ASSOCIATION OF OLD CROWS
Advancing Electromagnetic Warfare TOGETHER
crows.org

January 2024 Vol. 47, No. 1

JED

Journal of Electromagnetic Dominance

Protecting Bases from Drones

Also in this Issue:

- DARPA – Maintaining the DOD's Microelectronics Advantage
- EW 101: Emitter Location "Error Budget"
- News: Sweden Receives New SIGINT Vessel

C-UAS – Protecting Critical Infrastructu

By Andrew White

On Nov. 1, the UK Ministry of Defence (MoD) published an intelligence update regarding the war in Ukraine which declared Russian One Way Attack (OWA) drones had emerged as "one of the most effective new capabilities" over the past 12 months. Specifically highlighting Russia's Lancet OWA drone, the intelligence update described how it could fly in contested areas, loiter to identify a target and then dive towards a target before detonating. "Russia deploys Lancets to attack priority targets, and they have become increasingly prominent in the key counter-battery fight, striking enemy artillery. Traditionally, Russia has used small [uncrewed aerial systems – UAS] mainly for reconnaissance. With its attack capability, Lancet signifies a step change in how Russia uses this category of weapons," the update explained.

The OWA drone threat is not restricted to Ukraine. In the wake of the Hamas-led October 7 attack against Israeli towns near Gaza, pro-Iranian groups have used OWA drones to successfully strike US and multi-national bases in Syria and Iraq.

While the counter-uncrewed aerial systems (C-UAS) mission has been evolving for nearly a decade, one specific aspect of this mission is focused on requirements to protect bases and installations from an evolving UAS threat, particularly OWA drones employed in saturation attacks. These lessons from Ukraine and the Middle East have especially prompted European forces to consider optimal means of upgrading air defense and C-UAS capabilities to protect military bases and infrastructure, both at home and abroad.

HARD-KILL C-UAS

Most of Ukraine's C-UAS systems have been provided by arms transfers from foreign nations. This includes a mix of hard-kill air defense systems, man-portable air defense systems (MANPADS) and thousands of hand-held C-UAS jamming systems. Russia has launched its long-range drones, combined with a variety of missiles, in saturation attacks against a broad set of food, energy and military targets. These include electrical plants throughout the country, grain storage facilities near Odessa, weapons manufacturing facilities and weapons repair depots. Ukraine has relied mostly on larger air defense systems to counter these threats.

In August, the International Fund for Ukraine (IFU) contracted with Norway's Kongsberg to deliver CORTEX Typhon C-UAS systems to the war-torn nation as part of a wider strategy to enhance levels in air defense across the country. In partnership with Teledyne FLIR Defense, Kongsberg's solution uses the Cerberus XL advanced thermal/visual imaging system and radar sensors to locate and track UAS targets. These feed data to the Cortex Integrated Combat System, which controls a Kongsberg Protector RS4 remote weapon station (RWS). The CORTEX Typhon will be mounted on Dingo 2 MRAPs provided by the Norwegian Army, which is also supplying the RWS units.

"The IFU was established by the UK and international partners to identify and procure critical capabilities and deliver them quickly to Ukraine. Norway and the UK are among many nations that have contributed to the fund," a Kongsberg official explained. Kongsberg has also provided Ukraine with the National Advanced Surface-to-Air Missile System (NASAMS), which includes a command post, sensors, radar and munitions that can be fired from a stand-alone pod or from the back of a truck as part of a short to medium range ground based air defense system. In November 2022, Ukraine received its first NASAMS, which was deployed to protect the capital city of Kyiv from Russian UAS and missile threats.

Russia's Lancet one-way attack drones have proved effective at targeting Ukrainian forces. NICKEL NITRIDE PHOTO

"Fixed sites often use air defense systems like NASAMS for C-UAS because they can see those attacks coming from further away and defeat those threats, large and small," the company official said.

