ensure NATO and allied national forces can fully leverage the potential of UAS and C-UAS to contribute to multidomain effects in NATO operations, the alliance and individual allies should ensure training and education of leaders, operators, analysts and support personnel on doctrine, concepts, and standards related to UAS and C-UAS.[351]

Nations acquiring greater numbers and varieties of UAS and C-UAS will automatically expand training and education to meet their needs, but NATO can and should assist with this. NATO assistance can be in the form of policy focus on aspects of training, leader development, and education as well as training and education opportunities at NATO-sponsored or NATO-run courses and NATO training events and exercises. This includes the incorporation of new operational concepts and TTPs related to UAS and C-UAS into relevant training, exercises - be they single component (i.e., single service – army, navy, air force) or joint.

As new capabilities are introduced, new applications or concepts will follow (e.g., for collaborative crewed-uncrewed operations, swarms, cooperative or collaborative groups, and other AI-enabled autonomous functions) with new roles and missions. NATO and allied nations will need to track and share developments to inform training and education in line with doctrine and concept refinement.

Given these considerations, NATO and allied nations should:

- Take a holistic approach to training and educating personnel and leaders on UAS and C-UAS capabilities, doctrine, and concepts;
- Incorporate UAS and C-UAS lessons learned from recent conflict, current UAS and C-UAS capabilities and development trends, and NATO doctrine, concepts, and TTPs (as developed) in appropriate specialist training and leader education (e.g., NATO School Oberammergau, NATO Defense College, NCI Academy, NATO AGS Force, etc.);
- Assign the development of NATO UAS and C-UAS training and education to appropriate NATO institutions and centers of excellence (including, ideally a NATO UAS / C-UAS center of excellence);
- Consider consolidation or federation of specialist training and education for personnel directly involved in UAS and C-UAS operations (e.g., operators, pilots, analysts, UAS force leaders, maintainers and supporters, EW specialists, airspace managers, air traffic controllers);
- Ensure UAS and C-UAS capabilities are regularly integrated into national and NATO training and exercises;
    - Ensure UAS and C-UAS employment in training and exercises incorporates NATO doctrine, concepts, and TTPs, and integrated secure communications networks and data architecture;
    - As appropriate, incorporate federated TCPED, integrated targeting and fire networks, and IAMD concepts in training and exercises involving UAS and C-UAS employment;

Photo: New Jersey Army National Guard soldiers, with the 254th Regimental Training Institute, and Albanian Armed Forces service members work on the setup of Puma AE3 DDL drone at Land Forces Headquarters, Zall-Herr, Tirana, Albania, Dec. 3, 2023.
Credit: 1st Lt. Tyshawn Jenkins/US Air National Guard

    - Ensure EW, cyber, and space capabilities are incorporated in training and exercises (as both enablers and disruptors) involving UAS and C-UAS employment;
- Include UAS and C-UAS employment in senior leader training for military leaders and civilian policy makers (i.e., scenario-based exercises, crisis management exercises);
- Share new national UAS and C-UAS applications and concepts (e.g., for collaborative crewed-uncrewed operations, swarms, cooperative or collaborative groups, other AI-enabled autonomous functions, self-protection systems, directed energy weapons, etc.) across the alliance as they are developed and incorporate them in leader training and education;
- Incorporate outcomes of NATO-led UAS or C-UAS interoperability trials and operational experimentation in briefs to NATO military leaders and civilian policy-makers.

Conclusion

The time for action is now. As the war in Ukraine and other recent conflicts have confirmed, uncrewed aerial systems, and the ability to defend against them, have proven to be essential components of combined arms warfare, multi-domain combat, and national defense capabilities from peacetime to crisis and conflict.

The roles of UAS and C-UAS are poised to expand exponentially in future military operations. This trend is driven by decreasing costs, improved performances in terms of range, endurance, sensors and weapons, improved enabling capabilities related to AI, data and network architecture, cyber, and space, and an unprecedented focus on and support from the private sector.

Increased capabilities are in the field or on the near horizon to enable new applications and missions for UAS, such as teaming up with crewed systems, operating in collaborative groups or swarms, and performing historically crewed air power missions (close air support, armed reconnaissance, interdiction, electronic warfare [EW] attack, suppression of enemy air defenses [SEAD], communications relay, and even resupply and refueling).

The alliance has a rare window of opportunity to capitalize on the present sense of urgency and renewed commitments to defense investment, strengthening deterrence and defense, and innovation to recalibrate its approach to UAS and C-UAS technology.

A recalibrated approach should be comprehensive, incorporating increased UAS and C-UAS capabilities, improved interoperability, new doctrine, and concepts to enable multi-domain operations, a focus on enabling capabilities, leveraging of innovation efforts and advanced technologies, and tailored collective and individual training, and personnel development.

Failure to adapt starting now could prevent rapid response and battlefield success in a future crisis or conflict resulting in lost opportunities, lives, critical equipment, and valuable infrastructure. Seizing the window of opportunity NATO has now would help ensure decisive military advantage and a technological edge for the alliance in the face of future threats and challenges.

Acknowledgements

The authors would like to thank Dr. Amy Nelson, Rubenstein Fellow at The Brookings Institution, Dr. Andrea Gilli, Senior Researcher at the NATO Defense College, and Catherine Sendak, Director of CEPA's Transatlantic Defense and Security (TDS) Program for their invaluable feedback on various drafts of this report. The authors are also grateful to CEPA colleagues who have been instrumental in the publication of this report, in particular Ivanna Kuz, Senior Program Officer with the TDS Program, and Michael Newton, CEPA's Deputy Director for Communications and Operations.

This Report has been kindly supported by Leonardo US Corporation.

All opinions in this publication are those of the authors and do not necessarily represent the position or views of the Center for European Policy Analysis, Leonardo, the US Department of Defense, or NATO.

CEPA is a nonpartisan, nonprofit, public policy institution. All opinions are those of the author(s) and do not necessarily represent the position or views of the institutions they represent or the Center for European Policy Analysis.

About the Authors

Federico Borsari

Federico Borsari is a Leonardo Fellow with the Transatlantic Defense and Security Program at the Center for European Policy Analysis (CEPA). He is also a NATO 2030 Global Fellow and, prior to joining CEPA, he was a Visiting Fellow at the European Council on Foreign Relations (ECFR). His main research interests include security and defense, transatlantic relations, and the impact of new technologies on warfare. He has authored several analyses and publications on defense and security issues, including the use and implications of armed drones in the Middle East and North Africa region.

Gordon B. "Skip" Davis Jr.

Gordon B. "Skip" Davis Jr. is a Non-resident Senior Fellow with the Transatlantic Defense and Security Program at the Center for European Policy Analysis (CEPA). Skip recently served as NATO's Deputy Assistant Secretary General for Defense Investment where he assisted allies in capability development to meet allied and national needs and in policy development related to armaments, aviation, air and missile defense, communications, innovation, technology, interoperability, and industry relations. Skip joined NATO after retiring from the US Army as a Major General with more than 37 years of service. Skip's final assignments included Director of Operations for U.S. European Command, Commanding General of Combined Security Transition Command – Afghanistan, and Director of Operations and Intelligence, Supreme Headquarters Allied Powers Europe.

Skip's military career was characterized by operational and institutional assignments interspersed with study and practice of international affairs and defense issues, primarily in Europe. He speaks French and Italian and has lived over 26 years in Europe. He spent over five years on US, NATO, and United Nations operations across Africa, Iraq, and Afghanistan. While attending graduate school in France as an Olmsted Scholar, Mr. Davis worked as an intern at the Assembly of Western European Union in Paris, later renamed the European Security and Defense Assembly. This experience began a long relationship with NATO and European defense issues, which continued as a common thread through Mr. Davis's post graduate theses and led to numerous assignments with NATO forces and headquarters before joining NATO as a diplomat in 2018.

Endnotes

1 The AGS is a NATO-owned intelligence, surveillance, and reconnaissance capability based on the high-altitude, long-endurance (HALE) class RQ-4D "Phoenix" UAS. There may be a future exception depending on the final solution chosen for the Alliance Future Surveillance and Control (AFSC), but this capability is not foreseen before 2030. See: "Luxembourg to bolster NATO's future surveillance capability development," NATO, March 25, 2022, https://www.nato.int/cps/en/natohq/news_195803.htm.

2 The term "kill chain" as used in this report refers to a military concept which describes the stages or structure of an attack from identification to engagement of a target. See https://en.wikipedia.org/wiki/Kill_chain.

3 David Johnson, "Ending the Ideology of the Offense, Part I and II," War on the Rocks, August 15, 2022, https://warontherocks.com/2022/08/ending-the-ideology-of-the-offense-part-i/.

4 Charles Collins, "Mobilising the British Army," The British Army Review 182 (2023): 8. https://chacr.org.uk/wp-content/uploads/2023/02/BAR_SPR23.pdf.

5 Antonio Calcara, Andrea Gilli, Mauro Gilli, Raffaele Marchetti, and Ivan Zaccagnini. 2022. "Why Drones Have Not Revolutionized War: The Enduring Hider-Finder Competition in Air Warfare." International Security 46 (4): 130–71. https://doi.org/10.1162/isec_a_00431.

6 Ibid.

7 Generally speaking, a nondeterministic algorithm can produce different outputs based on a particular input. Conversely, a deterministic algorithm will always produce the same output for a given input.

8 See, for example: "Strikes against Russian trenches," n.d. X (formerly Twitter). https://twitter.com/PaulJawin/status/1671439656951398400; "The Black Raven group strikes at the Russian infantry in the Kreminna direction," n.d. X (formerly Twitter). https://twitter.com/PaulJawin/status/1671025722478002177; Vasco Cotovio, Frederik Pleitgen, William Bonnett and Daria Markina Tarasova, "'From Ukraine with love:' The elite night-time drone units bombing Russian military," CNN. June 16, 2023, https://www.cnn.com/2023/06/16/europe/ukraine-drone-night-strike-russia-intl-cmd/index.html.

9 Gordon B. "Skip" Davis Jr., "The future of NATO C4ISR: Assessment and recommendations after Madrid," Atlantic Council, March 16, 2023. https://www.atlanticcouncil.org/wp-content/uploads/2023/03/C4ISR-report-v3b.pdf.

