MQ-9: © Digital Storm/shutterstock, Quadcopter: © sdecoret/shutterstock

A Comprehensive Approach to Countering Unmanned Aircraft Systems

And Why Current Initiatives Fall Short

1 Introduction

Over the last decades, Unmanned Aircraft Systems (UAS) have been fielded in every military service, ranging from handheld micro-UAS to medium-sized tactical systems to fully grown and Remotely Piloted Aircraft (RPA). At the same time, the civilian market has witnessed an exponential growth of predominantly smaller systems intended for public and recreational use. However, the latter use case has gained the attention of law enforcement agencies and military force protection communities due to the increased misuse of Commercial-Off-The-Shelf (COTS) 'drones' near and over airports, public events and military installations.

Recently, various industry players reacted to the emerging demand for capabilities to defend against these COTS UAS by developing Counter-UAS (C-UAS) sensors and effectors. These systems are specifically designed to detect, track and engage Low, Slow and Small (LSS) flying objects, ranging from man-portable systems such as 'Droneguns'[1–3] to truck-mounted models such as the 'Silent Archer'[4]. NATO also reacted to this new threat by conducting a series of studies centred on defence against LSS air threats [5–7] and by establishing a C-UAS Working Group with a focus on terrorist misuse of UAS.[8]

However, technology is developing rapidly, in many cases, faster than the defence industry or NATO can react. For example, many 'traditional' countermeasures against small UAS rely on electronic jamming of the command and control link between the 'drone' and its remote control. Many current COTS products are, however, able to navigate autonomously to a given coordinate or can be controlled via a GSM network from the operator's mobile phone. These features make jamming either completely useless, since the Command and Control (C2) link is no longer required to navigate, or, because of peacetime restrictions, the frequencies that need to be jammed are often off limits, as they are used by the public.

Additionally, a sole focus on the low, slow, and small end of the C-UAS spectrum covers only a fraction of current UAS technology and excludes most military applications. Peer competitors to NATO can be expected to employ UAS at the same level of technology, and under comparable operational principles, as in the Alliance. Consequently, NATO has to anticipate enemy use of UAS in the same mission sets as with friendly UAS, covering the spectrum from Intelligence, Surveillance & Reconnaissance to unmanned airstrikes, conducted in Line of Sight (LOS) as well as Beyond Line of Sight (BLOS) operations, utilizing the electromagnetic spectrum and the space domain in the same way as NATO.

The following sections briefly describe a spectrum of C-UAS considerations and why the current focus on the low, slow, and small end, although imminent and essential, is not sufficient to cover all aspects of defence against potential adversary UAS engagements.

2 The Spectrum of Countering Unmanned Aircraft Systems

To understand the full spectrum of countering UAS, it is important to note that exclusively focussing on the Unmanned Aircraft (UA) or 'drone' does not provide a complete picture. UAS are grouped into several categories and consist of numerous components, depending on their size and application.

Unmanned Aircraft System Components. The basic setup of a small UAS consists of an operator, a remote control, a C2 link and the aircraft or 'drone' itself. Larger systems, such as the one depicted in Figure 1, may also incorporate a dedicated Ground Control Station (GCS) for Launch and Recovery as well as a Mission Control Element (MCE) for conducting the operation. The larger systems typically utilize space-enabled BLOS communications for the C2 and data links. GCSs and MCEs consist of physical infrastructure such as trucks and containers or buildings, which typically host the computer hardware and software that, in turn, run the applications required to operate the overall system.

As a general rule, the larger the UAS, the larger the requirement for infrastructures such as shelters, runways, airfields or airports. The same is true for the amount of logistics, such as fuel, ammunition, and maintenance.

Finally, unmanned systems always require personnel to operate them. This can vary from a single individual operating a small 'drone' up to multiple aircrew rotating in shifts for larger systems. Higher class military UAS performing collection missions also require a significant amount of Processing, Exploitation and Dissemination personnel to analyse the information provided by the UAS.