Kongsberg has also provided "hundreds" of remote weapon stations (RWS) to NATO allies in the the Czech Republic, Germany, Lithuania, Poland, Romania, Slovenia and the UK, many of which support C-UAS protection of fixed sites. "Kongsberg is providing C-UAS solutions for a number of customers, and each one is slightly different to address unique requirements," the company official explained. "As a provider of RWS, we have the software, engineering and manufacturing expertise and can add C-UAS capability to those systems by incorporating the Cortex ICS [Integrated Combat Solution] – it doesn't need to be part

Military Bases and re from Drones

of a new, separate system. And that is the same architecture at the heart of NASAMS. That common lineage allows customers to use Kongsberg›s larger systems and architecture so there can be collaborative engagement between Kongsberg RWS and NASAMS, providing a more wholistic approach to airborne threats," the Kongsberg official continued.

SENTRY TOWERS

On October 29, the UK's Ministry of Defence (MoD) awarded Anduril Industries a £17 million contract to deploy "Counter-Intrusion/Counter-Drone" solutions across permanent joint operating bases in Europe and further afield. According to a company statement, Anduril is working alongside the MoD's "jHub" Joint Innovation Team to protect bases against "changing and evolving" threats as part of a wider force protection strategy. The 31-month contract will explore "future capabilities for fixed installation force protection and counter-intrusion and C-UAS for the Royal Air Force [RAF] and Strategic Command on Permanent Joint Operating Bases (PJOBs)", according to the statement. The contract, which could be extended to a total sum of £24 million, is part of Anduril's TALOS program which aims to "accelerate a defense-wide approach to Integrated Command and Control [C2] for force protection," a company official said.

Specifically, TALOS includes Anduril's Lattice software platform, which supports autonomous applications, edge processing, big data and artificial intelligence to provide the customer with capability to harness machine-speed in decision-making. It will also help to integrate all defense-wide platforms, sensors and effectors into a single network.

The jHub will benefit from the third phase of TALOS – referred to as "Entrelazar" – which is exploring advancements in key technologies to "inform decisions on the integration of future capabilities into defense-wide platforms," the company said in a press release. "Phase 1 of Programme TALOS delivered an initial understanding of Anduril›s autonomous Sentry Towers and their utility at active RAF air bases, and Phase 2 introduced the assurance of multiple force protection layers at multiple locations across the MoD estate. This contract focuses on continuing the capability layering in Phase 2 and informing the requirements across multiple MoD sites. It will progress and expand experimentation with mature integrated technologies, and enable further understanding of the various options available in the wider C2 network that can provide end-to-end solutions."

Anduril's solution was demonstrated to the MoD at the UK's Cranfield Ordnance Test and Evaluation Centre in October, illustrating how TALOS could support the UK MoD as "threats evolve and the UK faces new multi-domain security challenges", according to company officials.

Anduril director Tristam Constant explained how Lattice software and a suite of Android products cooperated to provide comprehensive force protection at a base location. As an "unfriendly" vehicle entered the monitored space, it was autonomously detected and tracked by Anduril's Standard Range Sentry Tower (SRST). Anduril's Long Range Sentry Tower (LRST) then detected and tracked a second "non-cooperative" UAS threat (which was launched by the same pilot) using Wide-Area Infrared System for Persistent Surveillance (WISP) cameras that also contributed to a "comprehensive picture of the threat scenario," Constant explained. "Upon determining the [second] UAS as a suspected threat, we tasked the [Anvil] interceptor drone to launch and track [it] through the air and then quickly make a kinetic impact," he continued before describing how the SRST then handed off tracking of the pilot to Anduril's Ghost UAS which "freed up" the sentry tower to continue searching for additional threats. Neither Anduril nor the MoD was able to comment on which operating bases would be protected by the TALOS solution.