10 Authors' written correspondence with Michael Callender, Head, Aerospace Capabilities Section, NATO, July 2023.

11 It is worth noting that most lessons are still preliminary and may change with the evolution of the ongoing war. Equally important, experts, military planners, and decision-makers should resist the temptation to consider these lessons as universal. War is arguably the most non-linear and unpredictable of social phenomena. Each conflict presents specific characteristics that may render some lessons more relevant than others.

12 NATO's UAS Category 2 and 3. See the table at p. 26.

13 The TB2 has been selected by 29 countries, including Azerbaijan, Ethiopia, Libya, Morocco, Nigeria, Pakistan, Poland, Qatar, Romania, and United Arab Emirates, among others. Besides China, Wing Long II operators include Algeria, Morocco, Nigeria, Pakistan, Saudi Arabia. See Stijn Mitzer, Joost Oliemans. "An International Export Success: Global Demand for Bayraktar Drones Reaches All Time High," Oryx. Accessed on September 8, 2023, https://www.oryxspioenkop.com/2021/09/an-international-export-success-global.html.

14 Federico Borsari, "Reflecting on One Year of War: Remotely Piloted Threats, Lessons from Drone Operations in Ukraine," Center for Maritime Strategy, February 8, 2023, https://centerformaritimestrategy.org/publications/reflecting-on-one-year-of-war-remotely-piloted-threats-lessons-from-drone-operations-in-ukraine/.

15 "Bayraktar TB2," Baykar Tech. Accessed on September 8, 2023. https://www.baykartech.com/en/uav/bayraktar-tb2/.

16 Tier 1 TB2s are equipped with Wescam MX-15 suite while Tier 2 TB2s sport the domestically produced Aselsan Common Aperture Targeting System (CATS). See "Bayraktar TB2", Baykar Tech, and Aselsan, "CATS". Accessed on September 8, 2023. https://wwwcdn.aselsan.com/api/file/CATS_ENG%20(1).pdf.

17 According to independent estimates based on open-source data, the TB2 has a median frontal radar cross-section (RCS) of 0.4 Sqm at most common radar frequencies. See: "Bayraktar TB-2 Radar Cross Section Estimates," n.d. X (formerly Twitter). Accessed on September 8, 2023. https://twitter.com/Flankerchan/status/1411986571356635142.

18 Peter W. Mattes, "Systems of Systems: What, Exactly, is an Integrated Air Defense System?," The Mitchell Forum, No. 26, June 2019, https://mitchellaerospacepower.org/wp-content/uploads/2021/02/a2dd91_2f17e209f90f4aaab80b116e4d139eb4.pdf.

19 This had been previously the case in Syria, Libya, and Nagorno-Karabakh.

20 Stijn Mitzer, Joost Oliemans, "A Monument of Victory: The Bayraktar TB2 Kill List," Oryx, February 23, 2022. https://www.oryxspioenkop.com/2021/12/a-monument-of-victory-bayraktar-tb2.html.

21 Mykhaylo Zabrodskyi, Jack Watling, Oleksandr V Danylyuk, Nick Reynolds, "Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February–July 2022, Report," The Royal United Services Institute. November 2022, p 26. https://static.rusi.org/359-SR-Ukraine-Preliminary-Lessons-Feb-July-2022-web-final.pdf.

22 Stijn Mitzer, Joost Oliemans, "Attack on Europe: Documenting Ukrainian Equipment Losses During The 2022 Russian Invasion of Ukraine." Oryx, February 24, 2022. Accessed on March 22, 2023. https://www.oryxspioenkop.com/2022/02/attack-on-europe-documenting-ukrainian.html.

23 "Russian military received the first long-range unmanned complex," Top War, April 2020. https://en.topwar.ru/170430-rossijskie-voennye-poluchili-pervyj-bespilotnyj-kompleks-dalnego-dejstvija.html.

24 Based on open access satellite imagery analyzed by the authors. The Kirovskoe airbase is located at 45.168987, 35.183293.

25 "Iranian UAVs in Ukraine: A Visual Comparison," Defense Intelligence Agency, February 13, 2023, https://www.dia.mil/Portals/110/DIA_Iranian_UAVs_in_Ukraine-A_Visual_Comparison.pdf.

26 Thomas Newdick, Tyler Rogoway, "Russia's Predator-Style Drone with big Export Potential has Launched its First Missiles," The War Zone, December 28, 2020. https://www.thedrive.com/the-war-zone/38446/russias-predator-style-drone-with-big-export-potential-has-launched-its-first-missiles. See also: Said Aminov. "Unmanned aerial vehicles from JSC «Kronstadt». Army-2020," Live Journal, August 25, 2020. https://saidpvo.livejournal.com/979205.html. For the Mohajer-6 see: "The Ukrainians army managed to land Iranian "Mohajer-6." n.d. X (formerly Twitter), October 3, 2022. Accessed on September 8, 2023. https://twitter.com/11Knuk123/status/1576951064913678336.

27 Stijn Mitzer, Joost Oliemans, "Attack on Europe: Documenting Russian Equipment Losses During The 2022 Russian Invasion of Ukraine," Oryx, https://www.oryxspioenkop.com/2022/02/attack-on-europe-documenting-equipment.html. (Accessed on March 22, 2023).

28 Roger McDermott, "Russia's UAVs and UCAVs: ISR and Future Strike Capabilities," Jamestown Foundation. March 23, 2022. https://jamestown.org/program/russias-uavs-and-ucavs-isr-and-future-strike-capabilities/#_ftnref9.

29 Alexander Yermakov, "Unmanned Aerial Vehicles over Nagorno-Karabakh: Revolution or Another Day of Battle," Valdai Discussion Club, December 4, 2020. https://valdaiclub.com/a/highlights/unmanned-aerial-vehicles-over-nagorno-karabakh/?sphrase_id=1476180.

30 Konstantin Makienko quoted in Ray Finch, "Karabakh War Might Spur Russian Attack UAV Development, Operational Environment Watch," Volume 11, Issue 1, January 2021, p. 13. https://community.apan.org/wg/tradoc-g2/fmso/m/oe-watch-past-issues/362218/download.

31 Can Kasapoğlu, "Techno-Geopolitics and the Turkish Way of Drone Warfare," Issue Brief, Atlantic Council, March 2022. https://www.atlanticcouncil.org/wp-content/uploads/2022/03/Techno-Geopolitics_and_the_Turkish_Way_of_Drone_Warfare.pdfhttps://www.atlanticcouncil.org/wp-content/uploads/2022/03/Techno-Geopolitics_and_the_Turkish_Way_of_Drone_Warfare.pdf.

32 "KORAL Land Based Radar Defence Electronic Attack Warfare System," Army Recognition. Accessed on September 8, 2023. https://www.armyrecognition.com/turkey_turkish_field_military_combat_equipment_uk/koral_radar_defence_electronic_attack_warfare_technical_data_sheet_specifications_pictures_video_12402164.html.

33 Feridun Taşda, "Electronic Warfare: Global Trends & Turkish Capabilities Report," SETA Emerging Military Technologies Series 1, 2022, pp. 41-42. https://setav.org/en/assets/uploads/2022/07/EMT-Series-1.pdf.

34 See, among others: John Antal, Seven Seconds to Die. A Military Analysis of the Second Nagorno-Karabakh War and the Future of Warfighting (Philadelphia and Oxford: Casemate, 2022), p. 25; Uzi Rubin, "The Second Nagorno-Karabakh War: A Milestone in Military Affairs," Begin-Sadat Center for Strategic Studies, December 2020, https://besacenter.org/wp-content/uploads/2020/12/184web-no-ital.pdf.

35 Antal, Seven Seconds to Die, 3.

36 Shaan Shaikh, Wes Rumbaugh, "The Air and Missile War in Nagorno-Karabakh: Lessons for the Future of Strike and Defense," Center for Strategic and International Studies (CSIS), December 8, 2020, https://www.csis.org/analysis/air-and-missile-war-nagorno-karabakh-lessons-future-strike-and-defense.

37 Ibid.

38 Scott Crino, Andy Dreby, "Turkey's Drone War in Syria – A Red Team View," Small Wars Journal, April 16, 2020, https://smallwarsjournal.com/jrnl/art/turkeys-drone-war-syria-red-team-view.

39 Stijn Mitzer, Joost Oliemans, "Tracking Worldwide Losses of Chinese-Made UAVs," Oryx. Accessed on September 8, 2023. https://www.oryxspioenkop.com/2021/11/tracking-worldwide-losses-of-chinese.html. For the TB2 losses, see: Pack, Pusztai, "Turning the Tide;" Drone Wars, "Drone Crash Database." Accessed on March 22, 2023. https://dronewars.net/drone-crash-database/.

40 Rosoboronexport Catalog, ""Pantsir-S1» Anti-aircraft missile and gun system." Accessed on September 8, 2023. https://roe.ru/eng/catalog/air-defence-systems/air-defense-systems-and-mounts/%22Pantsir-S1%22/; "Clash Report released another video of a Turkish TB2 UCAV strike on an Emirati Pantsir-S1," n.d. X (formerly Twitter), May 20, 2020. https://twitter.com/RALee85/status/1263104642315104256.

41 See: "#Libya- #Italy losses MQ-9 Reaper/Predator B UAV over #Tarhunah in #LNA territory," n.d. X (formerly Twitter), November 21, 2019. https://twitter.com/Oded121351/status/1197436033450811392; "Earlier today, an MQ-9 was shot down near Al-Maqzha just outside of Benghazi," Libya, n.d. X (formerly Twitter), August 22, 2022, https://twitter.com/ameliairheart/status/1561853826650587136.

42 John Reed, "Predator Drones 'Useless' in Most Wars, Top Air Force General Says," Foreign Policy, September 19, 2013. https://foreignpolicy.com/2013/09/19/predator-drones-useless-in-most-wars-top-air-force-general-says/.

43 See: Don Rassler, "The Islamic State and Drones: Supply, Scale, and Future Threats," Combating Terrorism Center (CTC), July 2018. https://ctc.usma.edu/wp-content/uploads/2018/07/Islamic-State-and-Drones-Release-Version.pdf; "#Turkey: #PKK/#HPG released the footage of their drone attack on #TAF/#TSK base on April," n.d. X (formerly Twitter), April 30, 2021. https://twitter.com/war_noir/status/1388091654050099200.

44 Thomas Newdick, "Bomblet Dropping Drones are Now Being Used by Cartels in Mexico's Drug War," The War Zone, January 12, 2022. https://www.thedrive.com/the-war-zone/43847/bomblet-dropping-drones-are-now-being-used-by-cartels-in-mexicos-drug-war.

45 See, for example: "#Ukraine: In #Donetsk Oblast, two more Russian T-72/T-80 tanks were destroyed by the SBU "Alpha" SSO using drone-dropped munitions based on PG-7L HEAT RPG projectiles," n.d. X (formerly Twitter), March 23, 2023. https://twitter.com/UAWeapons/status/1638858332462018561; "#Ukraine: A Russian MT-LB carrying 100mm ammunition for the MT-12 Rapira AT gun was destroyed by the Ukrainian 59th Brigade," n.d. X (formerly Twitter), March 11, 2023. https://twitter.com/UAWeapons/status/1634593353303052288;

46 "A Russian improvised FPV loitering munition with a MON-50 mine," n.d. X (formerly Twitter), March 21, 2023. https://twitter.com/RALee85/status/1638197498085875715.

47 "How could FPV drones change warfare?," The Economist, August 4, 2023, https://www.economist.com/the-economist-explains/2023/08/04/how-could-fpv-drones-change-warfare.

48 Alex Roslin, "Wild Hornets: Ukraine's Tiny Armor-Busting, Trench-Clearing Secret Weapon," Kyiv Post, July 8, 2023, https://www.kyivpost.com/post/19227.

49 See, among others, "Soldiers of the 74th reconnaissance battalion destroy the Russian Fagot ATGM using an FPV drone," n.d. X (formerly Twitter), July 15, 2023. https://twitter.com/PaulJawin/status/1680188357341528064; "FPV drone hit the Russian APC," n.d. X (formerly Twitter), July 13, 2023. https://twitter.com/PaulJawin/status/1679421392637374469.

50 Alia Shoaib, "A video shows an advanced Russian T-90 tank destroyed by a $500 hobby drone fitted with explosives, says Ukraine military," Business Insider, August 13, 2023, https://www.businessinsider.com/video-russian-t-90-tank-destroyed-by-cheap-hobby-drone-2023-8.

51 See, for example, "Ukrainian FPV kamikaze drones attack Russian military equipment," n.d. X (formerly Twitter), July 13, 2023. https://twitter.com/front_ukrainian/status/1679395403077148673; "Kreminna direction. Russian tank hit by FPV drone of the 23rd battalion," n.d. X (formerly Twitter), July 13, 2023. https://twitter.com/PaulJawin/status/1679564336312770560;

52 "Ukraine is Now Using AI-Powered Drones With Some Amazing Capabilities," Kyiv Post, September 4, 2023, https://www.kyivpost.com/post/21247.

53 "This is another Russian assembly shop for FPV drones," n.d. X (formerly Twitter), May 7, 2023. https://twitter.com/sambendett/status/1655177496269135872.

54 "Putin wants «mass production» of drones in Russia," Yahoo News, April 27, 2023, https://news.yahoo.com/putin-wants-mass-production-drones-212934678.html.

55 Missy Ryan, Isabelle Khurshudyan, Michael Birnbaum, "Ukraine aims to sap Russia's defenses, as U.S. urges a decisive breakthrough", The Washington Post, July 18, 2023, https://www.washingtonpost.com/national-security/2023/07/18/ukraine-counter-offensive-weapons-tactics/.

56 Zabrodskyi, Watling, Danylyuk, Reynolds, "Preliminary Lessons in Conventional Warfighting," 37.

57 "Shark UAS," Ukrspec Systems, https://ukrspecsystems.com/drones/shark-uas.

58 Alia Shoab, "Ukraine's army is using a nimble 'game-changing' drone called The Punisher that has completed scores of successful missions against the Russians, say reports," Business Insider, March 5, 2023, https://www.businessinsider.com/ukraines-punisher-drones-hit-russian-troops-multiple-times-reports-2022-3?r=US&IR=T.

59 "Russia to launch mass production of effective drones — Medvedev," Tass, October 14, 2022, https://tass.com/defense/1523079.

60 James Byrne, et al., The Orlan Complex. Tracking the supply chains of Russia's most successful UAV, RUSI, December 2022, https://static.rusi.org/SR-Orlan-complex-web-final.pdf.

61 "The Ministry of Defense of Ukraine ordered 105 Vector UAVs in Germany," Ukraine's Ministry of Defense, January 29, 2023, https://mil.in.ua/en/news/the-ministry-of-defense-of-ukraine-ordered-105-vector-uavs-in-germany/.

62 See, for instance: John Wendle, "The Fighting Drones of Ukraine," Smithsonian Magazine, February 2018. https://www.smithsonianmag.com/air-space-magazine/ukraines-drones-180967708/.

63 Greg Myre, "How Ukraine created an 'Army of Drones' to take on Russia," NPR, June 20, 2023, https://www.npr.org/2023/06/20/1183050117/how-ukraine-created-an-army-of-drones-to-take-on-russia.

64 Hanna Shelest, "Defend. Resist. Repeat: Ukraine's lessons for European defence," Policy Brief, European Council on Foreign Relations, November 2022, https://ecfr.eu/wp-content/uploads/2022/11/Defend.-Resist.-Repeat-Ukraines-lessons-for-European-defence.pdf.

65 Anita Hawser, "Ukraine's Drone Wars," Defence Procurement International, January 19, 2023, https://www.defenceprocurementinternational.com/features/air/the-start-ups-helping-ukraine-win-the-drone-war-with-russia.

66 Aerorozvidka website. https://aerorozvidka.ngo/.

67 Veronika Melkozerova, "Ukraine's Drone Academy is in session," Politico, February 26, 2023, https://www.politico.eu/article/ukraine-drone-academy-war-russia-kyiv-pilot/.

68 "Ukraine is betting on drones to strike deep into Russia," The Economist, March 2023, https://www.economist.com/europe/2023/03/20/ukraine-is-betting-on-drones-to-strike-deep-into-russia.

69 Ibid.

70 Jaroslaw Adamowski, "Ukraine plans to spend $540 million on drones this year," Defense News, February 1, 2023, https://www.defensenews.com/unmanned/2023/02/01/ukraine-plans-to-spend-540-million-on-drones-this-year/.

71 "Russian soldier with a DJI Matrice 300 UAV with a RKG-3EM anti-tank grenade," n.d. X (formerly Twitter), October 13, 2022. https://twitter.com/search?q=Russian%20soldier%20%20DJI%20&src=typed_query&f=image; Benoit Faucon, Ian Talley, "Chinese Drones Still Support Russia's War in Ukraine, Trade Data Show," Wall Street Journal, February 18, 2023, https://www.wsj.com/articles/chinese-drones-still-support-russias-war-in-ukraine-trade-data-show-cd39d40b; Hana Moumen, "Commercial Drone Tech Proliferates in Ukraine," National Defense Magazine, September 7, 2022, https://www.nationaldefensemagazine.org/articles/2022/9/7/commercial-drone-tech-proliferates-in-ukraine.

72 "Russia Faces Commercial Drone Shortage as War Increases Demand," The Moscow Time, June 15, 2022, https://www.themoscowtimes.com/2022/06/15/russia-faces-commercial-drone-shortage-as-war-increases-demand-a78004.

73 Samuel Bendett, "The Ukraine war and its impact on Russian development of autonomous weapons," Atlantic Council, August 30, 2022, https://www.atlanticcouncil.org/content-series/airpower-after-ukraine/the-ukraine-war-and-its-impact-on-russian-development-of-autonomous-weapons/. "Small-size recon drones arrive for Russian troops in Ukraine special operation zone," Tass, January 3, 2023. https://tass.com/russia/1558687.

74 "1/ Pro-Kremlin Telegram on the importance of FPV drones and the current command structure," n.d. X (formerly Twitter), March 24, 2022, https://twitter.com/sambendett/status/1639328939171512330.

75 Authors' assessment based on reviewed open-source information. See, among others: "The DPR "Sparta" battalion uses a DJI Mavic Enterprise drone with a thermal sensor," n.d. X (formerly Twitter), November 23, 2022, https://twitter.com/faineg/status/1595501071090257926; "Sparta battalion drop munitions," n.d. X (formerly Twitter), September 5, 2022, https://twitter.com/200_zoka/status/1566760341291368448.

76 Xiao Liang, Diego Lopes da Silva, Nan Tian, Lucie Béraud-Sudreau, Alexandra Marksteiner, "Trends in World Military Expenditure, 2021," Stockholm International Peace Research Institute (SIPRI), https://www.sipri.org/sites/default/files/2022-04/fs_2204_milex_2021_0.pdf.

77 Morgan Meaker, "High Above Ukraine, Satellites Get Embroiled in the War," Wired, April 3, 2022, https://www.wired.co.uk/article/ukraine-russia-satellites.

78 Rachel Lerman, "On Google Maps, tracking the invasion of Ukraine," The Washington Post, February 27, 2022, https://www.washingtonpost.com/technology/2022/02/25/google-maps-ukraine-invasion/.

79 Christopher Miller, Mark Scott, Bryan Bender, "UkraineX: How Elon Musk's space satellites changed the war on the ground," Politico, June 8 2022, https://www.politico.eu/article/elon-musk-ukraine-starlink/.

80 Chris Panella, "Starlink is key to Ukrainian operations, but the Russians 'will find you' if you use it too long, soldier says," Business Insider, March 24, 2023, https://www.businessinsider.com/starlink-key-ukrainian-operations-used-too-long-russians-will-find-2023-3?r=US&IR=T.

81 "Ukraine unveiled its own Delta situational awareness system," Ukrainian Military Center, October 27, 2022, https://mil.in.ua/en/news/ukraine-unveiled-its-own-delta-situational-awareness-system/. See also: "War in Ukraine: An advanced digital map. The Delta system," United24, YouTube, December 9, 2022, https://www.youtube.com/watch?v=rqzIUtJcZBs.

82 Tom Cooper, "Kropyva: Ukrainian Artillery Application," Medium, June 10, 2022, https://medium.com/@x_TomCooper_x/kropyva-ukrainian-artillery-application-e5c6161b6c0a#id_token; Mark Bruno, "'Uber For Artillery' – What is Ukraine's GIS Arta System?," The Moloch, August 24, 2022. https://themoloch.com/conflict/uber-for-artillery-what-is-ukraines-gis-arta-system/.

83 Ibid; "Defense Mapping Software," Army SOS, https://armysos.com.ua/defense-mapping-software/.

84 John Hudson, Kostiantyn Khudov, "The war in Ukraine is spurring a revolution in drone warfare using AI," The Washington Post, July 26, 2023, https://www.washingtonpost.com/world/2023/07/26/drones-ai-ukraine-war-innovation/.

85 Ibid.

86 both produced by Zala Aero Group.

87 "Lancet 3," Zala Aero Group, https://zala-aero.com/en/production/bvs/zala-lancet-3/.

88 See, for example: "3 attacks by Russian "Lancet"-series kamikaze drones against Ukrainian targets," n.d. X (formerly Twitter), March 24, 2023, https://twitter.com/imp_navigator/status/1639158493696458753.

89 "Russian forces operating Lancet kamikaze UAVs in Ukraine," n.d. X (formerly Twitter), https://twitter.com/clashreport/status/1634871266325700610.

90 Lancet 3, Zala Aero Group.

91 According to open-source analyses, the median Shahed-136's frontal RCS is around 0.01 Sqm between 2 and 36 Ghz frequencies. See, for instance, "So Russians using something like Shahed-136," n.d. X (formerly Twitter), September 19, 2022, https://twitter.com/Flankerchan/status/1572046686138302465. The range is estimated at 900 km for the Shahed-131 and between 1,000 and 1,500 km for the Shahed-136.

92 "IRN-05 (Shahed-131) UAV Technical Report" (Ukrainian), Ukraine Armed Forces Strategic Command, September 2023, https://t.me/AFUStratCom/7010. (Translated with Deepl Translator).

93 "Documenting Russia's advanced weapon systems in Ukraine," Ukraine Field Dispatch, May 2022, Conflict Armament Research, https://storymaps.arcgis.com/stories/19ca0782f2354c87b25972da7356f0e8.

94 "Dissecting Iranian drones employed by Russia in Ukraine," Ukraine field dispatch, Conflict Armament Research, November 2022, https://storymaps.arcgis.com/stories/7a394153c87947d8a602c3927609f572.

95 Maksim Panasovskyi, "Russia's Lancet kamikaze drone is equipped with an NVIDIA Jetson TX2 computer and an Xilinx Zynq chip," Gagadget, March 20, 2023, https://gagadget.com/en/226952-russias-lancet-kamikaze-drone-is-equipped-with-an-nvidia-jetson-tx2-computer-and-an-xilinx-zynq-chip/; "Jetson TX2," Edge Computing, Nvidia, https://www.nvidia.com/en-us/autonomous-machines/embedded-systems/jetson-tx2/.

96 For the exhaustive list of US-made loitering munitions provided to Ukraine see: "Fact Sheet on US Security Assistance to Ukraine," May 3, 2023, https://media.defense.gov/2023/May/03/2003214586/-1/-1/1/UKRAINE-FACT-SHEET-MAY-3.PDF; "Switchblade 300 in service of the Ukrainian SOF," n.d. X (formerly Twitter), March 30, 2023, https://twitter.com/TheDeadDistrict/status/1641349492141174784; "The first appearance of the Polish WARMATE loitering munition armed with a HE-FRAG warhead being used by the Ukrainian forces," n.d. X (formerly Twitter), April 24, 2022, https://twitter.com/UAWeapons/status/1518284891766636546.

97 "RAM II UAV," CDET LLC, https://ramuav.com/.

98 See: "The SBU "Alpha" SSO destroyed a Russian 9A331M TLAR of the Tor-M2 air defence system using a Ukrainian-made RAM II loitering munition," n.d. X (formerly Twitter), March 28, 2023, https://twitter.com/UAWeapons/status/1640639342279262208; "Video of Ukrainian SBU Alpha loitering munition strikes (including RAM II) on Russian Tor-M2 9A331M TLARs and a S-300V -series 9A83 -series TELAR," n.d. X (formerly Twitter), March 18, 2023. https://twitter.com/RALee85/status/1637245165529120770.

99 Stephen Kalin, Sylvia Westall, "Costly Saudi defenses prove no match for drones, cruise missiles," Reuters, September 17, 2019, https://www.reuters.com/article/us-saudi-aramco-security-idUKKBN1W22FR.

100 Joseph Trevithick, "Massive Drone Swarm Over Strait Decisive in Taiwan Conflict Wargames," The War Zone, May 19, 2022. https://www.thedrive.com/the-war-zone/massive-drone-swarm-over-strait-decisive-in-taiwan-conflict-wargames.

101 NATO C-UAS Expert, NATO Emerging Security Challenges Division (ESCD), Interview by authors, January 19, 2023.

102 According to independent estimates based on open-source data. See: "Iranian drones in the Russian invasion: analysis by Molfar experts," Molfar, October 18, 2022, https://www.molfar.global/en-blog/shahed.

103 Alia Shoaib, "How Ukraine uses high-tech anti-drone guns to down Russian drones and recover intelligence from them," Business Insider, February 18, 2023, https://www.businessinsider.com/ukraines-anti-drone-guns-down-russian-drones-recover-intelligence-2023-2.

104 See, for example: "#Ukraine: Rare footage from the Ukrainian 28th Mechanized Brigade in the area of #Bakhmut, showing a Russian Lancet loitering munition taken down by very manual means-small arms and ZU-23-2 autocannon fire," n.d. X (formerly Twitter), January 15, 2022, https://twitter.com/UAWeapons/status/1614581629372039169;

105 See, for example: "Well, it really works," n.d. X (formerly Twitter), January 22, 2022, https://twitter.com/OSINTua/status/1617152860940107776; "#Ukraine: A rare look at a failed Russian attack on an T-72 tank by two Lancet loitering munitions," n.d. X (formerly Twitter), December 23, 2022, https://twitter.com/UAWeapons/status/1606427763895943169.

106 Euronews, "Is Ukraine tricking Russia on the battlefield with inflatable decoy tanks and weapons?," March 7, 2023, https://www.euronews.com/next/2023/03/07/is-ukraine-tricking-russia-on-the-battlefield-with-inflatable-decoy-tanks-and-weapons.

107 David Axe, "Russia's Electronic-Warfare Troops Knocked Out 90 Percent Of Ukraine's Drones," Forbes, December 24, 2022, https://www.forbes.com/sites/davidaxe/2022/12/24/russia-electronic-warfare-troops-knocked-out-90-percent-of-ukraines-drones/?sh=389ea582575c.

108 Zabrodskyi, Watling, Danylyuk, Reynolds, "Preliminary Lessons in Conventional Warfighting," p. 37.

109 Jack Watling, Nick Reynolds, "Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine," Royal United Service Institute, May 19, 2023, p. 18. https://static.rusi.org/403-SR-Russian-Tactics-web-final.pdf.

110 Emma Helfrich, "Our Best Look At Ukraine's Shadowy 'Alibaba Drone' Used For Long-Range Strikes," The War Zone, March 2, 2023, https://www.thedrive.com/the-war-zone/our-best-look-at-ukraines-shadowy-alibaba-drone-used-for-long-range-strikes.

111 Thomas Withington, "Russia's Electronic Warfare Capabilities Have Had Mixed Results Against Ukraine," The War Zone, June 16, 2022, https://www.thedrive.com/the-war-zone/this-is-whats-happened-so-far-in-ukraines-electronic-warfare-battle.

112 Noel, "Andriy Matsola showed a new 'Spire' drone that is able to knock down Shahed-drones and is able to destroy other equipment," Twitter, February 23, 2023, https://twitter.com/NOELreports/status/1623620943439339520.

113 "Collaborative Air Combat Autonomy Program Makes Strides," DARPA, March 18, 2021, https://www.darpa.mil/news-events/2021-03-18a; Col Paul J. Calhoun, "LongShot," DARPA, accessed May 20, 2023; https://www.darpa.mil/program/longshot; LtCol Ryan Hefron, "Air Combat Evolution," DARPA, accessed May 20, 2023, https://www.darpa.mil/program/air-combat-evolution.

114 Thomas Newdick, Tyler Rogoway, "Marine XQ-58 Valkyries Will Be Electronic Warfare Platforms For F-35s," The War Zone, May 4, 2023, https://www.thedrive.com/the-war-zone/marine-xq-58-valkyries-will-be-electronic-warfare-platforms-for-f-35.

115 The AGS is a NATO-owned intelligence, surveillance, and reconnaissance capability based on the high-altitude, long-endurance (HALE) class RQ-4D "Phoenix" UAS. There may be a future exception depending on the final solution chosen for the Alliance Future Surveillance and Control (AFSC), but this capability is not foreseen before 2030. See: NATO, "Luxembourg to bolster NATO's future surveillance capability development," NATO, March 25, 2022, https://www.nato.int/cps/en/natohq/news_195803.htm.

116 David Cattler, NATO's Assistant Secretary General for Intelligence and Security, interview by authors, January 13, 2023.

117 Tom Goffus, Assistant Secretary General for Operations, NATO, interview by authors, January 11, 2023.

118 Ross McKenzie, Michael Callender, interview by authors.

119 LTC Roberto Patti, "Joint Operations with Unmanned Aircraft Systems (UAS) and their Future Development," NATO Combined Joint Operations from the Sea Centre of Excellence, 2021, p. 17, http://www.cjoscoe.org/infosite/wp-content/uploads/2021/01/Joint-Operations-with-Unmanned-Aircraft-Systems-and-their-Future-Development.pdf.

120 "Alliance Ground Surveillance (AGS)," NATO, https://www.nato.int/cps/en/natohq/topics_48892.htm.

121 The 15 countries included: Denmark, Germany, Luxembourg, Latvia, Norway, the US, Romania, Slovakia, Estonia, Poland, Bulgaria, the Czech Republic, Lithuania, and Slovenia.

122 [115] "Alliance Ground Surveillance (AGS)."

123 US Air Force Brigadier General Andrew Clark, NATO AGS Force Commander, Interview by authors, February 2023.

124 Ibid.

125 Ibid.

126 PED is part of the broader Tasking, Collection, Processing, Exploitation, and Dissemination (TCPED) process.

127 Brig. Gen. A. Clark, NATO AGS Force Commander, Interview by authors.

128 Allan McLeod, Director of Life Cycle Management, NATO Support and Procurement Agency (NSPA) and Doug Heintz, Programme Manager of the NSPA AGS and UAS program, interview by authors, May 2023.

129 NATO AGS Force Commander, Interview by authors.

130 Ibid.

131 Ibid.

132 Ibid.

133 Ibid.

134 Allan McLeod and Doug Heintz, interview by authors.

135 "Contracts For Sept. 2, 2022," US Department of Defense, https://www.defense.gov/News/Contracts/Contract/Article/3148681/#:~:text=August%2031%2C%202022)-,AIR%20FORCE,-Northrop%20Grumman%20Systems.

136 Allan McLeod and Doug Heintz, interview by authors.

137 NATO AGS Force Commander, Interview by authors.

138 John A. Tirpak, "Secret Global Hawk Successor Due in 2027-2029," Air and Space Forces Magazine, July 22, 2021, https://www.airandspaceforces.com/secret-global-hawk-successor-due-in-2027-2029/.

139 Jim Garamone, "Iran Shoots Down US Global Hawk Operating in International Airspace," US Department of Defense, June 20, 2019. https://www.defense.gov/News/News-Stories/Article/Article/1882497/iran-shoots-down-us-global-hawk-operating-in-international-airspace/.

140 Statement of Gen. Charles Q. Brown, Jr., "Department of the Air Force Posture Statement Fiscal Year 2022," Department of the Air Force Presentation to the Committees And Subcommittees of the United States Senate And the House of Representatives, 1st Session, 117th Congress, May 7, 2021, https://docs.house.gov/meetings/AP/AP02/20210507/112533/HHRG-117-AP02-Wstate-BrownC-20210507.pdf.

141 Ross McKenzie and Michael Callender, interview by authors.

142 NATO Countries operating MALE UAS: France, Germany, Greece, Italy, the Netherlands, Poland, Spain, Turkey, the UK, and the US. The NATO members currently operating the MQ-9 are France, Italy, the Netherlands, Poland, Spain, the UK, and the US. Belgium and Greece are prospective MQ-9B operators.

143 Ronald Watkins, "Czech Republic to Purchase Three Heron Drones From Israel," The Defense Post, August 9, 2022, https://www.thedefensepost.com/2022/08/09/czech-heron-drones-israel/.

144 Clement Charpentreau, "Turkey's Baykar Technologies unveils new images of Bayraktar TB3 combat drone," Aero Time Hub, March 27, 2023, https://www.aerotime.aero/articles/turkeys-baykar-technologies-unveils-new-images-of-bayraktar-tb3-combat-drone.

145 Burak Ege Bekdil, "The operational — and political — benefits of Turkey's new warship," Defense News, May 3, 2023, https://www.defensenews.com/naval/2023/05/03/the-operational-and-political-benefits-of-turkeys-new-warship/.

146 The upgraded version is the MQ-9B Sky Guardian. Representative from General Atomics Aeronautical Systems, interview by authors, March 2023.

147 Burak Ege Bekdil, "Albania orders three armed TB2 drones," Defense News, December 22, 2022, https://www.defensenews.com/unmanned/2022/12/22/albania-orders-three-armed-tb2-drones/; "Romania to buy drones from Turkey's Baykar as part of military endowment," Reuters, September 1, 2022, https://www.reuters.com/world/europe/romania-buy-drones-turkeys-baykar-part-military-endowment-2022-09-01/.

148 See: Gareth Jennings, "Slovakia considers Bayraktar buy from Turkey," Janes, April 13, 2022, https://www.janes.com/defence-news/news-detail/slovakia-considers-bayraktar-buy-from-turkey; Yusuf Çetiner, "Portugal in Talks with Turkish Drone Manufacturer Baykar for the Purchase of UAVs," Overt Defense, February 2, 2023, https://www.overtdefense.com/2023/02/02/portugal-in-talks-with-turkish-drone-manufacturer-baykar-for-the-purchase-of-uavs/; "The government is considering the purchase of brutally effective Bayraktar combat drones" (translated from Hungarian), Index, August 19, 2022, https://index.hu/belfold/2022/08/19/palkovics-laszlo-torokorszag-dron-bayraktar-magyar-kormany-technologiai-es-ipari-miniszterium.

149 Victor Barreira, "France to receive long-awaited Patroller UAVs," Janes, October 4, 2022, https://www.janes.com/defence-news/news-detail/france-to-receive-long-awaited-patroller-uavs.

150 Allan McLeod and Doug Heintz, interview by authors.

151 Ibid.

152 "Eurodrone," Airbus Defence, https://www.airbus.com/en/defence/eurodrone.

153 David Cattler, interview by authors.

154 Jaroslaw Adamowski, "Poland leases MQ-9A Reapers ahead of drone buy," Defense News, October 21, 2022, https://www.defensenews.com/global/europe/2022/10/21/poland-leases-mq-9a-reapers-ahead-of-drone-buy/.

155 Representative from General Atomics Aeronautical Systems, interview by authors.

156 Tyler Rogoway, "MQ-9 Reaper Is Capable Of Defending Itself With Air-To-Air Missiles," The War Zone, March 14, 2023, https://www.thedrive.com/the-war-zone/yes-the-mq-9-can-defend-itself-with-air-to-air-missiles; "Turkish defense industry eyes new air-to-air missiles for Akıncı UCAV," Daily Sabah, June 7, 2022, https://www.dailysabah.com/business/defense/turkish-defense-industry-eyes-new-air-to-air-missiles-for-akinci-ucav.

157 NSPA LQ Project Manager for AGS and UAS Doug Heintz, interview by authors.

158 Ibid.

159 At least 9 countries are known to operate the Black Hornet UAS: France, Germany, The Netherlands, Norway, Poland, Spain, Türkiye, the UK, and the US. See: "Black Hornet PRS," Teledyne FLIR, https://www.flir.com/products/black-hornet-prs/.

160 Overall, based on publicly available information, it remains difficult to assess the precise number of medium and small UAS in service and their distribution among the forces of single NATO countries.

161 Elise Vincent, "Kamikaze drones to make French army debut," Le Monde, March 25, 2023. https://www.lemonde.fr/en/france/article/2023/03/25/kamikaze-drones-to-make-french-army-debut_6020633_7.html.

162 Elisabeth Gosselin-Malo, "Documents reveal secret customer of Hero-30 kamikaze drones," January 23, 2023, https://www.defensenews.com/unmanned/2023/01/23/documents-reveal-secret-customer-of-hero-30-kamikaze-drones/.

163 "Estonia to order munitions in one of its largest military purchases," Reuters, February 18, 2023, https://www.reuters.com/world/europe/estonia-order-munitions-one-its-largest-military-purchases-2023-02-18/; Rojoef Manuel, "Lithuania Procures Switchblade Kamikaze Drones From US," The Defense Post, December 26, 2022, https://www.thedefensepost.com/2022/12/26/lithuania-switchblade-drones/.

164 On the cost comparison see, for example: "Usage Patterns and Costs of Unmanned Aerial Systems," Congressional Budget Office, June 2021, https://www.cbo.gov/file-download/download/private/162376; Todd Harrison, "Rethinking the Role of Remotely Crewed Systems in the Future Force," CSIS Brief, Center for Strategic and International Studies (CSIS), March 3, 2021, https://www.csis.org/analysis/rethinking-role-remotely-crewed-systems-future-force.

165 Belgium, Bulgaria, Canada, Denmark, France, Germany, Greece, Italy, the Netherlands, Norway, Poland, Portugal, Spain, Türkiye, the United Kingdom, and the United States – and NATO partner Australia. See: "Maritime Unmanned Systems (MUS) High Visibility Project," Factsheet, August 2022, NATO, https://www.nato.int/nato_static_fl2014/assets/pdf/2022/9/pdf/2209-factsheet-mus.pdf.

166 "NATO exercises with new maritime unmanned systems," NATO, September 15, 2022, https://www.nato.int/cps/en/natohq/news_207293.htm.

167 Ibid.

168 Ibid.

169 Authors' written correspondence with Catherine Warner, Director of NATO's Centre for Maritime Research and Experimentation (CMRE), March 2023.

170 Lee Willet, "Accelerating Advantage: NATO's DIANA Programme Picks up Speed in Harnessing Technological Innovation," European Security and Defense, April 20, 2023, https://euro-sd.com/2023/04/articles/30763/accelerating-advantage-natos-diana-programme-picks-up-speed-in-harnessing-technological-innovation/.

171 Authors' written correspondence with Catherine Warner.

172 Ibid.

173 "Thales and Schiebel Validate the Use of Schiebel's Camcopter S-100 Unmanned Air Vehicle (Uav) to Relay Acoustic Buoy Surveillance During the Nato Exercise Repmus 2022," Thales, https://www.thalesgroup.com/en/worldwide/defence/news/thales-and-schiebel-validate-use-schiebels-camcopterr-s-100-unmanned-airhttps://www.thalesgroup.com/en/worldwide/defence/news/thales-and-schiebel-validate-use-schiebels-camcopterr-s-100-unmanned-air.

174 William A. Perkins, "Unmanned Air Systems in NATO Anti-Submarine Warfare (ASW)," Transforming Joint Air Power, Joint Air Power Competence Centre, Ed. 25, Winter 2017/2018, pp. 27-33. https://www.japcc.org/wp-content/uploads/JAPCC_J25_screen.pdfhttps://www.japcc.org/wp-content/uploads/JAPCC_J25_screen.pdf.

175 Steven Horrell, Senior Fellow, Center for European Policy Analysis, interview by authors, March 2023.

176 The Royal Navy tested the Malloy Aeronautics' T-600 quadcopter and the Ultra drone produced by Windracers Autonomous Systems. After recent demonstrations, the US Marine Corp purchased TRV-150C drones for tactical resupply. See, respectively: "Drones deliver in trials by Royal Navy," News, Royal Navy, April 6, 2022. https://www.royalnavy.mod.uk/news-and-latest-activity/news/2022/april/06/220406-heavy-lift-challengehttps://www.royalnavy.mod.uk/news-and-latest-activity/news/2022/april/06/220406-heavy-lift-challenge; Jon Harper, "DOD announces purchase of 21 tactical resupply drones following Marine Corps demonstration," Defensescoop, April 12, 2023, https://defensescoop.com/2023/04/12/dod-announces-purchase-of-21-tactical-resupply-drones-following-marine-corps-demonstration/.

177 "MQ-25," Boeing, https://www.boeing.com/defense/mq25/https://www.boeing.com/defense/mq25/.

178 Xavier Vavasseur, "Video: SMDM – The New Fixed-Wing UAS Of The French Navy," Naval News, October 3, 2022, https://www.navalnews.com/event-news/euronaval-2022/2022/10/video-smdm-the-new-fixed-wing-uas-of-the-french-navy/.

179 Xavier Vavasseur, "VSR-700 VTOL UAV Successfully Tested Over Water," Naval News, February 1, 2023, https://www.navalnews.com/naval-news/2023/02/vsr-700-vtol-uav-successfully-tested-over-water/.

180 Tayfun Ozberk, "Turkish Navy Accepts Delivery of its Flagship, TCG ANADOLU," Naval News, March 7, 2023, https://www.navalnews.com/naval-news/2023/03/turkish-navy-accepts-delivery-of-its-flagship-tcg-anadolu/.

181 "Bayraktar TB3," Baykar, https://baykartech.com/en/bayraktar-tb3/.

182 "Thales and Schiebel to Deliver Innovative Eyes in the Sky Protection for Royal Navy Using Uncrewed Rotary Aircraft Solution," Press Release, Thales, February 10, 2023, https://www.thalesgroup.com/sites/default/files/prezly/documents/Thales%20and%20Schiebel%20to%20deliver%20innovative%20eyes%20in%20the%20sky%20protection%20for%20Royal%20Navy%20using%20uncrewed%20rotary%20aircraft%20solution.pdf.

183 George Hallison, "British aircraft carrier to trial 'Project Mojave' drones," UK Defence Journal, May 19, 2023, https://ukdefencejournal.org.uk/british-aircraft-carrier-to-trial-variant-of-reaper-drones/.

184 "Documento Programmatico Pluriennale della Difesa per il Triennio 2022-2024," Ministero della Difesa, 2022, https://www.difesa.it/Il_Ministro/Documents/DPP_2022_2024.pdfhttps://www.difesa.it/Il_Ministro/Documents/DPP_2022_2024.pdf.

185 "Piano Nazionale della Ricerca Militare 2022 - Proposta n. a2021.047 dal titolo "SCIAMANO - Progettazione concettuale della nave porta droni." Fase 1 di 2." Ministero della Difesa, Segretariato Generale della Difesa, Direzione Nazionale degli Armamenti, https://www.difesa.it/Amministrazionetrasparente/segredifesa/navarm/Documents/2Reparto4divisione/Relazioni_preliminari/2022/Relazione%20Preliminare_SCIAMANO_SP_Firmato.pdf.

186 Steven Horrell, interview by authors; Official of the Romanian Armed Forces, CEPA private discussion with a delegation of the Ministry of Defense of Romania, March 2023.

187 NATO formally recognized cyberspace and space as operational domains in 2016 and 2019 respectively.

188 On the commonalities between space and cyberspace see: Clémence Poirier, "The war in Ukraine from a space cybersecurity perspective," ESPI Report 84, European Space Policy Institute (ESPI), October 2022, https://www.espi.or.at/wp-content/uploads/2022/10/ESPI-Report-84.pdf.

189 "Ten Years Ago Iran Commandeered America's Stealthiest Aircraft: The Greatest US Tech Loss Since the Cold War?," Military Watch Magazine, December 6, 2021, https://militarywatchmagazine.com/article/iran-hacked-stealthiest-aircraft-RQ170-setback.

190 Mike Mount, Elaine Quijano, "Iraqi insurgents hacked Predator drone feeds, US official indicates," CNN, December 18, 2009, http://edition.cnn.com/2009/US/12/17/drone.video.hacked/.

191 "NATO's approach to space," NATO, February 16, 2023, https://www.nato.int/cps/en/natohq/topics_175419.htm.

192 NATO ASG for Intelligence David Cattler, interview by authors.

193 Ibid.

194 Kevin Pollpeter, Elizabeth Barrett, "NATO Ally Contributions to the Space Domain," China Aerospace Studies Institute, October 2021, https://www.airuniversity.af.edu/Portals/10/CASI/documents/Research/Space/2021-10-18%20NATO%20allies%20contributions.pdf?ver=iojEUw0U2tOyGD82QhZByA%3D%3D.

195 "Alliance Persistent Surveillance from Space (APSS)," Factsheet, NATO, February 2023, https://www.nato.int/nato_static_fl2014/assets/pdf/2023/2/pdf/230215-factsheet-apss.pdf.

196 Ibid.

197 See, for example: Pingyue Yue, et al., "On the Security of LEO Satellite Communication Systems: Vulnerabilities, Countermeasures, and Future Trends," ArXiv Preprint, January 2022, https://www.techrxiv.org/ndownloader/files/32825063/1.

198 Lt Col Tim Vasen, "Mega Constellations. Commercial Small Satellite Constellation in Low Earth Orbit," in "Readahead of the Joint Air and Space Power Conference 2020," Joint Air Power Competence Centre, pp. 23-30, p. 27. https://www.japcc.org/wp-content/uploads/Read_Ahead_2020_Screen.pdf.

199 Sam Skove, "Using Starlink Paints a Target on Ukrainian Troops," Defense One, March 23, 2023, https://www.defenseone.com/threats/2023/03/using-starlink-paints-target-ukrainian-troops/384361/https://www.defenseone.com/threats/2023/03/using-starlink-paints-target-ukrainian-troops/384361/.

200 "GA-ASI Flight Tests LEO SATCOM on MQ-9A," General Atomics Aeronautical Systems, February 2, 2023, https://www.ga.com/ga-asi-flight-tests-leo-satcom-on-mq-9a.

201 Ibid.

202 Christophe Fontaine, "New MALE Drone Capabilities with AI," in "Readahead of the Joint Air and Space Power Conference 2020," pp. 197-204, p. 200.

203 "Space Transport Layer," US Space Development Agency, https://www.sda.mil/transport/.

204 Gil Baram, Omree Wechsler, "Cyber Threats to Space Systems," in "Readahead of the Joint Air and Space Power Conference 2020," pp. 47-56; Pingyue Yue, et al., "On the Security of LEO Satellite Communication Systems."

205 "NATO's Capabilities: Other Initiatives," NATO, last updated February 21, 2022, https://www.nato.int/cps/en/natohq/topics_49137.htm; "NATO Policy for civil/military aircraft operating in support of NATO or NATO-Led Missions and Operations," NATO Aviation Committee, August 2018, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_08/20160804_1608-NATO-Policy-civil-military.pdf; Ross McKenzie, Michael Callender, interview by authors.

206 NATO Standardization Office (NSO), NATO Standardization Document Database (NSDD), accessed May 18, 2023, https://nso.nato.int/nso/nsdd/main/standards.

207 Gordon B. Davis Jr., "The Future of NATO C4ISR," p. 15.

208 Emmanuel Bloch et al., "Ethical and technical challenges in the development, use, and governance of autonomous weapons systems," IEEE Standards Association, https://standards.ieee.org/wp-content/uploads/import/documents/other/ethical-technical-challenges-autonomous-weapons-systems.pdf.

209 NATO's innovation activities currently focus on nine priority technology areas: artificial intelligence (AI), autonomy, quantum, biotechnologies and human enhancement, hypersonic systems, space, novel materials and manufacturing, energy and propulsion, and next-generation communications networks. See: "Emerging and disruptive technologies," NATO, https://www.nato.int/cps/en/natohq/topics_184303.htm.

210 See, for instance, Mariarosaria Taddeo, Alexander Blanchard, "A Comparative Analysis of the Definitions of Autonomous Weapons Systems," Science and engineering ethics, vol. 28 (5), Aug. 2022, doi:10.1007/s11948-022-00392-3; Paul Scharre, Army of None: Autonomous Weapons and the Future of War, W. W. Norton & Company, New York & London, 2018.

211 NATO definitions: Autonomous: pertaining to a system that decides and acts to accomplish desired goals, within defined parameters, based on acquired knowledge and evolving situational awareness, following an optimal but potentially unpredictable course of action; Automated: pertaining to a system that, in response to inputs, follows a predetermined set of rules to provide a predictable outcome; Automatic: pertaining to a process or equipment that, under specified conditions, functions without human intervention. "AAP-06 Edition 2021: NATO glossary of terms and definitions," NATO Standardization Office, 2021, p. 16.

212 [213] Ibid.

213 Expert on UAS and autonomous technologies from the Defense industry, closed-door discussion at CEPA, January 26, 2023.

214 Roberto Patti, "Joint Operations with Unmanned Aircraft Systems (UAS)," pp. 25-26.

215 NATO ASG for Intelligence David Cattler, interview by authors.

216 Ibid.

217 Gordon B. Davis Jr., "The Future of NATO C4ISR," p. 12.

218 Major Giuseppe Valentino, "Big Data in ISR. Big Opportunity for Data Analysis Challenges," JAPCC, Edition 32, Summer 2021, pp. 62-67, p. 64. https://www.japcc.org/wp-content/uploads/JAPCC_J32_screen.pdf.

219 Ibid.

220 "Using quantum technologies to make communications secure," NATO, September 27, 2022, https://www.nato.int/cps/en/natohq/news_207634.htm?selectedLocale=en.

221 "What is Quantum Sensing?," BAE System, https://www.baesystems.com/en-us/definition/what-is-quantum-sensing.

222 See, respectively, "Summary of the NATO Artificial Intelligence Strategy," NATO, October 2021, https://www.nato.int/cps/en/natohq/official_texts_187617.htm; "Summary of NATO's Autonomy Implementation Plan," NATO, October 2022, https://www.nato.int/cps/en/natohq/official_texts_208376.htm.

223 "NATO's Data and Artificial Intelligence Review Board," NATO, last updated October 13, 2022, https://www.nato.int/cps/en/natohq/official_texts_208374.htm.

224 Conor Hannigan, Defense Investment Staff Officer, NATO, interview by Gordon B. Davis, Jr., March 2023. See also: Andrea Gilli, "NATO-Mation": Strategies for Leading in the Age of Artificial Intelligence, NDC Research Paper 15, Nato Defense College, December 2020, https://www.ndc.nato.int/download/downloads.php?icode=671.

225 Capability integration addresses all aspects of NATO Doctrine, Organization, Training, Material, Leader Development, People, Facilities, Interoperability (DOTMLFPI).

226 NATO, "NATO sharpens technological edge with innovation initiatives," last updated April 7, 2022, https://www.nato.int/cps/en/natohq/news_194587.htm. See also https://diana.nato.int/.

227 NATO, "NATO launches Innovation Fund," last updated June 30, 2022, https://www.nato.int/cps/en/natohq/news_197494.htm.

228 Zoe Stanley-Lockman, interview by authors.

229 NATO, "NATO approves 2023 strategic direction for new innovation accelerator," last updated December 13, 2022, https://www.nato.int/cps/en/natohq/news_210393.htm.

230 Authors' correspondence with Zoe Stanley-Lockman, Emerging Security Challenges Staff Officer, NATO, June 2023.

231 Phillip Lockwood, Emerging Security Challenges Staff Officer, NATO, discussion with Gordon B. Davis, Jr. April 5, 2022.

232 although at the time of this report's publication Finland may also have joined

233 "NATO launches Innovation Fund," NATO.

234 "Allies complete appointment of the NATO Innovation Fund's Board of Directors," NATO, last updated May 3, 2023, https://www.nato.int/cps/en/natohq/news_214270.htm.

235 Authors' correspondence with Zoe Stanley-Lockman.

236 NATO's Joint Capability Group-UAS falls under NATO's Conference of National Armament Directors.

237 Ross McKenzie, Michael Callender, interview by authors.

238 Ibid.

239 "AEP-84 Vol.1, Standard Interfaces of Unmanned Aircraft (UA) Control System (UCS) for NATO UA Interoperability – Interface Control Document, Ed. A Vers.1," 2017, p. 3-6. This document constitutes the "body" of the NATO "Standardisation Agreement (STANAG) 4586 – "Standard Interfaces of UA Control System (UCS) for NATO UA Interoperability," Edition 4," 5 April 2017.

240 Ibid.

241 Ibid.

242 STANAG 4586 identifies five Levels of Interoperability (LOI) for UAS (i.e., the degree of control that an operator has on the aircraft and its payload): Level 1: Indirect receipt/transmission of UA-related data and metadata, Level 2: Direct receipt/transmission of UA-related data and metadata, Level 3: Control and monitoring of the UA payload, not the unit, Level 4: Control and monitoring of the UA without launch and recovery, Level 5: Control and monitoring of the UA, including launch and recovery.

243 Ibid, p. 1-1.

244 "GA-ASI Flies New Multi-Use NATO Pod on MQ-9," General Atomics Aeronautical Systems, December 20, 2022, https://www.ga-asi.com/ga-asi-flies-new-multi-use-nato-pod-on-mq-9.

245 See: "STANAG 4671 - Unmanned Aircraft Systems Airworthiness Requirements (USAR), Edition 3 - AEP-4671," April 2019; "STANAG 4702 - Unmanned Aircraft Systems Rotary Wing Airworthiness Requirements, Edition 2 - AEP-80," November 2016; "STANAG 4703 - Light Unmanned Aircraft Systems Airworthiness Requirements, Edition 2 - AEP-83," November 2016.

246 "STANAG 4670 - Minimum Training Requirements for Unmanned Aircraft Systems (UAS) Operators and Pilots, Edition 5 - ATP-3.3.8.1," May 2019.

247 "STANAG 4737 - Unmanned Aircraft Systems Weapons Integration, Edition 1 - AEP-82, AEP-82.1 SRD" (Classified), June 2017.

248 "STANAG 4660 - Interoperable Command and Control Data Link for Unmanned Systems (IC2DL), Edition A - AEP-77" (Classified), November 2016.

249 Ross McKenzie, Michael Callender, interview by authors.

250 Ibid.

251 "PROJECT X empowers young innovators to build technologies for the future," NATO, https://www.nato.int/cps/en/natohq/news_191406.htm?selectedLocale=en.

252 Chris Gordon, "'We're Weird': New Commander Details Life Inside Task Force 99," Air & Space Forces Magazine, March 2, 2023, https://www.airandspaceforces.com/were-weird-new-commander-details-life-inside-task-force-99/.

253 "OFFensive Swarm-Enabled Tactics (OFFSET)," DARPA, accessed May 20, 2023, https://www.darpa.mil/work-with-us/offensive-swarm-enabled-tactics; Col Calhounm, LongShot, cit; LtCol Hefron, Air Combat Evolution.

254 "Unmanned aerial vehicles in the United States military," Wikipedia, accessed May 1, 2023, https://en.wikipedia.org/wiki/Unmanned_aerial_vehicles_in_the_United_States_military. Ridvan Bari Ucosta, "Turkish Drone Doctrine and Theaters of War in the Greater Middle East," Small Wars Journal, April 11, 2021, https://smallwarsjournal.com/jrnl/art/turkish-drone-doctrine-and-theaters-war-greater-middle-east.

255 AGS Commander Andrew Clark, interview by authors.

256 "Summary of NATO's Autonomy Implementation Plan," NATO.

257 Ross McKenzie, Michael Callender, interview by authors.

258 Ibid.

259 Ibid.

260 "NATO Standard, "Aep-101 Guidance on Sense and Avoid for Unmanned Aircraft Systems," Edition A, Version 1, February 2018. https://nso.nato.int/nso/nsdd/main/standards/ap-details/2435/EN. Ross McKenzie, Michael Callender, interview by authors.

261 K. Pollpeter, E. Barrett, "NATO Ally Contributions to the Space Domain."

262 "Counter Terrorism," NATO, last updated April 4, 2023, https://www.nato.int/cps/en/natohq/topics_77646.htm.

263 "Operational Experimentation 2020 Fact Sheet – Countering Class I Unmanned Aircraft Systems (C-UAS)," NATO ACT, https://www.act.nato.int/application/files/3415/8257/4721/2020_cuas.pdf.

264 "NATO Agency holds exercise to improve counter-drone technology," NCIA, November 11, 2021, https://www.ncia.nato.int/about-us/newsroom/nato-agency-holds-exercise-to-improve-counterdrone-technology.html. "NCI Agency holds NATO's live-testing counter-drone exercise," NCIA, September 28, 2022, https://www.ncia.nato.int/about-us/newsroom/nci-agency-holds-natos-livetesting-counterdrone-exercise.html.

265 Claudio Palestini, "Countering drones: looking for the silver bullet," NATO Review, December 16, 2020, https://www.nato.int/docu/review/articles/2020/12/16/countering-drones-looking-for-the-silver-bullet/index.html.

266 Claudio Palestini, interview by authors. The doctrine on C-UAS operations applies to air defense and Integrated Air and Missile Defense (IAMD) rather than envisioning C-UAS as a distinct capability.

267 Ibid.

268 Ibid.

269 Ibid.

270 Ibid.

271 Anduril, interview by authors, April 2023.

272 [2]72 Claudio Palestini, interview by authors.

273 Ibid.

274 Ibid; "Tech in focus: C-UAS - Counter Unmanned Aerial Systems," NATO, September 28, 2022, https://www.ncia.nato.int/videos/tech-in-focus-cuas-counter-unmanned-aerial-systems.html.

275 John Harper, "U.S. Military Tests Counter-drone Smartphone App," Real Clear Defense, July 21, 2023, https://www.realcleardefense.com/2023/07/21/us_military_tests_counter-drone_smartphone_app_967621.html.

276 "Autonomous Aerial Defense," Anduril, https://www.anduril.com/capability/counter-uas/.

277 Ed House, Business development manager for land systems, and Matthew Green, Senior Vice President for Government Relations, Leonardo DRS, Interview by authors, March 2023.

278 Andrew Eversden, "'Bullet made out of light': Army to field first Stryker-mounted combat laser in next 45 days," Breaking Defense, August 10, 2022, https://breakingdefense.com/2022/08/bullet-made-out-of-light-army-to-send-first-stryker-mounted-combat-laser-to-soldiers-in-next-45-days/.

279 Ibid.

280 Antonio Calcara et al., "Why Drones Have Not Revolutionized War," p. 134.

281 Ed House, Matthew Green, Interview by authors.

282 "General Atomics' Self-Protection Pod (SPP) payload now integrated into the MQ-9 UAS family. GA-ASI Successfully Completes Self-Protection System Demo on MQ-9," General Atomics Aeronautical Systems, January 22, 2021, https://www.ga-asi.com/ga-asi-successfully-completes-self-protection-system-demo-on-mq-9.

283 Ella Vanderzyl, interview by authors.

284 Ibid.

285 Major André Haider, "Remotely Piloted Aircraft Systems in Contested Environments. A Vulnerability Analysis," Joint Air Power Competence Centre (JAPCC), September 2014, https://www.japcc.org/wp-content/uploads/JAPCC-RPAS-Operations-in-Contested-Environments.pdf.

286 Ibid.

287 Antonio Calcara et al., "Why Drones Have Not Revolutionized War," p. 134.

288 Lance Menthe et al., "The Future of Air Force Motion Imagery Exploitation," RAND Corporation, 2012, p. 5, https://www.rand.org/content/dam/rand/pubs/technical_reports/2012/RAND_TR1133.pdf.

289 Travis L. Norton, "Staffing for Unmanned Aircraft Systems (UAS) Operations, Institute for Defense Analyses," June 2016, https://prhome.defense.gov/Portals/52/Documents/MRA_Docs/TFM/Reports/F2108340_TFMR-Staffing%20for%20Unmanned%20Aircraft%20Systems%20(UAS)%20Operations-ForPIIWork-DM.pdf.

290 Ibid, p. 29.

291 NATO AGS Commander, interview by authors.

292 Ibid.

293 Ibid.

294 See, for example Nishawn S. Smagh, "Intelligence, Surveillance, and Reconnaissance Design for Great Power Competition," Congressional Research Service, June 4, 2020, https://sgp.fas.org/crs/intel/R46389.pdf; Lance Menthe et al., "The Future of Air Force Motion Imagery Exploitation," p. 5; Troy Thomas, Cameron Scott, Nate Miller, "How ISR Tech Will Disrupt the Market for Defense Drones," Boston Consulting Group, February 6, 2020, https://www.bcg.com/publications/2020/isr-tech-disrupt-market-defense-drones.

295 See, for example, "Air Force Should Take Additional Steps to Improve Aircrew Staffing and Support," Report GAO-20-320, Government Accountability Office, June 2020, https://www.gao.gov/assets/gao-20-320.pdf.

296 See, for example, Justin D. Durham et al., "UAS Air Carrier Operations Survey: Fatigue," Federal Aviation Administration, Technical Report, March 2023, https://www.faa.gov/sites/faa.gov/files/UAS_Air%20Carrier%20Operations%20SME%20Survey%20-%20Fatigue.pdf; Johnny Duray, "Forever Deployed: Why 'Combat-to-Dwell' Reform for MQ-9 Crews is Beyond Overdue," War on the Rocks, January 23, 2018, https://warontherocks.com/2022/09/keep-mq-9-pilots-flying/.

297 Cpt Sean M. Minton, "The UAS Training Imperative: How to Implement C-UAS Training at the Company Level," Infantry, Spring 2019 Issue, pp. 20-24, https://www.benning.army.mil/infantry/magazine/issues/2019/Spring/PDF/INF%20MAG_SPRING19.pdf.

298 Christine M. Covas-Smith et al., "Training Remotely Piloted Aircraft Operations and Data Exploitation: Development of a Testbed for Integrated Ground Control Station Experimentation and Rehearsal (Tiger)," Report No. DRDC-RDDC-2016-P061, Defence Research and Development Canada, https://cradpdf.drdc-rddc.gc.ca/PDFS/unc240/p804390_A1b.pdf.

299 Sam Skove, "Army's new training simulators on track for 2024 delivery", Defense One, July 24, 2023, https://www.defenseone.com/technology/2023/07/armys-new-training-simulators-track-2024-delivery/388797/.

300 Ibid.

301 NATO AGS Force Commander, interview by authors.

302 Ibid.

303 See: "5 CTS Hosts SPARTAN REAPER Exercise," Defense Visual Information Distribution Center, March 6, 2023, https://www.dvidshub.net/news/439752/5-cts-hosts-spartan-reaper-exercise; "Multinational Aircraft Support JTAC Training During Ample Strike 2021," Allied Air Command Public Affairs Office, NATO, September 10, 2021, https://ac.nato.int/archive/2021/multinational-aircraft-support-jtac-training-during-ample-strike-2021.

304 "NATO Flight Training Europe," Factsheet, NATO, June 2023, https://www.nato.int/topics/mcc/Factsheet-NFTE_en.pdf.

305 Jacquelyn Schneider, "Does Technology Win Wars?," Foreign Affairs, March 3, 2023, https://www.foreignaffairs.com/ukraine/does-technology-win-wars.

306 "Emerging and disruptive technologies," NATO, last updated December 22, 2021, https://www.nato.int/cps/en/natohq/topics_184303.htm; "NATO releases first-ever strategy for Artificial Intelligence," NATO, last updated October 22, 2021; "Summary of NATO's Autonomy Implementation Plan," NATO, last updated October 13, 2022; https://www.nato.int/cps/en/natohq/official_texts_208376.htm.

307 "NATO allies take further steps towards responsible use of AI, data, autonomy and digital transformation," NATO, last updated October 13, 2022, https://www.nato.int/cps/en/natohq/news_208342.htm.

308 "Fireside Chat with General David L. Goldfein," Center for New American Security (CNAS), January 20, 2020, https://www.youtube.com/watch?v=Q1o9L2epXYU.

309 Gordon B. Davis Jr., "The Future of NATO C4ISR," p. 9.

310 "NATO 2022 Strategic Concept," NATO, June 29, 2022, pp. 3-6, https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf.

311 NATO ASG for Intelligence David Cattler, interview by authors.

312 David Cattler, NATO ASG for Intelligence, interview by Gordon B. Davis Jr., July 13, 2022, and Maj. Gen. Philip Stewart, former SHAPE DCOS SEM, interview by Gordon B. Davis Jr., July 11, 2022.

313 Allan McLeod, NSPA Director for Life Cycle Management, interview by authors, May 2, 2023.

314 Ibid.

315 NATO ASG for Intelligence and Security David Cattler, interview by authors.

316 NATO AGS Force Commander, interview by authors.

317 Ibid.

318 Zoe Stanley-Lockman and Edward Hunter Christie, "An Artificial Intelligence Strategy for NATO," NATO Review, October 25, 2021, https://www.nato.int/docu/review/articles/2021/10/25/an-artificial-intelligence-strategy-for-nato/index.html.

319 NATO ASG for Intelligence David Cattler, interview by authors; Doug Heinz, NSPA UAS Program Manager, interview by authors, May 2023.

320 See, for example, Jeffrey Reynolds, Jeffrey Lightfoot, "Digitalize the Enterprise," Atlantic Council, October 14, 2020, https://www.atlanticcouncil.org/wp-content/uploads/2020/10/NATO-20-2020-Digitalize-the-enterprise.pdf; Gordon B. Davis Jr., "The Future of NATO C4ISR,"

321 NATO AGS Force Commander, interview by authors.

322 Ibid.

323 Ibid.

324 Ibid.

325 Caitlin M. Kenney, "NATO Details Defense Plans – And Reiterates Call for More Member Spending," Defense One, May 11, 2023, https://www.defenseone.com/policy/2023/05/nato-details-defense-plansand-reiterates-call-more-member-spending/386220/.

326 Michael Callender and Ross McKenzie, NATO International Staff - Defence Investment, interview by authors, January 2023. Lichen Purseley, General Atomics Aeronautical Systems, interview by authors, May 2023.

327 M. Callender and R. McKenzie, interview by authors.

328 NSO, NSDD.

329 Doug Heintz and Allan McLeod, NSPA, interview by authors.

330 "Summary of the NATO Artificial Intelligence Strategy," NATO, last updated October 22, 2022, https://www.nato.int/cps/en/natohq/official_texts_187617.htm.

331 "NATO's Data and Artificial Intelligence Review Board," NATO, last updated October 17, 2022, https://www.nato.int/cps/en/natohq/official_texts_208374.htm.

332 "ACT Leads a Digital Transformation Workshop," ACT, January 13, 2023, https://act.nato.int/articles/act-leads-digital-transformation-workshop.

333 "Summary of NATO's Data Exploitation Framework Policy," NATO, last updated December 9, 2022, https://www.nato.int/cps/en/natohq/official_texts_210002.htm.

334 "Collaborative Air Combat," DARPA; Calhoun, "LongShot;" Hefron, "Air Combat Evolution."

335 Jon Harper, "US Central Command's new Task Force 99 begins drone operations in Middle East," DEFENSESCOOP, February 13, 2023, https://defensescoop.com/2023/02/13/us-central-commands-new-task-force-99-begins-drone-operations-in-middle-east/.

336 "Army Warfighting Experiment," UK Army, accessed May 21, 2023, https://www.army.mod.uk/our-future/awe/; "ARIEL," UK Army, accessed May 21, 2023, https://www.army.mod.uk/our-future/innovation/.

337 "Science & Technology Trends 2023-2043: Across the physical, biological and informational domains," NATO STO, Volume 1 Overview, pages 30-35 (Robotics and Autonomous Systems), March 2023, Brussels.

338 See DIANA website at https://diana.nato.int/.

339 "Updated DIANA footprint: Test Centres," NATO DIANA, March 2023, https://diana.nato.int/resources/site1/general/test-centres_v2.pdf.

340 "Frequently Asked Questions: Which are DIANA's priority areas of focus for 2023?," NATO DIANA, https://diana.nato.int/faq.html.

341 "Allies take further steps to establish NATO Innovation Fund," NATO, last updated March 30, 2023, https://www.nato.int/cps/en/natohq/news_213002.htm.

342 Approved by NATO's Conference of National Armaments Directors in October 2021. Robert Weaver, NATO Deputy Assistant Secretary General for Defense Investment, interview by authors, March 11, 2022.

343 Gordon B. "Skip" Davis Jr., "The Future of NATO C4ISR," pp. 30-31.

344 Representatives from Anduril and General Atomics Aeronautical Systems, interview by authors.

345 JAPCC, "Strategic Concept of Employment for UAS in NATO," January 2010, https://www.japcc.org/wp-content/uploads/UAS_CONEMP.pdf.

346 "AJP-3.3 Allied Joint Doctrine for Air and Space Operations Edition B Version 1," April 2016, NSO, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/624137/doctrine_nato_air_space_ops_ajp_3_3.pdf.

347 "Joint Doctrine Publication 0-30.2 Unmanned Aerial Systems," UK Ministry of Defence Development, Concepts and Doctrine Centre, August 2017, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/673940/doctrine_uk_uas_jdp_0_30_2.pdf.

348 "NATO allies take further steps," NATO.

349 Lt. Col. Andre Haider, "Introduction," in Claudio Palestini, ed., "A Comprehensive Approach to Countering Unmanned Aircraft Systems," Joint Air Power Competence Centre, 2021, p. 12, https://www.japcc.org/wp-content/uploads/A-Comprehensive-Approach-to-Countering-Unmanned-Aircraft-Systems.pdf.

350 Claudio Palestini, interview by authors.

351 On the importance of the human element and the prospects of human-machine interaction see: Andrea Gilli, eds., "The Brain and the Processor: Unpacking the Challenges of Human-Machine Interaction," NDC Research Paper 6, December 2019. https://www.ndc.nato.int/download/downloads.php?icode=619.

Center for European Policy Analysis
1275 Pennsylvania Ave NW, Suite 400
Washington, DC 20004
info@cepa.org | www.cepa.org