Unmanned Aircraft System Categories. NATO categorizes UAS into three dedicated classes, ranging from Class I for the micro, mini and small ones, to Class II for medium-sized, tactical systems, to Class III for Medium-Altitude Long-Endurance (MALE) and High-Altitude Long-Endurance (HALE) aircraft. By looking at the three different classes, their application, size and operating altitude alone, it can be concluded that countering this spectrum of UAS requires a multitude of different, class-specific approaches.

3 Countermeasures' Points of Attack

Figure 2 provides an overview of UAS components and their relative spatial arrangements. Depending on the component itself, the domain it is operating in and its potential distance to NATO forces, there are different points of attack presented as options for the employment of countermeasures. While these points of attack can be addressed by the missions described in the sections below, all should complement each other and contribute to a comprehensive, multi-domain C-UAS effort.

Force Protection (FP). LSS UAS are readily available as COTS products to anyone and pose an imminent threat to critical public infrastructure and military installations. Force protection measures assuring the safety of friendly forces and critical infrastructure are typically very localized and focused on the area which requires protection. Natural and human-made

Figure 1: Unmanned Aircraft System Components.

Airport: © Mohd Syis Zulkipli/shutterstock, Drone: © krepnox/pixabay

obstacles such as trees or buildings can cover an approach of LSS UAS and significantly delay the detection of these objects in the area, further shortening available reaction time. Force protection measures should primarily be aimed at denying access of UAS to the protected area. However, it may also be desirable to safely capture the UAS for intelligence purposes.

Air Defence (AD). Larger UAS can operate at altitudes of up to 30,000 ft., and in some cases even higher. The Radar Cross Section of these UAS is comparable to any other non-stealthy aircraft, hence they can be detected and engaged by most Air and Missile Defence (AMD) systems. However. Modern surface-to-air ammunition is not cheap and is designed to engage high-value targets. Large numbers or a swarm of low-cost UAS may quickly turn the cost-benefit ratio of traditional AMD upside down and render current systems inefficient. Short-Range Air Defence and even legacy Anti-Aircraft Artillery may provide an effective, but also efficient, defence against UAS.

Air Interdiction (AI). Launch and Recovery of larger UAS is typically conducted from a GCS inside or near the mission area. GCS can be mobile and mounted on a truck or stationary when placed on the ground, e.g. near an airfield. In any case, the Launch and Recovery Element (LRE) of larger UAS is a high-value target as it is often responsible for launching and recovering several UA. Eliminating an LRE will likely bring UAS operations to a halt in the respective area as new UAS cannot be launched anymore and airborne ones cannot be recovered safely.

Special Operations Forces (SOF). Once airborne, larger systems can often be handed over from the LRE to an MCE and operated BLOS via Satellite Communications (SATCOM). The MCE can be located far outside the mission area, probably deep inside the adversary's territory and utilizing a hardened infrastructure. NATO Special Operations Forces may be employed as a means to attack the enemy's MCE itself, take out the SATCOM ground nodes which are essential for UAS BLOS operations, or even kill adversary combatants such as UAS crew members during their time off base.

Cyber Warfare. UAS are entirely dependent on their computer systems, information technology and network connectivity. Control stations, especially inside fixed installations such as an MCE, are potentially vulnerable to attack through cyberspace, exploiting security vulnerabilities of their hardware and software but also by taking advantage of human failure, negligence or susceptibility. COTS UAS being operated via a GSM network are likely only accessible through the cyberspace domain since countermeasures in the electromagnetic spectrum may be off limits, e.g. if frequencies are publicly used.

Electromagnetic Operations (EMO). C2 of UAS is conducted via LOS or BLOS radio transmissions and typically also reliant on Position, Navigation, and Timing (PNT) signals. Electromagnetic Operations can be used throughout all tiers of UAS to hinder and disrupt C2 and PNT transmissions or even to spoof PNT information to divert or land the UAS. However, 'traditional' Electronic Warfare has its limits with modern models of UAS which are capable of autonomous flight and are no longer reliant on continuous data links. However, upcoming Directed Energy Weapons such as High Power Microwaves or High Energy Lasers may add kinetic capabilities to the electromagnetic portfolio and could be used to render sensor payloads inoperable or destroy the UA itself.[9]

Intelligence, Surveillance, Reconnaissance (ISR). Detecting UA in flight is often the first step in defending against them. Larger UA can be detected even with legacy radar systems, whereas LSS UA require more specialized equipment to distinguish them from clutter, e.g. leaves and birds. However, apart from airspace surveillance, reliable identification of the intruding UAS and its capabilities, as well as identifying the origin of the C2 transmission, is critical for selecting appropriate countermeasures. For example, this includes information about the capabilities and the level of autonomy of the UA, locations of adversary LREs and MCEs, as well as SATCOM assets and frequencies used. C-UAS systems have to be fed with this information, preferably in real-time, to process a suitable target solution.

