INTEGRATED AIR & MISSILE DEFENCE CENTRE OF EXCELLENCE

Souda Air Base, 73100, Chania

https://www.iamd-coe.org

Chania 09 February 2024

The Evolving UAS Threat: Lessons from the Russian-Ukrainian War Since 2022 on Future Air Defence Challenges and Requirements

Report prepared for the Integrated Air and Missile Defence Center of Excellence coordinated with its Concept Development and Experimentation Branch; desk officers Col. E. PANOU, LtC. I. STATHAKIS, LtC D. KOUTSOUKOS, LtC. K. KIRILOV, Cpt. E. MAVROGIANNAKIS

By N. BLAKCORI [intern]

The proliferation of UAS employment on the battlefield has been a manifest characteristic of the war in Ukraine since Russia's invasion in February 2022. This has prompted significant scholarly attention around how traditional air defence capabilities need to adapt to the increasing range and complexity of threats. Aiming to capture the main challenges identified in the literature and areas of development seeking to address current vulnerabilities, this report argues that the issues confronted are representative of efforts to re-organise and prepare the Alliance for high-intensity, network-centric warfare. More precisely, cheap attritable class I drones have created an unfavourable cost-interception curve for traditional kinetic countermeasures, reinforcing the importance of private-public sector collaboration and flexible procurement process. The defence industry needs to remain reactive towards the diversity of technical challenges confronted, especially as innovations in sensing, AI and next-generation networks have expanded the mission sets of UAS. Considering the full-spectrum nature of drone warfare, multi-domain integration is identified as a critical effort towards converging effects and maintain a competitive decision-making tempo. Furthermore, AI, electronic warfare, space and cyber will remain key enablers. While exploiting human-machine interfaces will contribute towards higher fidelity detection, decentralized execution, and decreased vulnerability in denied environments, downlink data, software and PNT can still, however, be targeted by EW and cyber-attacks. It suggests that the balance between the offense and defence will depend on onboard means of protection, effective combinations of soft and hard-kill countermeasures as well as more generally network integration and standardization of operational concepts and TTPs across the Alliance.

This argument is established by first briefly outlining the employment of UAS by Russian and Ukrainian armed forces since February 2022, analysing the return of organic mass and its requirements from the defence industry, as well as the increasing diversity of technical challenges imposed on traditional air defence systems. The report then assesses capability enablers and areas of technological development for UAS and C-UAS, namely the importance of network integration, digitization, and data management for enabling the convergence of effects, the exploitation of AI for decision-making advantage and finally assessing the implications of an increasingly congested and contested EM spectrum.

UAS employment by Ukraine and Russia

UAS employment since Russia's 22 invasion of Ukraine, and its evolution, has proven illustrative of wider developments in UAS technology, its adaptation to high-intensity warfare and the increasing complexity of the modern-day battlefield. Before assessing the new opportunities, challenges, and requirements that current and emerging UAS technology pose to air defence, this report briefly outlines the type of drones used by Russian and Ukrainian armed forces and under which missions are set.

Class III or Medium Altitude Long Endurance (MALE) drones made a prominent appearance during the early stages of the war. For Ukraine this was Turkish-manufactured Bayraktar TB2, carrying "four smart laser-guided munitions" as well as a capable "multi-spectral sensor payload for information collection and targeting"[1]. For Russia this was the Kronshtadt Orion, Korsar and Forpost-R (licenced copy of the Israeli IAI Searcher Mk II drone) that constituted its indigenous MALE fleet. After several months, this also included the Iranian-manufactured

[1] Borsari, F. & Gordon B. 'Skip' Davis, Jr. (2023). *An Urgent Matter of Drones: Lessons for NATO from Ukraine—CEPA*. https://cepa.org/comprehensive-reports/an-urgent-matter-of-drones/

Mohajer-6 UAV. Both the Russian and Iranian platforms can also carry guided and unguided munitions, "including Kab-20 and Qaem-5 light precision-guided munitions (PGM) and "the heavier Kab-50 guided/unguided bomb"[2].

While these MALE UAV fleets provide persistent, high-quality standoff ISR, EW and strike options, and therefore valuable for "offensive air operations" as well as "gathering information over a long period of time", their survivability is poor under non-permissive environments[3]. Provided that neither side managed to establish air superiority, Ukraine and Russia have relied more heavily on small, attritable and often commercial UAS capabilities.

For Ukraine, this has been the "wild hornet" first person view (FPV) UAS, "the punisher" a low-cost reusable attack drone also domestically produced by UA dynamics, as well as several other models such as SHARK and Leleka-100, including those provided by western partners (ScanEagle and Puma ISR drones).[4] On the Russian side, this has mainly been the Orlan-10 multirole UAS, which can also be equipped with a variety of payloads and EW capabilities. Commercially, Russia has largely benefited from shipments from DJI, the Chinese drone manufacturer. According to official Russian customs data, the Kremlin has received more than "$12 million in drone and drone parts" since Feb 2022, likely to include both the Mavic and Matrice drone series[5].

Finally, both sides have employed UAS as loitering munitions (LM) for a broad range of missions, including the Suppression and Destruction of Enemy Air Defences (SEAD and DEAD), as such systems combine ISR, communication nodes, data transfer and strike functionality into a single platform[6]. While Kub-BLA and Lancet 3 systems constitute Russia's indigenous systems, its LM capabilities have been reinforced by shipments of the Shahed 136 and 131 variants from Iran[7]. As a long-range munition (over 2,000km) this has enabled Russia to strike deep into Ukrainian territory, and while the Shahed is limited by a lack of protection, has made notable "modifications to achieve noise reduction… and harden navigation"[8]. On the Ukraine's side, in addition to the improvised FPV kamikaze drones assembled by Ukrainian forces, more than 1,000 switchblade drones have been exported to Kyiv from the US since March 2022[9]. The Ukrayinska Pravda media outlet has also recently cited Ukrainian Strategic

---

[2] Ibid.

[3] Ibid.

[4] Ibid.