AROUND THE CLOCK

Securing bases and installations against UAS intrusions drives a slightly different set of requirements compared to mobile C-UAS applications. Chris Abraham, VP of marketing for CRFS, said the most important requirements facing armed forces in terms of fixed site C-UAS is the ability to run autonomous operations on a "24/7" basis. CRFS provides ESM and SIGINT solutions, including for C-UAS applications, based on its RFEye family of receivers and software.

Abraham highlighted the importance of being able to detect, track and neutralize a wide range of threat types ranging from commercial off-the-shelf (COTS) UASs (quad-copters and other mini-drones) through to medium-altitude/long-endurance (MALE) and other "modified" UAVs. Furthermore, he explained how C-UAS solutions must also minimize false positives and provide maximum reach in terms of range, allowing end users to detect and geolocate threats at the earliest opportunity to support better decision-making, enable the response chain and cue other sensors if necessary. Finally, Abraham described how any modern C-UAS solution must be easily integrated into a wider C2 platform and contribute to a common operating picture that can be updated in near real-time.

Abraham was unable to comment on CRFS's customer base, but the company has received several contracts from the US Air Force and NASA for base and installa-

tion security. He did say, "We have solved a lot of the common deployment and capability gaps due to an iterative development that›s taken place over the past five years, driven by real field experience. But urban deployments remain a key challenge for all sensors and systems in this field." He also described a trend away from C-UAS solutions focused mainly on ISM [radio] bands to newer requirements for wider frequency sensing capabilities, which he believes are better suited to detecting and tracking MALE and modified UAV threats. He added that solutions must also be capable of dealing with multiple targets and swarms simultaneously, which CRFS solves via real-time passive RF sensing to geolocate drone and operator emissions; 3-D positioning (latitude, longitude and altitude); and high probability of intercept on drone command and datalink signals.

In addition to detecting, identifying and geolocating a drone, another emerging military requirement includes capacity to accurately geolocate the position of a pilot or ground control station. "Most clients state this is a useful capability, but the detection and geolocation of the drones remain top priority, as they pose the most significant threat," Abraham said. "CRFS systems can perform detection and geolocation of both the controller and drone(s)."

Finally, Abraham described how C-UAS sub-systems must be easily integrated into third-party C2 systems: "Clients can use our user interface to drive the workflow and then a simple geolocation streaming service (using industry standard protocols)," he said, "or they can use a fully documented and open [API] to allow complete integration and fusion of the CRFS element into the C2 system. The most recent work has been to utilize 'best of both worlds' with multiple antenna types to greatly enhance detection and geolocation range, even against lower powered COTS drones," Abraham added, before describing ongoing innovations to deploy sensors on "drone-based platforms to massively increase operational range and operational flexibility."

MEETING EMERGING C-UAS REQUIREMENTS

MBDA's director of future systems, Bruno Verzotti, said European armed forces require "next-generation sensors" to be integrated into existing C-UAS networks to defend against saturated attack by swarms. "If a company provides C-UAS, in six months it will be obsolete because the enemy will find a way to get around it," he said. "Customers have to understand if they just have the same [C-UAS] solution, it will just have the same answers."

ARDRONIS is offered in multiple variants that can provide detection and DF of the drone pilot, as well as jamming and control of the command link. ROHDE & SHWARZ PHOTO

Instead, Verzotti said MBDA and its partners need work in a "very different way." "We are already doing this with our French [MoD] customer, so we are facing these challenges in a totally new way and delivering capability from a blank sheet of paper in just four years," he explained. As an example, Verzotti described how the MBDA is supporting the French Government's C-UAS mission at the Olympic Games in Paris this summer. This solution, he said, will feature Cilas's Helma-P high energy laser in a C-UAS role.

Verzotti also said malicious or non-cooperative UAS should be safely neutralized to avoid collateral damage – a particular threat when protecting military bases or infrastructure in densely populated areas. "In some situations," he explained, "if we see a UAS with a weapon on it, we don't want to destroy it where it is. So instead we went to industry for good ideas to capture [the command signal of] a UAV and bring it to a selected area," he said.

