International Conference KNOWLEDGE-BASED ORGANIZATION
Vol. XXX No 1 2024

COUNTERING UNMANNED AIRCRAFT SYSTEMS – A MULTI-DOMAIN EFFORT

Constantin GRIGORAȘ, Octavian-Ștefan MUȘAT

"Nicolae Bălcescu" Land Forces Academy, Sibiu, Romania
grigoras.constantin@armyacademy.ro, octavianmusat@yahoo.com

Abstract: *In the last decades, the proliferation of the unmanned aircraft systems (UASs) has altered the modern battlefield and the need to counter these inexpensive, flexible, and expendable systems has become paramount. UASs come in a variety of sizes and capabilities, the larger ones may achieve effects compared to a cruise missile and the smaller systems are difficult to detect as they manoeuvre across the battlefield in order to successfully conduct tactical-level strikes. So it is a must to understand that countering this kind of threat is a shared and joint responsibility and the approach has to be a comprehensive one, covering a broad spectrum of military, civil and legal perspective on this subject matter. Moreover, as it is clear that there is a need to employ multi-domain solutions to nullify the UAS threat, nations should aim to achieve technical interoperability and standardization given by a common doctrine and operating procedures.*

Keywords: UAS, C-UAS, drone

1. Introduction

Unmanned Aircraft Systems (UAS) now play a vital role in NATO operations, evolving into a crucial asset for Intelligence, Surveillance, and Reconnaissance (ISR) tasks, as well as for combat missions [1].

However, other state and non state actors, among which the declared enemies of NATO have struggled to develop similar types of systems in order to gain an advantage in the air domain. China, Russia and Iran have invested a lot in creating and producing UASs and their state of the art models have similar characteristics as the Western products.

At the same time, the civilian market is focusing on small UASs, used by the public for recreational purposes and these flying objects are known as Commercial-Off-The-Shelf (COTS) drones. The latest iteration of COTS technology is capable of autonomous flight to designated coordinates or can be remotely controlled through a Global System for Mobile Communications (GSM) network using the operator's mobile phone [1].

A 'traditional' countermeasure against an UAS is the electronic jamming of the Command and Control (C2) link. The GSM network and the autonomous flight make the jamming ineffective so there is a need for a new approach in countering these emerging technologies.

2. Understanding the Components of an UAS

In order to counter the UAS threat, it is important to understand that we have to see the bigger picture, not only the Unmanned Aircraft (UA) or 'drone'. UASs are composed of several components depending on their size and mission. In contrast to a small UAS, which typically consists of an operator, a remote control, a

DOI: 10.2478/kbo-2024-0011

command and control link, and the aircraft itself, a larger system additionally necessitates a specialized land-based control system for launching and recovering the aircraft. Often, it also requires a mission control element to execute specific operations [1]. Moreover, these systems may use space based beyond line of sight (BLOS) communications for the datalinks and command and control. In conclusion, the systems requires, in addition to an aircraft, more physical infrastructure like buildings, containers and hardware /software to control the flight and engagements and the bigger the UAS is, the larger need for land based support.

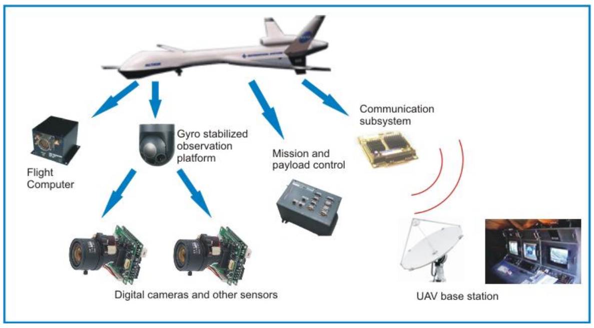

Figure 1: Main components of a UAS Source: Enric Pastor, Juan Lopez and Pablo Royo. UAV Payload and Mission Control Hardware/Software Architecture. Aerospace and Electronic Systems Magazine. July 2007

3. UAS/C-UAS in the Ukraine Conflicts

The war in Ukraine is thus not “the first drone war”. This isn't the initial conflict where drones hold significance, nor is it the first where both opposing forces utilize them. However, their deployment in Ukraine signifies a notable shift. Never before has there been such extensive use of drones in a military standoff [2].

Among the observations from the Ukrainian Crisis in 2014 one is that Russia made use of UASs as Intelligence Surveillance Target Acquisition and Reconnaissance (ISTAR) assets in a very effective manner. By integrating multiple sensing platforms at different altitudes over the same targets, Russia succeeded in providing a real-time targeting system with complementary imaging while keeping the fire units at a safe distance. It is also worth to note that Russia used Electronic Warfare (EW) and Cyber in a C-UAS role very effective as most of the small number of Ukraine drones were jammed and downed.

Between 2015 and 2022, the UAS capabilities were enhanced by both parties involved in the conflict as they were fighting trench warfare in the East of Ukraine. Russia started the weaponization of small octocopters, using them to drop incendiary grenades but was blocked in having hands on key technologies by the sanctions imposed by the West. On the other hand, Ukraine initially used the commercial drones to do target acquisition for mortars and artillery but they benefited from the western training so it was a huge built-up of experience as well as investments and developments of drone technology.

In the Eastern Ukraine resistance movement, civilian UAVs play a crucial role in confirming enemy positions and intentions, as well as carrying out sabotage by deploying simulated weaponry against enemy forces. These direct actions prove highly effective due to their rapid decision-making process, reliable target verification by the UAVs, and immediate engagement with the identified targets [9].

As per the open-source intelligence outlet Oryx, between February 24, 2022, and September 13, 2023, there were 300 confirmed losses of Russian reconnaissance and combat UAVs in Ukraine, verified through photographic or video evidence. Among these losses were 183 instances of Orlan-10 drones and their variants, thirty-eight Eleron drones, thirty-eight Zala drones, six Orion drones, six Forpost drones, and several others.

The Ukrainian Armed Forces' general staff reported that Russia suffered losses of 4,650 drones of various types. This includes numerous Iran-made Shahed drones, classified as loitering munitions, along with potentially some commercial drones utilized extensively alongside military-grade ones by the Russian armed forces. The exact number of drones Russia lost on Ukrainian occupied territories due to technical malfunctions and human errors remains uncertain. Additionally, the count of small commercial drones, such as DJI Mavic and others, provided by Russian regional administrations and volunteers, that have been lost, remains unclear [2].

Figure 2: Orlan-10 jamming UAV captured Source: Oryx, "Attack on Europe: Documenting Russian Equipment Losses during the Russian Invasion of Ukraine" February 24, 2022

Recent advancements in the drone conflict in Ukraine indicate that Russia is employing Shahed attack drones, also referred to as "kamikaze" drones, to target population centers and power stations, aiming to disrupt Ukraine's electricity and heating supply. In response, the Ukrainian armed forces have employed various countermeasures, including small arms fire, heavy machine guns, portable anti-air missiles, and electronic jamming devices, to intercept these drones. However, shooting down drones becomes challenging when they are deployed en masse, or in "swarms" [2].

As general takeaways from the war in Ukraine we can say that the local air supremacy is something of the past, the drone threat is now on the lowest tactical level, so C-UAS capabilities need to be fielded at the lowest tactical level.

4. C-UAS - a NATO Perspective

NATO Defence Ministers endorsed in February 2019 a practical framework for countering Class I UAS. On 9 July 2021, under silence procedure, the NATO C-UAS working group work programme was approved with the intent to create a NATO C-UAS doctrine.

The idea is to focus the doctrine at operational level, while leaving in depth strategical and tactical elements to other following publications. The doctrine will cross boundaries between multiple functions such as Force Protection and Air Defense.

It is important to note that the NATO Counter Class I Doctrine will ensure connection and coherence with other doctrinal documents; in particular the interaction / de-confliction between C-UAS assets with hostile, neutral and friendly operations such as air operations and electromagnetic operations. It will also take into consideration the interaction and interoperability and authorities coordination with NATO Integrated Air and Missile Defense (IAMD) and in particular with Surface Based Air and Missile Defense (SBAMD) capabilities [3].

At the Defence Ministers Meeting held in Brussels on Thursday, October 12, 2023, NATO allies deliberated on the subsequent actions required to operationalize the alliance's new defense strategies. This included the allocation of forces, the advancement of novel capabilities, and adaptations to command and control structures [4]. So it is crystal clear that NATO is preparing to adopt the C-UAS doctrine in the near future.

NATO is not only working on a doctrine but it also focusing on exercises with the intent to boost technical interoperability and to increase the ability to counter UASs. NATO organized the Counter Unmanned Aircraft System Technical Interoperability Exercise (C-UAS TIE23), which convened military, scientific, and industry experts to evaluate advanced commercial solutions for detecting, identifying, and mitigating drone threats. Approximately 70 systems and technologies, including sensors, effectors, jammers, and live threat drones, underwent live testing. The objective was to verify that these cutting-edge solutions could swiftly connect and collaborate effectively. The exercise was coordinated by the NATO Communications and Information Agency (NCI Agency) and hosted by the C-UAS Joint Nucleus under the Dutch Ministry of Defence [5].

Figure 3: An Autel Evo Max UAV and a DJI Matrice quadcopter flying above a General Dynamics Land Systems LAV700 vehicle at C-UAS TIE23
Source: Janes/Olivia Savage

In conclusion, NATO has taken important steps in managing the UAS threat and the organization's first aim is to prevent by focusing on laws, regulations, using warning signs and gathering intelligence. The next step is to have situational awareness and to be able to detect, track, classify and identify the threat. Then it must move to the respond phase and be able to deter, defeat destroy or capture. Last but not least, an UAS threat protection system should be able to take the necessary post event actions like recover, exploit or assess.
The future researches will encompass the incorporation of practical UAS integration solutions that have been thoroughly tested and confirmed. An implicit objective is to include a set of recommendations that will be scrutinized concerning the direct impact of UAS integration on various aspects, such as force structure, decision-making processes, standardization, training, and personnel specialization. Additionally, it will explore how this integration contributes to the collective efficacy in military operations against adversaries, encompassing both defensive and offensive strategies [10].

5. A Multi-Domain Approach in Countering UAS

5.1. Defensive Counter-Air Operations

Surface Based Air and Missile Defense (SBAMD) systems are designed to protect the assets against air breathing targets, cruise missiles and ballistic missiles. Many unmanned aircrafts have similarities with the manned systems so certain SBAMD systems may be used to counter the unmanned aircrafts. However, the traditional Air Defense has some limitation especially against small systems.
Contemporary air defense radar sensors can target smaller unmanned aircraft. Yet, as unmanned aircraft decrease in size and the range shortens, it becomes increasingly practical and necessary to employ specialized sensors designed specifically for detecting these targets. Additionally, emitting radio frequency (RF) energy heightens the vulnerability of the SBAMD unit [1].
Moreover, SBAMD interceptors, especially long range ones like PATRIOT and THAAD are expensive so employing them is not cost-effective.
As a takeaway from the analysis on the employment of the traditional AD we can say that there is a need of adaptation of the SBAMD systems in terms of sensors, effectors and command and control requirements. The future AD systems must rely more on passive sensors, airborne sensors and cheaper interceptors.

5.2. Offensive Counter-Air Operations

When we plan how to counter an UAS, the first thought is to shoot it down while flying. But what if we could prevent it from being launched by affecting the components of the systems on the ground? This is achievable using Air Interdiction (AI) operations.

AI refers to air operations aimed at diverting, disrupting, delaying, degrading, or destroying an adversary's military capability before it can be effectively deployed. These operations typically occur at a distance where detailed integration of each air mission with the movements of friendly forces is not typically necessary [6].

Disrupting or neutralizing any component of the UAS, such as launch and recovery units, Ground Control Stations, Communications Equipment, Logistics, and Supporting Systems, will ultimately hinder the operations of the UAS.

5.3. Electromagnetic Operations

Among the active measures against UAS for Electronic Warfare (EW) are jamming and deception. Jamming is conducted by directing a high amount of energy towards the UA to mask the radio frequency control or data signals. When it comes to deception, it involves the manipulation of the UAS behaviour by using a signal with a different content and directing it towards the control station.

Figure 4: U.S. Marine Corps tests Drone Killer Counter-UAS Technology Source:https://www.military.com/daily-news/2020/01/15/new-pentagon-team-will-develop-ways-fight-enemy-drones.html

Another method that has already been tested is the use of directed energy weapon systems such as high energy lasers, electro-magnetic pulse and high-power microwaves systems. The United States Airforce, Navy, Marine Corps and the Army are running several projects that involve the use of directed energy weapons. The Air Force has stationed a 15-kilowatt (kW) vehicle-mounted C-UAS system known as the High-Energy Laser Weapon System (HELWS) in locations outside the Continental United States (OCONUS). HELWS is designed to rapidly detect and eliminate hostile or unauthorized UAS within seconds. Additionally, when linked to a generator, HELWS can deliver "a nearly unlimited number of shots," as stated by Raytheon, the developer of HELWS [7].

5.4. Cyberspace Operations

The Cyberspace Domain can be delineated into three main interconnected layers: a physical layer, a logical layer, and a cyber-persona layer. The physical layer encompasses Information Technology (IT) hardware, equipment, and networking infrastructure utilized for data processing, storage, and transmission. The logical layer consists of interrelated yet abstract elements like data, operating systems, applications, network operations, and protocols. Lastly, the cyber-persona layer constitutes a digital representation of an actor or identity formed by the data and regulations of the logical layer [8].

The use of cyber operations as a C-UAS method is not focusing on the unmanned aircraft in the air but is influencing the components of the system that are located on the ground. For instance some cyber operations may be oriented to target the drone operators. Certain operators may become targets through their social media profiles or email accounts, either to manipulate their actions and choices or to infiltrate malware into the Unmanned Aircraft Systems (UAS) [8].

Another way to use cyber domain as C-UAS is to try to hack or interrupt the communication data link and capture or force the flying unmanned aircraft to return to the launching position. As the 5G network is becoming more and more actual, and the future drone threat will also include swarms of drones controlled by artificial intelligence, the only feasible C-UAS method to address these challenges seems to belong to the cyber domain.

5.5. Space Operations

Some UASs require specific services provided by space capabilities. Among these services we can identify space-based positioning, navigation and timing (PNT) from Global Navigation Satellite Systems (GNSS) and satellite communications (SATCOM).

The countermeasures against enemy space assets that are supporting UAS consist of physical attacks and non physical attacks. The physical countermeasures aim to destroy the space satellites using anti-satellite missiles or to destroy the ground stations of the space assets.

Figure 5: MiG-31BM "Foxhound" aircraft is carrying what has since been identified as a potential anti-satellite weapon. Source: shipsash / jetphotos.com

Non-physical attacks aim at disrupting the means of transmission by interfering with the signals constituting the link segment. This interference can occur through jamming or spoofing techniques and typically lasts for a limited duration.

NATO is in competition with its potential adversaries in the Space Domain Countries like China, Russia, Iran and North Korea have developed or have laid the foundation for counter space weapons so the space will be very contested in a future conflict.

6. Conclusions

The UAS threat is very actual as the recent conflict in Ukraine has shown since it was extensively used for both acquiring intelligence and conducting deep strikes into the enemy territory. It is proven to be a versatile weapon and cost effective in relation with the actual countermeasures and the effects inflicted.

To counter the UAS threat, NATO and partners need to coordinate the efforts in order to be effective and the task of fighting with this type of systems does not belong to the Air Force only. This fight must encompass various domains like Air, Land, Maritime and especially Cyber and Space.

The coordination has also to be implemented at all levels starting with the strategic level where there is a need for inter-agency, civil-military, multi-national, whole of government approach. Then, at operational level, the C-UAS mission must be integrated seamlessly within different communities and integrate all relevant capabilities and at the tactical level it is paramount to reach the highest level of interoperability in order to avoid blue on blue effects.

Last but not least, the C-UAS must be addressed as a capability gap into the capability codes and this lack of specialized assets must be covered by finding resources for procurement and training.

References List

[1] The Joint Air Power Competence Centre ”A Comprehensive Approach to Countering Unmanned Aircraft Systems” Available from: https://www.japcc.org/books/a-comprehensive-approach-to-countering-unmanned-aircraft-systems/

[2] “Attack On Europe: Documenting Russian Equipment Losses During The Russian Invasion Of Ukraine,” Oryx, February 24, 2022, Available from: https://www.oryxspioenkop.com/2022/02/attack-on-europe-documenting-equipment.html.

[3] NATO Integrated Air and Missile Defence Available from: https://www.nato.int/cps/en/natohq/topics_8206.htm

[4] Defence Ministers address deterrence and defence, NATO missions, situation in the Middle East, Available from: https://www.nato.int/cps/en/natohq/news_219120.htm

[5] NATO tests counter drone technology during interoperability exercise Available from: https://www.ncia.nato.int/about-us/newsroom/nato-tests-counter-drone-technology-during-interoperability-exercise--2.html

[6] AJP-3.3 Allied Joint Doctrine for Air and Space Operations, Edition B Version 1, April 2016

[7] Thomas Gnau, ‘The Air Force just fielded its first high-energy laser weapon overseas’, Dayton Daily News, 6 Apr. 2020. Available from: https://taskandpurpose.com/military-tech/air-force-laser-weapon-fielding

[8] US Department of Defense, Joint Publication 3-12, ‘Cyberspace Operations’, 8 Jun. 2018, I-2. Available from: https://fas.org/irp/doddir/dod/jp3_12.pdf.

[9] Constantin-Adrian CIOLPONEA, “The Integration of Unmanned Aircraft System (UAS) in Current Combat Operations”, Revista Academiei Forţelor Terestre nr. 4 (108)/2022

[10] Constantin-Adrian CIOLPONEA, Ghiţă BÂRSAN “NATO Corps HQ – Land Component –Integration of Unmanned Aerial Vehicles (UAVs)”, Revista Academiei Forţelor Terestre nr. 4 (108)/2022