The Space Domain. Space-based communications are an essential part of BLOS UAS operations. But COTS UAS also utilize PNT signals provided by respective satellite constellations. Within the limits of the 'Outer Space Treaty', countermeasures against space-based communications and PNT may be a legitimate option to defend against an entire fleet of adversary UAS. This does not necessarily require kinetic engagements by anti-satellite weapons. Indeed, ground or space-based jamming capabilities could be effective without risking large amounts of debris which could render entire orbits unusable for mankind.

4 Legal Considerations for the Application of Countermeasures

Applications for UAS range from public and recreational purposes to military missions including airstrikes. Consequently, depending on their use, defending against these systems is governed by either domestic or international law, and the legal framework that needs to be applied is also dependent on whether it is peacetime or wartime.

Peacetime vs Wartime. Defending against UAS is not only a wartime requirement. Frequent incidents[10,11] have already proven that COTS 'drones' can easily be flown into restricted airspace and are able to stop an entire airport's flight operations. It is only a question of time before the first incident will be witnessed over military installations, e.g. air bases, headquarters or military training grounds.

Depending on the country and its domestic law, which is applicable during peacetime, circumstances may prohibit certain types of countermeasures and limit the options for defending against UAS. These possibly prohibited countermeasures include kinetic engagement of airborne unmanned systems, jamming of publicly used frequencies, such as GSM or wireless networks, or interference with the commercial PNT signals.

In general, it can be assumed that countering UAS in peacetime will be subject to a multitude of civilian restrictions which may or may not fully apply in a conflict scenario. C-UAS doctrine and Tactics, Techniques and Procedures (TTP) need to include these particulars and adhere to individual legal environments.

Law Enforcement vs Military Engagement. In peacetime, the responsibility for the defence against 'drones' and UAS typically lies with civil law enforcement agencies. However, responsibilities may overlap near military installations and critical infrastructure. Moreover, law enforcement agencies may require military support since the equipment to detect, identify and engage UAS might only be provided by the armed forces.

Hence, close cooperation and coordination between civilian law enforcement agencies and the armed forces are essential for a comprehensive C-UAS approach. Mutual exercises could help establish common C-UAS TTPs and ensure an effective level of interoperability between civil and military organizations.

Public Safety and Collateral Damage. The protection of civilians from harm is the primary principle of both international as well as domestic law. Therefore, defence against UAS requires consideration of the potential risks to human life, both in peacetime and in wartime. Civilians may be endangered by kinetic measures such as the shooting down of UA or an attack on its ground facilities.