[5] Mozur, P., Krolik, A., & Bradsher, K. (2023, March). *As War in Ukraine Grinds On, China Helps Refill Russian Drone Supplies—The New York Times*. The New York Times. https://www.nytimes.com/2023/03/21/business/russia-china-drones-ukraine-war.html

[6] Goldstein, L., & Waechter, N. (2023, November). *Chinese Strategists Evaluate the Use of 'Kamikaze' Drones in the Russia-Ukraine War | RAND*. https://www.rand.org/pubs/commentary/2023/11/chinese-strategists-evaluate-the-use-of-kamikaze-drones.html

[7] Kunertova, D. (2023). Drones have boots: Learning from Russia's war in Ukraine. *Contemporary Security Policy*, *44*(4), 576–591. https://doi.org/10.1080/13523260.2023.2262792

[8] Watling, J., & Reynolds, N. (2023). *Stormbreak: Fighting Through Russian Defences in Ukraine's 2023 Offensive* (Special Report, pp. 19). RUSI.

[9] Elise Vincent. (2023, June). *War in Ukraine loosens Western restrictions on remotely operated munitions*. Le Monde. https://www.lemonde.fr/en/international/article/2023/06/18/war-in-ukraine-loosens-western-restrictions-on-remotely-operated-munitions_6033279_4.html

Industries Minister on the domestic manufacturing of drones, including the mass-production of long-range kamikaze drones[10].

EW capabilities have also been a cornerstone C-UAS capabilities but will be later analysed when discussing vulnerabilities associated with a contested electromagnetic spectrum (EM).

The return of mass - new operating possibilities, challenges and sustainment requirements

The proliferation of cheap, expendable class I drones has created an unfavourable cost-interception curve for traditional air defence platforms as well as contributing to wider observations concerning the return of mass as "a foundational force planning principle"[11]. The growing importance of quantity also raises questions about current procurement process, opportunities for closer collaboration with the private sector and the adequacies of the Alliance's current military-industrial capacities for sustaining high-intensity warfare.

The fielding of small, low cost, less sophisticated UAVs, including loitering munitions has permitted their use as "consumable item(s)", creating new opportunities for saturation attacks and deep strikes[12].

The first challenge of saturation pertains the ability to conduct cost-effective "rudimentary drone swarming tactics or fake swarms" whereby current air defence platforms are overwhelmed by "an insuppressible collection of targets that are, seemingly, everywhere and nowhere at once"[13], or equally that it remains too costly to resort to "relatively expensive kinetic interceptors"[14]; air-to-air missiles or ground-based interceptors cost between $400,000 and $1.2 million each[15] .

Secondly, conducting deep strikes have become increasingly difficult provided the increasing range of anti-air/air-denial (A2/AD) assets and the cost of precision guided munitions. Current capabilities rely on a limited stockpile of medium range missiles[16], however loitering munitions could change this. First given their small radar signature and slow speed, loitering munitions such as the Sahed series, problematize tracking and detection as well as offering strike capabilities at increasing range[17]. They're also more affordable to field in large numbers; It costs roughly "$20,000 per piece versus $1 million for a single standard cruise missile"[18].

---

[10] Huaxia. (2023, December). *Ukraine launches mass production of long-range kamikaze drones*. Xinhua. https://english.news.cn/20231228/c37f6a6a08274e4294a0ed4bf01ce0f4/c.html

[11] Eaglen, M. (2023, October). Wars of Mass and Attrition Demand a Military Sized for Three Theaters. *American Enterprise Institute - AEI*. https://www.aei.org/foreign-and-defense-policy/wars-of-mass-and-attrition-demand-a-military-sized-for-three-theaters/

[12] Vallée, P. (2023). The Role of Unmanned Aerial Vehicles in Current and Future Conflicts. *Les Cahiers de La Revue Défense Nationale*, 95–102.

[13] Scharre, P. (2014). *Robotics on the Battlefield Part II The Coming Swarm* (pp. 5–50). Center for a New American Security.

[14] Borsari, F. & Gordon B. 'Skip' Davis, Jr. (2023). *An Urgent Matter of Drones: Lessons for NATO from Ukraine—CEPA*. https://cepa.org/comprehensive-reports/an-urgent-matter-of-drones/

[15] Knights, M., & Almeida, A. (2022). *What Iran's Drones in Ukraine Mean for the Future of War* [Policy Analysis]. The Washington Institute for Near East Policy.

[16] Vallée, P. (2023). The Role of Unmanned Aerial Vehicles in Current and Future Conflicts. *Les Cahiers de La Revue Défense Nationale*, 95–102.

[17] Borsari, F. & Gordon B. 'Skip' Davis, Jr. (2023). *An Urgent Matter of Drones: Lessons for NATO from Ukraine—CEPA*. https://cepa.org/comprehensive-reports/an-urgent-matter-of-drones/

[18] Kunertova, D. (2023). Drones have boots: Learning from Russia's war in Ukraine. *Contemporary Security Policy*, *44*(4), 576–591. https://doi.org/10.1080/13523260.2023.2262792

Overall, it suggests that drone warfare has become "less about technological sophistication, more about the ability to deploy in large numbers" as well as the necessity for "multi-spectrum" and "layered combinations" of both kinetic and non-kinetic counter-measures for air defence to be effective[19].

To respond to the increasing importance of mass, closer collaboration with the private sector to acquire commercial off-the shelf technology (COTS) will also play a crucial role. The Ukrainian government's partnership with private companies and work outside of the traditional military procurement process has illustrated the advantages of integrating commercial systems that are relatively cheap in comparison and often "quicker to produce and deploy… and already exist in large numbers off shelf"[20]. Indeed, according to the research conducted by Pierre Vallée on the role of Unmanned Aerial Vehicles in Current and Future Conflicts, private actors have "emphasises the speed of communications with their Ukrainian counterpart"[21].

Part of this public-private collaboration to offset Russian airpower, has been spurred by the Army of Drones initiative. A joint project between the digital transformation ministry and the governmental UNITED24 fundraising platform, it has deliberately pushed for the domestic expansion of drone industry to support not only procurement but also the repairing of drones and the training of Ukrainian drone units[22]. Recently, the PM has stated that "more than 200 Ukrainian companies have begun developing drones, fuelling a massive increase in production as well as technical innovation"[23]. In addition, the shortening obsolescence window for fielded software suggested the procurements of COTS is also advantageous in exploiting modularity. According to RUSI report on Multi-Domain Integration of UK Robotic and Autonomous Systems (RAS), "almost all RAS employed in Ukraine require alterations and updates to be made on a six-week cycle in order to keep ahead of EW tactics"[24]. For this reason, procuring commercial UAVs is also beneficial in the long-term, provided they often employ open-architecture and modular systems and therefore using flexible and reusable hardware/software.