"We launched a call for ideas and selected seven concepts, and by the end, one of them looked ready for next year and efficient enough for us to acquire a few sets of UAV catching systems. This is a new way of working – we explained what we wanted to achieve but didn't know how to do it, so [we] approached industry and they were able to help," Verzotti concluded.

In Italy, ELT Group is taking a "system of systems" approach to modern C-UAS requirements, a company official said, enabling customers to face different threats in different operational situations and environments. "The paradigm C-UAS systems adopt is 'detect–recognize-defeat', always including evaluation by an operator," the official explained. "This means that the sub-systems employed in the C-UAS system must be capable of performing the entire sensor-to-shooter cycle according to the operational situation and the configuration in place. The most important requirement for a C-UAS system is to detect at the maximum possible distance in order to allow enough time for the operator to put in place the appropriate countermeasure. In terms of countermeasures, recent conflicts highlight how the defeat phase is shifting fast from a pure EW countermeasure to a combination of soft- and hard-kill," the official explained. "Many customers require the kinetic effector to be present and integrated in the system in order to grant the operator a wider choice of countermeasures based on rules of engagement or the current operational situation."

ELT Group's C-UAS offerings include the Anti-Drone Interception Acquisition Neutralization (ADRIAN) system – a completely scalable system that can be deployed from a shelter to protect bases. "Configurations, if required by the end user, integrate third-party subsystems including a kinetic one," the official added, before suggesting ADRIAN is "extremely effective against mini- and micro-drones. The challenge is having the same effectiveness also against class II [UAS]. Air defense systems cannot be so distributed on the ground as a C-UAS system, so protecting troops and population will be a C-UAS system priority thanks to a massive distribution on the ground and an efficient C2 system."

Developing the ability to identify the position of a UAS pilot continues to play a critical role in emerging C-UAS capabilities. "Having the position of the pilot helps to identify launch areas so they can be better monitored in the future to prevent further attacks," the company

official said. "But at the other end, it is extremely difficult to capture a pilot, considering that mini-/micro-drone attacks typically last anywhere between 40 and 90 seconds."

Looking to the future, the ELT Group official described how the threat of malign and non-cooperative drones continues to evolve very quickly. "New conflicts have [depended on] the concept of the 'Forward Operating Base.' Military bases will be part of the area of the battle, which means they may or may not necessarily be in contact. Scenarios are also moving to the urban area, forcing everybody to change operating paradigms. The challenge is to have modular, scalable and integrated systems that can be easily adapted to any kind of scenario. Our team is constantly scouting new solutions able to face new threats. At the moment, we are pursuing the extension of the capability of ADRIAN in order to be effective also against small UAS and Class II UAS, integrating C-UAS capability into our Tactical EW System (TEWS)."

"As technology moves forward quickly," the official added, "ELT Group is also diving into other technologies in the cyber domain. We are talking about 'Cyber RF,' which constitutes a complement to jamming, radar and visual modules which further enhances performance by forcing a 'safe landing' or diverting a threat. This capability is an example of using the electromagnetic spectrum for cyber operations and supporting a broader Cyber Electromagnetic Activities (CEMA) capability."

In Germany, Rhode & Schwarz continues to press ahead with capability extensions to its family of C-UAS solutions which have been in service with the Bundeswehr since 2020. The company's "ARDRONIS" family is offered in four basic configurations. ARDRONIS-I performs detection of frequency-hopping spread spectrum (FHSS) command signals from a ground pilot to a drone. In ideal conditions, the system can detect command signals on some COTS drones up to 7km away and DJI Phantom drone signals at ranges up to 4-5 km. ARDRONIS-D adds a direction finding (DF) capability to locate the drone pilot. Two variants, ARDRONIS-R and ARDRONIS-P provide countermeasures capabilities that disrupt the drone's command link.

ARDRONIS can also be integrated with other C-UAS systems. The ARDRONIS DF system plays an integral role in the Bundeswehr's "Guardion" or "ASUL" C-UAS system – a collaborative effort with ESG and Diehl designed to support "field camp protection in deployment areas," a company statement confirmed.

As described by the company spokesperson, "The drone defense solution can detect and prevent unauthorized situations with UAVs by continuously monitoring the frequency bands used by UAS remote controls and generating an alert when a remote control is activated. This gives security personnel the earliest possible warning, saving valuable time for clarifying the situation." ARDRONIS uses an emitter library to identifiy the manufacturer and type of commercial drones and their remote controls, and it determines the direction of its signal.

The two jamming variants of ARDRONIS disrupt remote control signals received by the UAS, which typically forces it to engage a failsafe mode and stop flying. "This only disrupts the control signals of UAS previously identified as unauthorized, without affecting other radio links in the same frequency band," the spokesperson stated. "Relatively large areas can be covered by two or more networked DF stations, allowing drones and remote controls to be located and their positions displayed on a digital map." The ARDRONIS family of systems is also capable of integrating with kinetic effectors, although the company was unable to comment on any such integration to date.

OPEN ARCHITECTURE APPROACHES

In September, Rohde & Schwarz's latest ARDRONIS variant – Locate Compact – was one of 70 C-UAS systems and related technologies that participated in NATO's C-UAS Technical Interoperability Exercise (C-UAS TIE23) in Vredepeel, the Netherlands. At the event, UK officials announced that NATO would adopt the UK MoD's Sensing for Asset Protection with Integrated Electronic Networked Technology (SAPIENT) open architecture and protocol as a NATO standard (pending a formal agreement among members). SAPIENT will support greater interoperability among C-UAS sensors, countermeasures and C2 systems, essentially enabling "plug and play" C-UAS solutions to be rapidly fielded and upgraded. At C-UAS TIE23, Rohde & Schwarz demonstrated that Locate Compact is "fully compliant" with SAPIENT.

NATO evaluated 70 C-UAS systems and technologies at its C-UAS TIE23 exercise in September. NATO PHOTO

Due to the large number of available sensors, effectors and C2 systems, open architectures are not only desirable but are essentially becoming a requirement for fixed-site C-UAS applications. Leonardo UK's campaign manager for C-UAS, Ben Hewitt, suggested scalability and modularity remain the most critical requirements for the protection of military bases. "The ongoing conflicts in eastern Europe and the Middle East have highlighted the use of UAS in surveillance, fire control and attack roles, which has highlighted the imperative need for a C-UAS solution for fixed sites and mobile assets," he explained. "No two sites are alike, in either geography or threat profile. The ability to amend a sensor and effector lay-down will ensure that the solution is suited to the threat, but the ability to develop this solution is also key, as we have seen the use of UAS increase alongside the developing technology. A solution that utilizes open architecture standards is also very important, because drone threats are rapidly evolving. You cannot expect your current solution to meet the threat context and performance levels in the long term, as the threat continues to diversify and update. It is crucial to be able to evolve your system to outpace the threat, drawing on new and emerging technologies as they become available."

Leonardo is currently under contract to the UK and Italian armed forces providing its Falcon Shield C-UAS solution – a rapidly deployable, scalable and modular system designed to address the threat from "low, slow and small" UAS, as well as OWA drones. The system uses 3D radar and ESM sensors to provide 360-degree coverage, EO trackers, and RF jammers to defeat drones.

"Elements of Falcon Shield equipment were notably operated by the RAF Force Protection Force in 2018 and 2019, following drone sightings at Gatwick and Heathrow airports, allowing airport operations to resume," Hewitt confirmed before also describing how four baseline "ORCUS" C-UAS solutions (based on Falcon Shield) remain in service with the RAF. "ORCUS is playing a key role in the RAF›s wide-ranging 'Synergia' research and development program, managed by Defence Equipment & Support›s Future Capability Group," he said. "ORCUS is also being maintained as a national standby capability, able to rapidly respond to a drone-based crisis anywhere in the UK in support of Emergency Services. UK and US Armed Forces are collaborating on fixed site C-UAS through the Synergia program, and ORCUS system operators have already shown the capability of the system. The ability to detect dozens of small drone platforms in the airspace around airbases and then mitigate them has been aptly demonstrated."

According to Hewitt, one of greatest emerging threats challenging the C-UAS mission is the proliferation of low, slow and small UAS, which are typically undetectable by conventional air surveillance equipment. "This is where Falcon Shield comes in," he said. "The system has performed admirably on a range of operations throughout the UK and further afield, and the agile nature of Falcon Shield means we can integrate sensors at a moment›s notice to stay ahead of the threat." Hewitt also stressed the importance of geolocating drone operators, but warned that in operational environments armed forces were now seeing more deployment of autonomous UAS flying on way points or other navigational aids and therefore avoiding detection via a their C2 link.

In terms of effects, Falcon Shield is capable of supporting an electronic attack capability, designated as "Guardian," which according to Hewitt can deny, disrupt or defeat UAS C2, navigation and UAS data downlinks. "In addition, as part of the UK and US Armed Forces' continued collaboration on counter-drone research and development, Leonardo has integrated the US Air Force›s NINJA [Negation of Improvized Non-State Joint Aerial threats] technology into the RAF›s ORCUS counter-drone system. "Developed by the US Air Force Research Laboratory, NINJA can electronically take command of a hostile drone. Its integration into ORCUS provides another tool for operators to defeat rogue drones. Guardian provides a long-range 'electronic sniper rifle' jamming effect, while NINJA provides a similarly surgical cyber effect at a shorter range, which can take control of a drone›s command protocols and maneuver it to a safe location."

The RAF's ORCUS C-UAS system (left) is based on Leonardo UK's Falcon Shield.

RAF PHOTO

Hewitt also stressed emerging C-UAS requirements for more hard-kill countermeasures to complement RF jamming. "Leonardo has integrated a number of different kinetic effectors developed by our industry partners ranging from missile systems to a 30-mm cannon," Hewitt said. "All of these means of mitigation provide an effective layered defense. The development of both kinetic and non-kinetic mitigation continues, including exploitation of other CEMA techniques to counter more complex threats."

In terms of Falcon Shield's integration into C2 systems, Hewitt described how Falcon Shield is representative of Leonardo›s wider approach to create a more connected battlespace where multi-domain integration is underpinned by secure cloud technologies, data and analytics. "By integrating sensors and products from across domains and making better use of data, it is possible to augment the human decision maker and enable faster and better decisions. For example, Falcon Shield's built-in Geospatial Information Systems enable the accurate geolocation of a threat, which can then be handed off to an effector, countermeasure or external actor, potentially in another domain."

Finally, Hewitt shed some light on how the company is seeking to upgrade its C-UAS solutions in the future. "Falcon Shield's open framework enables the system to be tailored and optimized to meet the demands of various locations, threats and end-user concepts of operation as both a fixed-site and mobile capability. This will remain the case as all of these continue to change in the future. Fixed-site protection is not all going to be about C-UAS, although this will play a major part," he said. "The future of fixed-site protection is going to be based around a multitude of sensors monitoring all aspects of defense on land, in the air and electromagnetic spectrum. The future is an ever-growing capability fused into common C2 [architecture] reducing operator workload supported by AI. All this information will be accessible throughout the operating environment, ensuring that the threats are mitigated as and when required with the appropriate oversight specific to the operational environment."

The drone threat is growing in complexity, as industry creates more UAS capabilities and as military users develop more sophisticated tactics to employ them. C-UAS solutions are keeping pace with these developments through new technologies, open architectures and standards, and from developing solid requirements gained through user experience. Protecting bases and fixed sites from drones may become more challenging, but so far the C-UAS mission is proving equal to the task.