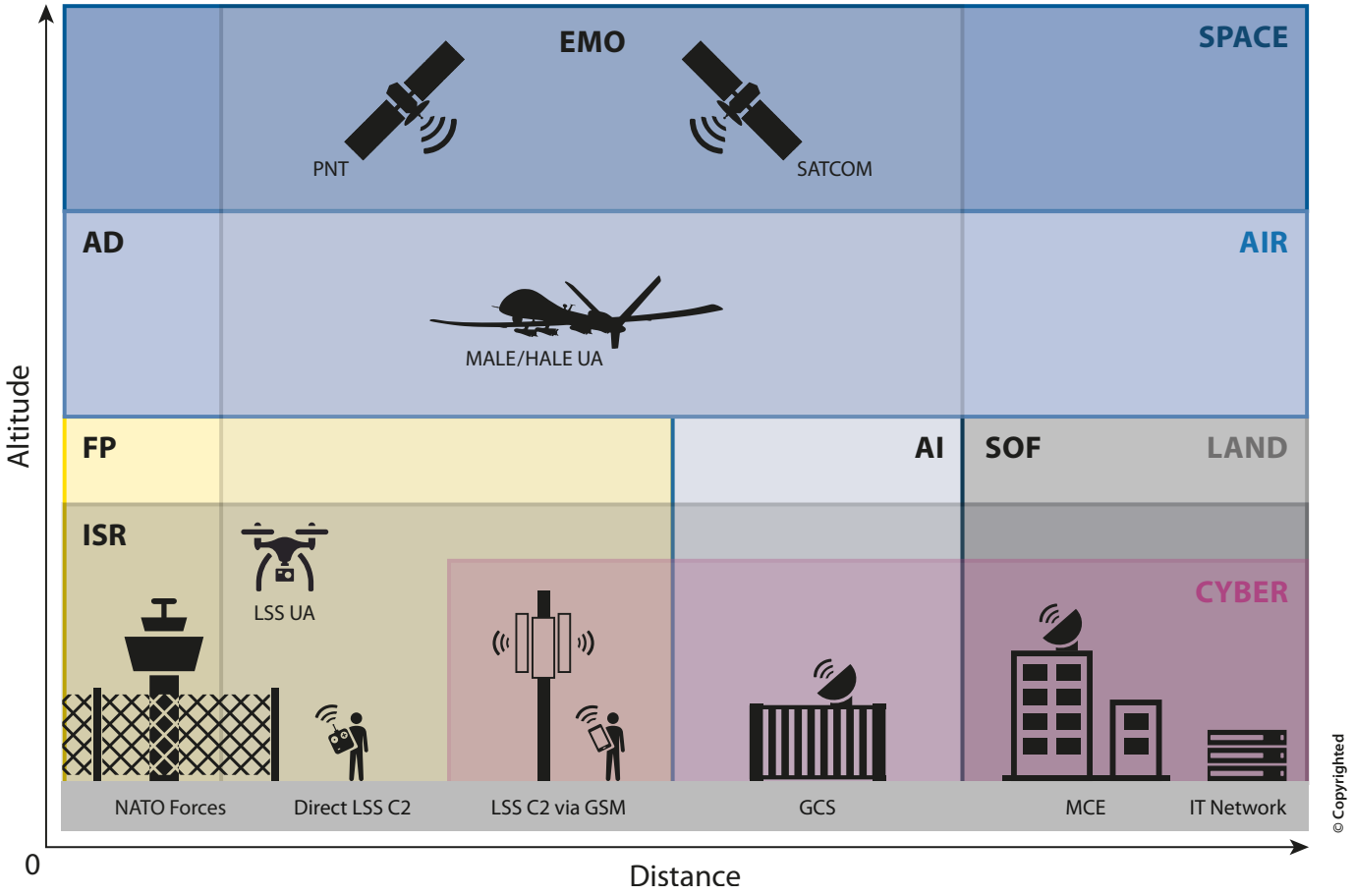

Figure 2: Spatial Arrangement of Unmanned Aircraft System Components.

Additionally, non-kinetic measures such as jamming radio frequencies or PNT signals may affect public and commercial communications infrastructure and may, therefore, be restricted or off limits. Especially in peacetime, countermeasures have to be balanced against potential adverse impacts on critical communication systems and economic loss.

Depending on the payload, e.g. biological toxins, chemical gases or explosives, it may be required to manoeuvre the UA out of range of friendly forces or civilians before the actual countermeasure comes into force. Therefore, 'traditional' C-UAS approaches which take effect on the spot need to be reviewed and should consider new approaches such as capturing aerial vehicles and neutralizing payloads.

Pre-emptive vs Reactive Countermeasures. Larger UAS require a significant amount of computer hardware, software and networks to operate. Therefore, the cyberspace domain may offer potential countermeasures capable of rendering the entire network and communications infrastructure of one or more unmanned systems inoperable. However, countermeasures in the cyberspace domain may require more than only a defensive posture. Pre-emptive and disguised placement of 'backdoors' in adverse computer systems may ensure access to these networks when required and it is probably the only way to be prepared and react promptly on an imminent UAS threat.