Considering the aforementioned, employing UAS competitively on the battlefield will necessitate sustainment from the defence industry as a critical enabler. Franke and Soderstrom have rightly highlighted "Mass-still matters. The war has called into question western military-industrial capacities"[25]. According to the Fortune Business Insight market research report "The global Unmanned Aerial Vehicle (UAV) market size is projected to grow from $31.70 billion

---

[19] Ibid.

[20] Söderström, U. F., Jenny. (2023). *Star tech enterprise: Emerging technologies in Russia's war on Ukraine* [Policy Breif]. European Council On Foreign Relations. https://ecfr.eu/publication/star-tech-enterprise-emerging-technologies-in-russias-war-on-ukraine/

[21] Vallée, P. (2023). The Role of Unmanned Aerial Vehicles in Current and Future Conflicts. *Les Cahiers de La Revue Défense Nationale*, 95–102.

[22] Ostiller, N. (2023, October 25). *Minister: Ukraine to produce tens of thousands of drones per month by year's end*. The Kyiv Independent. https://kyivindependent.com/minister-ukraine-to-produce-tens-of-thousands-of-drones-per-month-by-years-end/

[23] Ibid.

[24] Kaushal, S. (2023). *Pathways Towards Multi-Domain Integration for UK Robotic and Autonomous Systems* (pp. iii–30) [Occasional Paper]. RUSI.

[25] Söderström, U. F., Jenny. (2023). *Star tech enterprise: Emerging technologies in Russia's war on Ukraine* [Policy Breif]. European Council On Foreign Relations. https://ecfr.eu/publication/star-tech-enterprise-emerging-technologies-in-russias-war-on-ukraine/

in 2023 to $91.23 billion by 2030"[26]. NATO has already begun to respond to this requirement through recent initiatives such as the DIANA 2022 and the NATO Innovation Fund (NIF). They aim to "bring allied nations and their industries and research communities into a closer partnership to fund, develop, and deploy dual use EDTs" and offer "good prospects of commercialization at scale", while the NATO Support and Procurement Agency (NSPA) also plays a key role in facilitating and harmonizing the acquisition of UAS across the Alliance[27]. Nonetheless challenges remain in terms of the RQ-4 remotely piloted aircraft employed under NATO's Alliance Ground Surveillance (**AGS**) system. As an "aging platform without an active industrial production line", it raises the issue of "diminishing manufacturing sources, with inevitable implications in terms of spare parts and life-cycle sustainment" [28].

For the Alliance to limit adversarial UAS capacity and production, the monitoring of exported dual-use drone components will also be important[29]. Both the Lancet 3 and Iranian Shahed series were found to include "several commercial and dual use electronic components produced by western countries"[30] [31].

Increasing diversity of technical challenges imposed on traditional air defence systems

Technical innovations that have expanded the variety of drone roles and mission sets, increasing the complexity of the UAS threat to air defence. Aside from traditional ISR, targeting and strike functions, drones have become more and more capable of carrying out SEAD/DEAD missions. Bosari and David also highlight that "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"[32].

The opportunity to combine with manned systems is a significant area of concept and capability development being explored, given recent technological improvements in sensing, AI and next-generation networks, albeit not yet tested in the Ukrainian conflict. The idea consists of combining high-end, yet cheap expendable systems with next generation autonomous wingman platforms to "conduct collaborative operations with crewed aircraft"[33]. According to the journal of the JAPCC, as early as 2015 the Joint Unmanned Aerial Vehicle (UAV) Swarming Integration (JUSI) Quick Reaction Test (QRT) was established to "develop, test, and validate a Concept of Employment (CONEMP) for the integration and synchronization of swarming UA performing Electronic Attack (EA) in support of the joint force against an advanced

---

[26] *Unmanned Aerial Vehicle [UAV] Market Growth & Share, 2030*. (2023, December). Fortune Business Insights. https://www.fortunebusinessinsights.com/industry-reports/unmanned-aerial-vehicle-uav-market-101603

[27] Borsari, F. & Gordon B. 'Skip' Davis, Jr. (2023). *An Urgent Matter of Drones: Lessons for NATO from Ukraine—CEPA*. https://cepa.org/comprehensive-reports/an-urgent-matter-of-drones/

[28] Ibid.

[29] Kunertova, D. (2023). Drones have boots: Learning from Russia's war in Ukraine. *Contemporary Security Policy*, *44*(4), 576–591. https://doi.org/10.1080/13523260.2023.2262792

[30] Borsari, F. & Gordon B. 'Skip' Davis, Jr. (2023). *An Urgent Matter of Drones: Lessons for NATO from Ukraine—CEPA*. https://cepa.org/comprehensive-reports/an-urgent-matter-of-drones/

[31] Byrne, J., Watling, J., Bronk, J., Somerville, G., Byrne, J., Crawford, J., & Baker, J. (2022). The Orlan Complex: Tracking the Supply Chains of Russia's Most Successful UAV. *RUSI*, 1–24.

[32] Borsari, F. & Gordon B. 'Skip' Davis, Jr. (2023). *An Urgent Matter of Drones: Lessons for NATO from Ukraine—CEPA*. https://cepa.org/comprehensive-reports/an-urgent-matter-of-drones/

[33] Ibid.

(Integrated Air Defence Systems) IADS"[34]. In the anticipation that future advanced UAS equipped with EW payloads will look to attack adversary air defence with layered offensive capabilities and lead a subsequent wave of attacking aircraft to enter and counter an adversary's A2/AD environment, the experimentation and development of CONEMPs are already being used to inform "requirements development, roadmaps, and eventually, Tactics, Techniques, and Procedures (TTP) in several areas, including communication, automation, UA, and EA to deliver intended effects"[35].

Another key focus for UAS employment since the 22' invasion of Ukraine has been the improvement of precision of fires. As well as shortening the targeting and firing cycles from 30 mins to 3-5 mins, changing the operational tempo of artillery, the use of UAVs in support of Russia's reconnaissance fire complex concept has been a key adaptation noted during Ukraine's counter-offensive, last summer. According a RUSI report, "the use of UAVs to designate for Kransnopol" during the Ukrainian offensive has increased - the Lancet having "been used extensively along with FPV UAVs to strike lead elements of Ukrainian units" - illustrating the shifting focus on effects (through improving the accuracy of fires) and "reducing the number of rounds necessary to achieve the desired outcome rather than resorting to saturation fires"[36].

Finally, the design of UAVs as loitering munitions (LMs), representing "a bridge between precision-guided weapons… and future autonomous weapon systems"[37], has been a hallmark of drone warfare in Ukraine. While loitering munitions date back to the 1980s with Israel use of the Harpy loitering munition, Chinese analysts have noted the extent to which LM have been able to achieve "big results in the Ukrainian war of attrition", destroying "air defence radars and missiles", relatively high value and expensive targets in a cost-effective way[38]. Briefly, LMs are autonomous missiles that stay "airborne for some time, identify a target and attack", whereby the munition's loiter indicates "the amount of time between launch and detonation"[39]. According to Atherton, developments in "communication technology, computing, processing and miniaturized sensors means that loitering munitions can now serve a range of functions in war once reserved for crewed aircraft or artillery". It's the ability to combine ISR, data transfer capabilities and strike functionality within a singular platform[40] that enables LMs to condense and simplify the sensor-to-shooter cycle[41]

Overall, the novel ways UAS are being employed against air defence systems is adding further complexity to the battlefield. Many scholars have called for the revision of existing NATO Joint Allied Doctrine, operational concepts and TTPs to cover "new and expanded roles of

---

[34] Gorenc, G. F. (2016). Breaking Intergrated Air Defence with Unmanned Aerial Vehicle Swarms—Developing and Testing the US Employment Concept. *The Journal of the JAPCC, 22*.
[35] Ibid.
[36] Watling, J., & Reynolds, N. (2023). *Stormbreak: Fighting Through Russian Defences in Ukraine's 2023 Offensive* (Special Report, pp. 1–28). RUSI.
[37] Atherton 2022
[38] Goldstein, L., & Waechter, N. (2023, November). *Chinese Strategists Evaluate the Use of 'Kamikaze' Drones in the Russia-Ukraine War | RAND*.
[39] Atherton 2022
[40] Goldstein, L., & Waechter, N. (2023, November). *Chinese Strategists Evaluate the Use of 'Kamikaze' Drones in the Russia-Ukraine War | RAND*.
[41] Borsari, F. & Gordon B. 'Skip' Davis, Jr. (2023). *An Urgent Matter of Drones: Lessons for NATO from Ukraine—CEPA*. https://cepa.org/comprehensive-reports/an-urgent-matter-of-drones/

UAS and the growing importance of C-UAS"[42]. Indeed, at the time of writing, NATO's adoption of its first C-UAS doctrine is undergoing approval.

Integration of information networks, enabling the convergence of multi-domain effects, digitization and data management

The Ukrainian conflict has notably displayed the importance of converging multi-domain effects. In terms of UAS, the overwhelming of Russian air defence systems in Sevastopol Bay by drone boats carrying explosives, deployed in tandem with aerial commercial/military unmanned platforms, is representative of the full-spectrum nature of drone warfare that is likely to become the defining feature of the third-drone age[43]. In addition to drone swarms, operating on varying degrees of autonomy, and other novel operating possibilities introducing further complexity on the battlefield, effective data management and interoperability across domains remain as critical as ever.

The success of UAS-enabled targeting networks currently depends on their effective integration into a battle management architecture that leverages multi-modal information across C2 nodes, combined with precision-fire capabilities, whilst remaining resilient under a degraded communications environment. According to a CEPA feature long report, this is "essential for preserving information dominance and expediting the kill chain"[44].

Presently, drones are integrated into the delta system, created by "the military A2724 unit and further developed by the Ukrainian Ministry of Defence"[45]. It's a cloud-based situational awareness and battle management system that fuses real-time multi-modal information (including from "distributed sensors behind and beyond the FLOT, including ISR from UAS, smartphones, radars, satellite imagery and OSNIT") onto a digital map that can be accessed across all levels[46]. On the Russian side, the Reconnaissance Fires Complex also depends on the integration of data from multiple sources. Watling and Reynold's assessment of Ukraine's counter-offensive in June 2023 notes Russia's increasing reliance on "military-bearer networks" and "app-based services for encoding and accessing data"[47]. This is a key enabler of cross-domain networks given the technology allows military platforms to communicate with each other using different types of networks such as satellites, cellular, radio or optical and should also improve resilience by being able to switch in the case of failure. An example of this can be found in the integration of the Strelets system to improve the accuracy of Russian artillery engagements. It allows multiple feeds from ground-based sensors or detections by reconnaissance troops to be programmed and transmitted through a wide range of bearers, which are then integrated into Russian digital fire control. The system also permits the bypassing of "centralised fire control for the delivery of effects". For example, any artillery engagements managed by Strelets during "the actions of Russian assault groups against the village of Artemivske in December 2022" information flows were carried "both to the CP, but

---

[42] Ibid.

[43] Kunertova, D. (2023). Drones have boots: Learning from Russia's war in Ukraine. *Contemporary Security Policy, 44*(4), 576–591. https://doi.org/10.1080/13523260.2023.2262792

[44] Borsari, F. & Gordon B. 'Skip' Davis, Jr. (2023). *An Urgent Matter of Drones: Lessons for NATO from Ukraine—CEPA*. https://cepa.org/comprehensive-reports/an-urgent-matter-of-drones/

[45] Rosengren, O. (2023, February 3). Network-centric Warfare in Ukraine: The Delta System. *Grey Dynamics*. https://greydynamics.com/network-centric-warfare-in-ukraine-the-delta-system/

[46] Borsari, F. & Gordon B. 'Skip' Davis, Jr. (2023). *An Urgent Matter of Drones: Lessons for NATO from Ukraine—CEPA*. https://cepa.org/comprehensive-reports/an-urgent-matter-of-drones/

[47] Watling, J., & Reynolds, N. (2023). *Stormbreak: Fighting Through Russian Defences in Ukraine's 2023 Offensive* (Special Report, pp. 19). RUSI.

also to a fire observer directly to the barrels", whereby the commander is "on, but does not need to be in the loop for the engagement to proceed"[48].

The conversation on improving cross-domain interoperability and integration cannot be separated from the future role of autonomy and improving human/machine teaming with uncrewed systems. Many initiatives recently underway, demonstrate NATO's interest in this domain. For example, the NATO Centre for Maritime Research and Experimentation (CMRE) have collaborated with partners in the NATO Science and Technology Organisation (STO) to standardize communications "among different C2 systems and uncrewed systems operating in communications limited environments". Ultimately, by developing a Collaborative Autonomy Tasking Layer (CATL) - they have worked towards a "set of languages for enabling multi-domain autonomous tasking and data sharing", which according to the CMRE's director, "these federated, multi-domain C2 architectures" should have "enormous implications…. in improving both human-machine interactions during operations and the utilization of uncrewed systems - including UAS - in communications-denied environments"[49].

Yet, these innovative developments should not diminish the challenge of standardization and training requirements that come with cross-domain integration. As Bosari and David rightly note, NATO will certainly require a "unified approach to data governance, common data formats and protocols; shared storage policies and standardized data management"[50]. Indeed, the NATO Data Exploitation Framework (DEF) policy was adopted in October 2021 in order to support such an alignment between NATO datasets and address the "absence of an optimized processing criterion in the overall exploitation process" through an "open and scalable data architecture, AI integration and standardized data management process"[51]. These challenges also apply for counter UAS measures. In this domain, NATO is looking to adopt the UK-developed SAPIENT interface as an Alliance wide, common C-UAS architecture. By providing clear guidelines concerning the communication between the diverse panoply of C2 sensors and effectors, and their effective integration into the overall air and missile defence network and civilian air traffic management system, alongside other encrypted/coded protocols such as Link-16 and Asterix, it provides a promising solution to "the technical issues hindering a common C-UAS architecture"[52]. Indeed, the interface control document was assessed as "an interoperability standard for multi-sensor counter-UAS systems, at the NATO technical interoperability exercise (TIE21) in The Netherlands[53]. Facilitating over 70 connections between C-UAS sensor systems and Command and Control (C2) systems, it was deemed highly successful. At the TIE22, it further enabled 31 advanced autonomous sensor nodes from different vendors to connect to 13 decision-making nodes during its evaluation[54].

[48] Watling, J. & Nick Reynolds. (2023). Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine. *RUSI*.

[49] Borsari, F. & Gordon B. 'Skip' Davis, Jr. (2023). *An Urgent Matter of Drones: Lessons for NATO from Ukraine—CEPA*. https://cepa.org/comprehensive-reports/an-urgent-matter-of-drones/

[50] Ibid.

[51] Ibid.

[52] Ibid.

[53] DSTL. (2021). *SAPIENT autonomous sensor system*. GOV.UK. https://www.gov.uk/guidance/sapient-autonomous-sensor-system

[54] Ibid.

Exploiting a data-rich battlefield through AI and autonomy

Innovations in human-machine interfaces have been at the forefront of efforts to exploit the increasing volume of data collected by ISR platforms. Here, AI for predictive analytics and decision-making can provide an information advantage within a data rich battlefield and where developments in edge computing can also support the concepts of distributed warfare in disconnected, dispersed environments. UAVs and drone operations hold enormous potential for exploiting autonomy. As note "the effectiveness of UAVs depends on the ability to process data received from drones almost in real time and distribute them to appropriate command posts"[55].

At present, the use of AI in drone operations in Ukraine has been to automate processes such as take-off, landing and in target acquisition "after which humans are notified to confirm the selected targets and the information is automatically sent back to the Ukrainian battle management system"[56].

While not yet fielded in combat, the Autonomous Air Combat Operations team within the US Air Force Research Laboratory (AFRL) have made strides in developing AI and machine learning agents that can execute modern air-to-air and air-to-surface skills (Georgina DiNardo Defence News 2023). For example, the Valkyrie XQ-58A developed by Kratos Defence & Security Solutions is one of many experimental stealthy Unmanned Combat Aerial Vehicle (UCAV)[57] currently undergoing development that has been able to "combine mission-configuration, autonomy and AI" whilst remaining within the attritable class range and successfully performing "manned/unmanned teaming, flying multiple teams of uncrewed aircraft together" as proof of concepts[58]. This drone, in particular, is designed to run a variety of missions in contested airspace using its AI pilot. Monitoring and interpreting feedback from multiple sensors, the AI would then issue commands to the onboard computer system, which would determine the flight path and settings to determine where it needs to go. Additionally, if a target is acquired, the UCAV would need authorization before it can be neutralised (human-in-the loop) - carrying up to 1,800Lbs of payload it could launch a variety of weapons[59]. According to the AFRL a successful three-hour sortie was led in July 2023 and demonstrated skills "immediately transferable to the Collaborative Combat Air program"[60]. Previous flights have equally supported the Air Force's loyal wingmen research. Overall, as a highly capable, yet significantly less expensive and risky option to traditional piloted vehicles, it can enable competitive decision-making cycles in non-permissive environments[61]. As the AFRL have

---

[55] Marcinek, K., & Han, E. (2023). *Russia's Asymmetric Response to 21st Century Strategic Competition: Robotization of the Armed Forces* (pp. 1–132). RAND Corporation. https://www.rand.org/pubs/research_reports/RRA1233-5.html

[56] Söderström, U. F., Jenny. (2023). *Star tech enterprise: Emerging technologies in Russia's war on Ukraine* [Policy Breif]. European Council On Foreign Relations. https://ecfr.eu/publication/star-tech-enterprise-emerging-technologies-in-russias-war-on-ukraine/

[57] Also see the Boeing MQ-28 Ghost Bar, HAL Combat Air Teaming System, nEUROn (European program for an unmanned combat air vehicle (UCAV) technology demonstrator)

[58] *Valkyrie: This Autonomous AI Drone Could Be the Military's Next Weapon [video]*. (2023, October). Wall Street Journal. https://www.wsj.com/video/valkyrie-this-autonomous-ai-drone-could-be-the-militarys-next-weapon/69F7725D-45F1-4464-8271-7A07DB74227A

[59] Ibid.

[60] Georgina DiNardo. (2023). Artificial intelligence flies XQ-58A Valkyrie drone. *Defense News*. https://www.defensenews.com/unmanned/2023/08/03/artificial-intelligence-flies-xq-58a-valkyrie-drone/

[61] Ibid.

stated, the employment of "a class of attritable aircraft like the XQ-58A provides the war fighter the opportunity to project air power with mass, complexity, and unpredictability"[62].

The UK SAPIENT (Sensing for Asset Protection with Integrated Electronic Networked Technology) autonomous sensory system is another key example of how AI has been combined to enable data fusion at the edge. The SAPIENT architecture uses AI algorithms to enable "multi-sensor fusion (correlation, association, and tracking) and sensor management (dynamic tasking of the sensors in response to the unfolding scenario)"[63]. Individual sensors are able "to make detections and classifications locally" and "make operating decisions autonomously such as which direction to look or whether to zoom-in, in order to fulfil higher-level objectives", managed by "a decision-making module which controls the overall system and makes some of the decisions normally made by the operators"[64].

The development of the SAPIENT system is additionally illustrative of how edge computing can be leveraged by UAS for decentralized execution. Palantir technologies, a key industry partner in data fusion at the edge, describes this as "AI embedded on disconnected, remote endpoints", whereby the model enables autonomous decision-making for UAS consuming real-time sensor data[65]. In doing so it reduces the "data that needs to be stored and transmitted" which is not only key in enabling low-latency, real time decision making but improves resilience against EW measures as throughput back to command nodes are reduced[66]. Additionally, Palantir also highlight their developing capacity to support multi-sensor fusion as separate edge AI communicating through mesh networks (identified as a key enabler of cross-domain communications) can enable sensor fusion across diverse payloads and modalities [such as RF and EO collections] which in turn can enable higher fidelity detection of entities of interest and in doing so "achieve higher fidelity detection of entities of interest"[67].

However, it's an imperative to remain conscious of vulnerabilities still associated with autonomy. First, while full autonomy, as described by the US DoD directive 3000.09 as the ability once activated to "select and engage targets without further intervention of the human operator" and therefore not requiring communication and data links, onboard autonomy can still be vulnerable in denied environments if UAS are employed with a human-in-the-loop/-on-the-loop approach[68]. Second, the internal process of autonomous systems - combining inputs from sensors to direct action - is itself prone to error, for example "misjudging distance or misunderstanding sensor information fed to it"[69]. Indeed, one recent report from the United Nations Institute for Disarmament Research found that "in addition to errors from data or coding, spoofing or other adversarial measures could misdirect an autonomous system"[70].

---

[62] *XQ-58A VALKYRIE – Air Force Research Laboratory*. (2023). AFRL. https://afresearchlab.com/technology/successstories/xq-58a-valkyrie/

[63] DSTL. (2021). *SAPIENT autonomous sensor system*. GOV.UK. https://www.gov.uk/guidance/sapient-autonomous-sensor-system

[64] Ibid.

[65] *Palantir Edge AI*. (2022). [Technical Whitepaper]. Palantir

[66] *Palantir Edge AI*. (2022). [Technical Whitepaper]. Palantir

[67] Ibid.

[68] Atherton, K. (2021). *Loitering munitions preview the autonomous future of warfare*. Brookings. https://www.brookings.edu/articles/loitering-munitions-preview-the-autonomous-future-of-warfare/

[69] Ibid.

[70] Ibid.

Nonetheless, AI, autonomy and human-machine teaming hold enormous potential for increasing both UAS and C-UAS capability, but as the CEPA report rightly highlights, exploiting human-machine teams to "enhance both offensive and defensive" forces require "network architectures, training and leader development"[71].

Contested EM spectrum and space/cyber vulnerabilities

An increasingly congested and contested EM spectrum has been a defining characteristic of the Russia-Ukrainian conflict, which has had a visible impact both on the use and defence against UAS. Whilst the proliferation of cheap, expendable class I drones arguably incentivise offensive action, as discussed in the beginning of this report, the use of jamming (including anti-drone guns and other EW equipment) have notably improved defence systems given that small drones are still sensitive to the electromagnetic environment. Given that UAVs are connected to ground control systems, the data links always run the risk of being corrupted without electronic counter measures[72].

By enabling connectivity between UAS and command modules, operators, analysts, cyberspace security remains closely linked as a critical vulnerability. Examples of attacks, in addition to the interception of downlink data from the UAS to the operator, include "the disruption of the drone through malicious code to impair its functions or capabilities" and "the intrusion in or disablement of the GCS operating system"[73]. In short, cyber-attacks against communication networks, software, payload, and intelligence, constitute the four different types of emerging security threats to UAS architecture[74]. Similarly, space assets also provide critical services for UAS, such as positioning, navigation, and timing (PNT) for guiding precision strikes, meteorological information and satellite-based communications. For example, loitering munitions use a "combination inertial guidance and commercial satellite navigation" and have therefore been vulnerable to jamming[75]. The Ukrainian's have in fact been able to intercept more than 80% of incoming Shahed 136s because their success depends on keeping a low profile on radars[76]. Vulnerable commercial navigation systems have enabled the use of "anti-aircraft missiles, rifles, machine guns and electromagnetic jamming" for interception[77]. Overall, Russia's C-UAS effort had notably improved during the second year of its invasion. The Armed Forces of the Russian Federation [AFRF] "now employ one major EW system per 10km of frontage, situated approx. 7km from the front line" and now employing more "specialized EW capabilities" at higher echelons[78]. More precisely, the Shipovnik-Aero jamming station been very effective at downing UAS through "its sophisticated range of effects" and making extensive "use of navigational interference in the battle as a form of

---

[71] Borsari, F. & Gordon B. 'Skip' Davis, Jr. (2023). *An Urgent Matter of Drones: Lessons for NATO from Ukraine—CEPA*. https://cepa.org/comprehensive-reports/an-urgent-matter-of-drones/

[72] Vallée, P. (2023). The Role of Unmanned Aerial Vehicles in Current and Future Conflicts. *Les Cahiers de La Revue Défense Nationale*, 95–102.

[73] Borsari, F. & Gordon B. 'Skip' Davis, Jr. (2023). *An Urgent Matter of Drones: Lessons for NATO from Ukraine—CEPA*. https://cepa.org/comprehensive-reports/an-urgent-matter-of-drones/

[74] Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, *97*, 101804. https://doi.org/10.1016/j.inffus.2023.101804

[75] Kunertova, D. (2023). Drones have boots: Learning from Russia's war in Ukraine. *Contemporary Security Policy*, *44*(4), 576–591. https://doi.org/10.1080/13523260.2023.2262792

[76] Ibid.

[77] Ibid.

[78] Watling, J. & Nick Reynolds. (2023). Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine. *RUSI*.

electronic protection" which has contributed, according to Watling and Reynold's interviews, to a loss rate of approx. 10,000 UAVs by the Ukrainian Armed Forces a month[79]. The AFRF has also ensured organic EW effector capabilities across the unit level; platoons equipped with directional jammers and arrays for hijacking UAVs as part of its C-UAS capability. As a result, the RUSI report on Preliminary Lessons in Conventional Warfighting, emphasises the use of non-kinetic means; targeting sensors, denial of navigation or control, within NATO's C-UAS strategy, recommending that electronic attack is available at all echelons as the "most efficient protection against (the) UAS" threat[80].

On the other hand, the lack of UAS onboard means of protection is slowly changing, keeping the balance between the offense and defence tenuous. In addition to the problem of EM spectrum fratricide, which has been "a major challenge of widespread employment" due to insufficiently trained UAF and AFRF battalion staff in synchronizing and managing EW assets, test "mating electronic attack payloads onto a coordinated semi or fully autonomous swarm of smaller unmanned aircraft" are maturing[81]. The defence industry is further looking into UAV electronic warfare solutions. A promising avenue has been manufactures and programmers using AI to enable small drones to strike their identified targets even with loss of communications[82]. However, defence analysts have warned that "AI is unlikely to impact the EW offense vs. drone defence balance in the short term" given that both "AI, particularly computer vision, models are not at a level of performance… to operate without a constant link to an operator" and "most COTS drones used in Ukraine don't have enough onboard processing power to effectively run state-of-the-art computer vision models in the first place"[83]. In fact, more generally, there are limits to equipping smaller mini-drone with anti-EW protection due to "weight, power consumption, and cost" - therefore on the level of class I drones, prioritising quantity should be a more cost-effective approach[84]. Notwithstanding, investment into low-orbit satellite-based communication terminals has already increased the resilience of UAS in spite "intense cyber and EW efforts" to deny communications[85].

Looking forward: concluding remarks

The proliferation of small, cheap, and attritable drones on the battlefield do not represent a revolution in military affairs - this disjuncture in offensive and defensive capabilities, like most emerging technologies present a transient advantage, fleeting in nature as most technological innovations eventually spawn into counter systems (in this case the development of C-UAS capabilities). The importance is therefore monitoring the perception of advantages conferred by such capabilities and finding conceptual innovations to address vulnerabilities. Indeed, when assessing capability, as one of the three foundational mechanisms that enables the

[79] Ibid.
[80] Zabrodskyi, M. (2023). *Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February–July 2022* (pp. 1–66). RUSI.
[81] Gorenc, G. F. (2016). Breaking Intergrated Air Defence with Unmanned Aerial Vehicle Swarms—Developing and Testing the US Employment Concept. *The Journal of the JAPCC*, *22*.
[82] Borsari, F. & Gordon B. 'Skip' Davis, Jr. (2023). *An Urgent Matter of Drones: Lessons for NATO from Ukraine—CEPA*. https://cepa.org/comprehensive-reports/an-urgent-matter-of-drones/
[83] Sydney J. Freedberg JR. (2023). *Dumb and cheap: When facing electronic warfare in Ukraine, small drones' quantity is quality*. Breaking Defense. https://breakingdefense.com/2023/06/dumb-and-cheap-when-facing-electronic-warfare-in-ukraine-small-drones-quantity-is-quality/
[84] Ibid.
[85] Borsari, F. & Gordon B. 'Skip' Davis, Jr. (2023). *An Urgent Matter of Drones: Lessons for NATO from Ukraine—CEPA*. https://cepa.org/comprehensive-reports/an-urgent-matter-of-drones/

defender to influence the adversary's cost-benefit calculus, as per traditional deterrence theory, it should be desegregated not only in terms of power and agility[86] but concepts as well. The UK joint doctrine identifies this as a key component for conventional deterrence, describing it as the ability "of our Armed Forces to execute plans and missions in timely, efficient ways and ***imaginative*** ways, using the best aspects of the moral and physical components (of fighting power)"[87].

This paper's mapping of the current and future operating environment in terms of (C-)UAS capabilities aims to guide analysis around "the design, development and disruptive innovation of the future force", but this constitutes only a third of the co-evolutionary process towards developing NATO's conceptual advantage. It also requires the "identification of concept to doctrine pathways…. making incremental improvements as elements of a concept are validated through its development" in tandem with the development of policy responding to the experimentation and lessons identified by Allied Command Transformation, Centres of Excellence or Multinational Capability Development Campaign studies which outline the ever-changing political-military envrionment we operate in.

Bibliography

Atherton, K. (2021). *Loitering munitions preview the autonomous future of warfare*. Brookings. https://www.brookings.edu/articles/loitering-munitions-preview-the-autonomous-future-of-warfare/

Borsari, F. & Gordon B. 'Skip' Davis, Jr. (2023). *An Urgent Matter of Drones: Lessons for NATO from Ukraine—CEPA*. https://cepa.org/comprehensive-reports/an-urgent-matter-of-drones/

Byrne, J., Watling, J., Bronk, J., Somerville, G., Byrne, J., Crawford, J., & Baker, J. (2022). The Orlan Complex: Tracking the Supply Chains of Russia's Most Successful UAV. *RUSI*, 1–24.

DSTL. (2021). *SAPIENT autonomous sensor system*. GOV.UK. https://www.gov.uk/guidance/sapient-autonomous-sensor-system

[86] See USCENTCON Model: Herr, W. E. (1996). *Operation Vigilant Warrior: Conventional Deterrence Theory, Doctrine and Practise*. School of Advanced Airpower Studies, pp. 56

[87] Development, Concepts and Doctrine Centre. (2019). *Deterrence: The Defence Contribution* (pp. 1–114) [Joint Doctrine Note 1/19]. UK Ministry of Defence

Eaglen, M. (2023, October). Wars of Mass and Attrition Demand a Military Sized for Three Theaters. *American Enterprise Institute - AEI*. https://www.aei.org/foreign-and-defense-policy/wars-of-mass-and-attrition-demand-a-military-sized-for-three-theaters/

Elise Vincent. (2023, June). *War in Ukraine loosens Western restrictions on remotely operated munitions*. Le Monde. https://www.lemonde.fr/en/international/article/2023/06/18/war-in-ukraine-loosens-western-restrictions-on-remotely-operated-munitions_6033279_4.html

Georgina DiNardo. (2023). Artificial intelligence flies XQ-58A Valkyrie drone. *Defense News*. https://www.defensenews.com/unmanned/2023/08/03/artificial-intelligence-flies-xq-58a-valkyrie-drone/

Goldstein, L., & Waechter, N. (2023, November). *Chinese Strategists Evaluate the Use of 'Kamikaze' Drones in the Russia-Ukraine War | RAND*. https://www.rand.org/pubs/commentary/2023/11/chinese-strategists-evaluate-the-use-of-kamikaze-drones.html

Gorenc, G. F. (2016). Breaking Intergrated Air Defence with Unmanned Aerial Vehicle Swarms—Developing and Testing the US Employment Concept. *The Journal of the JAPCC*, *22*.

Huaxia. (2023, December). *Ukraine launches mass production of long-range kamikaze drones*. Xinhua. https://english.news.cn/20231228/c37f6a6a08274e4294a0ed4bf01ce0f4/c.html

Kaushal, S. (2023). *Pathways Towards Multi-Domain Integration for UK Robotic and Autonomous Systems* (pp. iii–30) [Occasional Paper]. RUSI.

Kelsey, A. (2021). *Loitering munitions preview the autonomous future of warfare* [Commentary]. Brookings. https://www.brookings.edu/articles/loitering-munitions-preview-the-autonomous-future-of-warfare/

Knights, M., & Almeida, A. (2022). *What Iran's Drones in Ukraine Mean for the Future of War* [Policy Analysis]. The Washington Institute for Near East Policy. https://www.washingtoninstitute.org/policy-analysis/what-irans-drones-ukraine-mean-future-war

Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, *97*, 101804. https://doi.org/10.1016/j.inffus.2023.101804

Kunertova, D. (2023). Drones have boots: Learning from Russia's war in Ukraine. *Contemporary Security Policy*, *44*(4), 576–591. https://doi.org/10.1080/13523260.2023.2262792

Marcinek, K., & Han, E. (2023). *Russia's Asymmetric Response to 21st Century Strategic Competition: Robotization of the Armed Forces* (pp. 1–132). RAND Corporation. https://www.rand.org/pubs/research_reports/RRA1233-5.html

Mozur, P., Krolik, A., & Bradsher, K. (2023, March). *As War in Ukraine Grinds On, China Helps Refill Russian Drone Supplies—The New York Times*. The New York Times. https://www.nytimes.com/2023/03/21/business/russia-china-drones-ukraine-war.html

Ostiller, N. (2023, October 25). *Minister: Ukraine to produce tens of thousands of drones per month by year's end*. The Kyiv Independent. https://kyivindependent.com/minister-ukraine-to-produce-tens-of-thousands-of-drones-per-month-by-years-end/

Palantir Edge AI. (2022). [Technical Whitepaper]. Palantir.

Rosengren, O. (2023, February 3). Network-centric Warfare in Ukraine: The Delta System. *Grey Dynamics*. https://greydynamics.com/network-centric-warfare-in-ukraine-the-delta-system/

Scharre, P. (2014). *Robotics on the Battlefield Part II The Coming Swarm* (pp. 5–50). Center for a New American Security.

Söderström, U. F., Jenny. (2023). *Star tech enterprise: Emerging technologies in Russia's war on Ukraine* [Policy Breif]. European Council On Foreign Relations. https://ecfr.eu/publication/star-tech-enterprise-emerging-technologies-in-russias-war-on-ukraine/

Sydney J. Freedberg JR. (2023). *Dumb and cheap: When facing electronic warfare in Ukraine, small drones' quantity is quality*. Breaking Defense. https://breakingdefense.com/2023/06/dumb-and-cheap-when-facing-electronic-warfare-in-ukraine-small-drones-quantity-is-quality/

Unmanned Aerial Vehicle [UAV] Market Growth & Share, 2030. (2023, December). Fortune Business Insights. https://www.fortunebusinessinsights.com/industry-reports/unmanned-aerial-vehicle-uav-market-101603

Valkyrie: This Autonomous AI Drone Could Be the Military's Next Weapon [video]. (2023, October). Wall Street Journal. https://www.wsj.com/video/valkyrie-this-autonomous-ai-drone-could-be-the-militarys-next-weapon/69F7725D-45F1-4464-8271-7A07DB74227A

Vallée, P. (2023). The Role of Unmanned Aerial Vehicles in Current and Future Conflicts. *Les Cahiers de La Revue Défense Nationale*, 95–102.

Watling, J. & Nick Reynolds. (2023). Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine. *RUSI*.

Watling, J., & Reynolds, N. (2023). *Stormbreak: Fighting Through Russian Defences in Ukraine's 2023 Offensive* (Special Report, pp. 1–28). RUSI.

XQ-58A VALKYRIE – Air Force Research Laboratory. (2023). AFRL. https://afresearchlab.com/technology/successstories/xq-58a-valkyrie/

Zabrodskyi, M. (2023). *Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February–July 2022* (pp. 1–66). RUSI.