Dedicated legislation may also assist in defending against UAS in such a way that COTS 'drones' are required to transmit an identification and positioning signal comparable to the regular civilian air and maritime traffic. Some manufacturers already equip their drones voluntarily with transponders that provide this information on a separate and unencrypted radiofrequency. Of course, this will not prevent criminal or terroristic abuse of these systems, but if legislation were in place, any system not providing a transponder signal could be classified as potentially hostile.

5 The JAPCC Approach and Recommended Way Ahead

As outlined in this article, defending against UAS is not only a Force Protection or Air Defence issue, nor is it only about the aircraft or drone itself.

As of this year, the Joint Air Power Competence Centre established a Counter-UAS Focus Group (CUASFG) comprised of Subject Matter Experts from Intelligence, Surveillance, and Reconnaissance, Surface-Based Air and Missile Defence, Force Protection, Close Air Support and Air Interdiction, Electronic Warfare, Space Operations, Cyber Warfare and, of course, Unmanned Systems.

The JAPCC's CUASFG plans to liaise between the different subject matter areas and to provide cross-domain expertise with regard to the defence against the full spectrum of UAS. A comprehensive JAPCC study on C-UAS, to include a perspective from law enforcement agencies, is planned in the 2020 timeframe.

The JAPCC highly recommends NATO to establish a similar focus group to address the complex challenges of C-UAS comprehensively as current NATO doctrine and TTP need to be aligned across services and military branches to provide an effective C-UAS approach.

1. Koller Engineering GmbH, 'DroneGun', [Online]. Available: https://www.koller.engineering/dronegun/. [Accessed 15 Jul. 2019].
2. DroneShield, 'DroneGun Tactical', [Online]. Available: https://www.droneshield.com/dronegun-tactical. [Accessed 15 Jul. 2019].
3. IXI EW, 'DRONEKILLER', [Online]. Available: https://ixiew.com/page/. [Accessed 15 Jul. 2019].
4. SRC Inc., 'Silent Archer® Counter-UAS Technology', [Online]. Available: https://www.srcinc.com/what-we-do/counter-uas/silent-archer-counter-uas.html. [Accessed 15 Jul. 2019].
5. NATO Science & Technology Organization (STO), 'SCI-301-RTG Defeat of Low Slow and Small (LSS) Air Threats'.
6. NATO Science & Technology Organization (STO), 'SCI-ET-241 Development of a Counter Small UAS Analysis, Research and Demonstration Strategy', 2017.
7. NATO Industrial Advisory Group (NIAG), SG-170 (2013), SG-188 (2015), SG-200, SG-220 and SG-238 (2019).
8. The NATO Countering Unmanned Aircraft System Working Group (NATO C-UAS WG) has been formally established through the approval of the Countering Class I UAS practical framework, endorsed by NATO's Defence Ministers on their meeting on 13–14 Feb. 2019.
9. Raytheon Advanced Missile Systems, 'Defense at the speed of light', 24 Apr. 2019, [Online]. Available: https://www.raytheon.com/news/feature/defense-speed-light. [Accessed 16 Jul. 2019].
10. Dedrone, 'Worldwide Drone Incidents', [Online]. Available: https://www.dedrone.com/resources/incidents/all. [Accessed 16 Jul. 2019].
11. Federal Aviation Administration (FAA), 'UAS Sightings Report', 2014–2019, [Online]. Available: https://www.faa.gov/uas/resources/public_records/uas_sightings_report/. [Accessed 16 Jul. 2019].

Author: Lieutenant Colonel André Haider, DEU Army. Lieutenant Colonel Haider is the Joint Air Power Competence Centre's (JAPCC) Unmanned Aircraft Systems Subject Matter Expert since 2011 and JAPCC's representative in the NATO Joint Capability Group Unmanned Aircraft Systems (JCGUAS) since 2012. He joined the German Armed Forces in 1992 and is an artillery officer by trade with over fifteen years' experience in command and control and operational planning. He is also a trained United Nations Missions Observer and participated in several EU and NATO missions. His last post was Deputy Commander of the German Army's MLRS Rocket Artillery Battalion.

Contact: Visit us on www.japcc.org, write us an e-mail at contact@japcc.org, or contact the author directly at haider@japcc.org.

Follow us on Social Media: