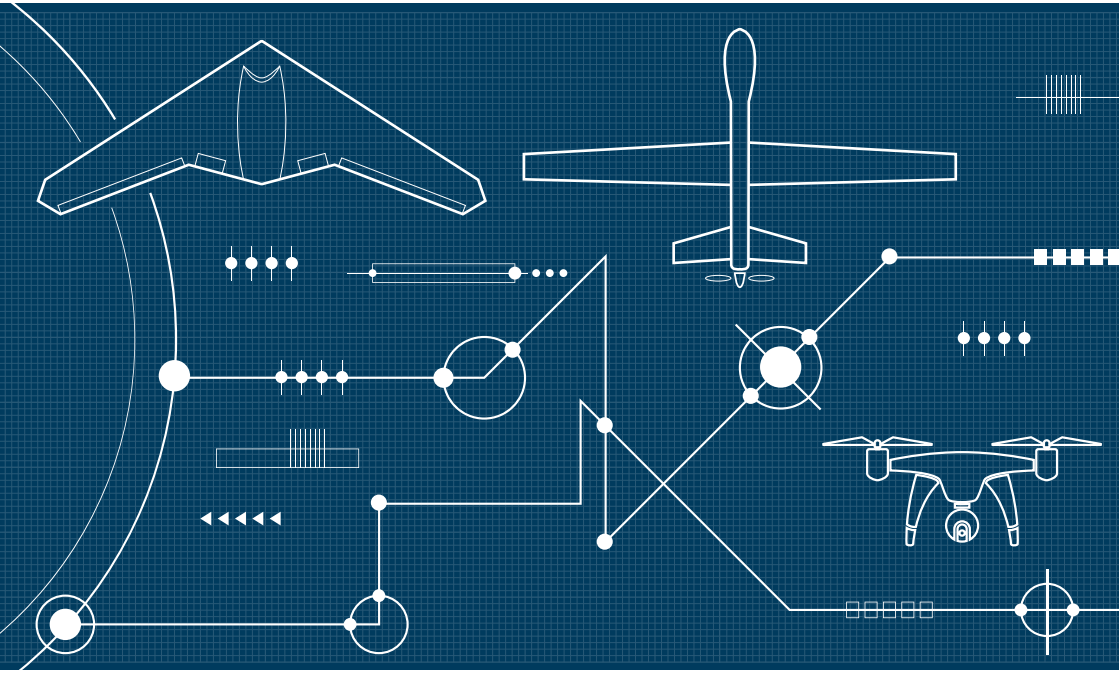


A Comprehensive Approach to Countering Unmanned Aircraft Systems

15th ANNIVERSARY

Joint Air Power Competence Centre

A Comprehensive Approach to Countering Unmanned Aircraft Systems

A Comprehensive Approach to

Countering Unmanned Aircraft Systems

Joint Air Power Competence Centre

Cover Montage M Circuit Board: © pluie_r / Shutterstock.com; Background Grid: © Copyrighted; Sentinel and Pterodactyl I: © Copyrighted; Quadcopter: © FARBAI / Shutterstock.com

Authors (in alphabetical order)

Maj Osman Aksu (TU AF)
Dr Christian Alwardt (GE)
Chief Insp Sascha Berndsen (GE)
Joel Bollö (SWE)
Capt Daniel Cochran (US N)
Dr James Corum (US)
Dr Ulrich Dieckert (GE)
Dr Hans-Albert Eckel (GE)
Lt Col Heiner Grest (GE AF)
Lt Col André Haider (GE A)
Dr Martin Hellmann (GE)
Lt Col Henry Heren (US SF)
Heleen Huijgen LLM BSc (NE)
Liisa Janssens LLM MA (NE)
Adam Jux BA (UK)
Maj Fotios Kanellos (GR AF)
David Kovar (US)
First Chief Insp Jürgen Künstner (GE)
Lt Col Roy Milke (GE AF)
Christoph Müller (GE)
Lt Col Paul MacKenzie (CA AF)
Alex Morrow (US)
Dr Thomas Neff (GE)
Wg Cdr (ret.) Jez Parkinson (UK AF)
Phil Pitsky (US N)
Lt Col Berry Pronk (NE AF)
Dr James Rogers (UK)
Amit Samani (UK)
Lt Col Andreas Schmidt (GE AF)
Georg Schweizer (CH)
Lt Col (ret.) Panagiotis Stathopoulos (GR AF)
Lt Col Giuseppe Valentino (IT AF)
Lt Col Tim Vasen (GE AF)
Lt Col Jürgen Welsch (NE AF)
Maj Andreas Wurster (GE A)
Dr Dirk Zimper (GE)

Editorial Team: Col Matthew Willis (US AF), Lt Col André Haider (GE A), Lt Col Daniel C. Teletin (RO AF), Lt Col Daniel Wagner (GE AF)

All contributions to this publication have been peer reviewed by the appropriate subject matter experts. Where necessary, external expertise has been consulted.

Published and distributed by: The Joint Air Power Competence Centre, von-Seydlitz-Kaserne, Römerstraße 140, 47546 Kalkar, Germany.

Acknowledgements

We would like to thank all authors and their respective organizations for their contributions and expertise in helping to publish this compendium and advance this topic for discussion within NATO.

About This Book

This technical manual covers all aspects of having to counter the full spectrum of unmanned aircraft and their respective system components. It should serve to bring together both civilian and military experts by initiating thought and emphasizing NATO's approach to a comprehensive solution for countering unmanned aircraft systems. We hope that you will find this book useful and a valuable addition to the academic body of work published by the JAPCC on Joint Air and Space Power.

Jeffrey L. Harrigian
General, US AF
Commander, Allied Air Command
Commander, United States Air Forces in Europe
Commander, United States Air Forces Africa
Director, Joint Air Power Competence Centre

Table of Contents

Acknowledgements V

Preface 1
By Dr Claudio Palestini, IT
North Atlantic Treaty Organization

Foreword 5
By Lieutenant General Klaus Habersetzer, GE AF
Joint Air Power Competence Centre

Part I – Overview

1 **Introduction** 11
By Lieutenant Colonel André Haider, GE A
Joint Air Power Competence Centre

2 **The Differences Between Unmanned Aircraft, Drones, Cruise Missiles and Hypersonic Vehicles** ... 27
By Lieutenant Colonel Andreas Schmidt, GE AF
By Lieutenant Colonel André Haider, GE A
Joint Air Power Competence Centre

3 **Unmanned Aircraft System Threat Vectors** 33
By Lieutenant Colonel André Haider, GE A
Joint Air Power Competence Centre

4 The Vulnerabilities of Unmanned Aircraft System Components 55
By Lieutenant Colonel André Haider, GE A
Joint Air Power Competence Centre

5 A Methodology for Countering Unmanned Aircraft Systems 75
By Lieutenant Colonel André Haider, GE A
Joint Air Power Competence Centre

Part II – Military Perspectives

6 Joint Intelligence, Surveillance, and Reconnaissance 87
By Major Giuseppe Valentino, IT AF
By Major Andreas Wurster, GE A
Joint Air Power Competence Centre

7 Defensive Counter-Air Operations 103
By Lieutenant Colonel Andreas Schmidt, GE AF
By Lieutenant Colonel Berry Pronk, NE AF
Joint Air Power Competence Centre

8 Offensive Counter-Air Operations 129
By Major Osman Aksu, TU AF
Joint Air Power Competence Centre

9 **Targeting** 147
By Adam Jux, UK
Civilian Targeting Consultant

10 **Electromagnetic Operations** 167
By Lieutenant Colonel (ret.)
Panagiotis Stathopoulos, GR AF
Joint Air Power Competence Centre

11 **Cyberspace Operations** 183
By Lieutenant Colonel Paul MacKenzie, CA AF
By Major Fotios Kanellos, GR AF
Joint Air Power Competence Centre

12 **Space Operations** 209
By Lieutenant Colonel Heiner Grest, GE AF
By Lieutenant Colonel Henry Heren, US SF
By Lieutenant Colonel Tim Vasen, GE AF
Joint Air Power Competence Centre

13 **Force Protection Considerations** 227
By Wing Commander (ret.) Jez Parkinson, UK AF
Joint Air Power Competence Centre

14 **Command and Control** 257
By Lieutenant Colonel Andreas Schmidt, GE AF
By Lieutenant Colonel Jürgen Welsch, NE AF
Joint Air Power Competence Centre

15 **Education and Training** 269
By Lieutenant Colonel André Haider, GE A
By Lieutenant Colonel Roy Milke, GE AF
Joint Air Power Competence Centre

16 **Strategic Communications** 283
By James S. Corum PhD, Lieutenant Colonel (ret.), US A
University of Salford

Part III – Civil Perspectives

17 **Protection of Critical Infrastructure** 303
By Alex Morrow, US
By Phil Pitsky, US N (vet.)
By Amit Samani, UK
Dedrone
By Lieutenant Colonel André Haider, GE A
Joint Air Power Competence Centre

18 **Law Enforcement** 319
By Senior Chief Inspector Jürgen Künstner, GE
By Chief Inspector Sascha Berndsen, GE
German State Police of North Rhine-Westphalia
By Lieutenant Colonel André Haider, GE A
Joint Air Power Competence Centre

19 **Drone Forensics** 337
By David Kovar, US
Unmanned & Robotics Systems Analysis
By Joel Bollö, SWE
Micro Systemation AB

20 **Cloud-based Command and Control for Security and Drone Defence Applications** 351
By Georg Schweizer, CH
Securiton GmbH, Germany

Part IV – Legal Perspectives

21 **Regulatory Frameworks in Support of Counter-UAS** 375
By Dr iur. Ulrich Dieckert, GE
Dieckert Recht und Steuern GbR

22 **The Juridical Landscape of Countering Unmanned Aircraft Systems** 395
By Heleen Huijgen LLM BSc, NE
By Liisa Janssens LLM MA, NE
The Netherlands Organisation for Applied Scientific Research (TNO)

23 **Arms Control of Unmanned Weapons Systems: Facing the Challenges 415**
By Dr Christian Alwardt, GE
Institute for Peace Research and Security Policy at the University of Hamburg

Part V – Future Perspectives

24 **Research, Development, and Acquisition of Counter-UAS Technologies 437**
By Christoph Müller, GE
By Dr Martin Hellmann, GE
By Dr Hans-Albert Eckel, GE
By Dr Thomas Neff, GE
By Dr Dirk Zimper, GE
German Aerospace Center (DLR)

25 **Employing Friendly UAS for Counter-UAS Operations 467**
By Captain Dan Cochran, US N
By Lieutenant Colonel Andreas Schmidt, GE AF
Joint Air Power Competence Centre

26 **Future Threats: Military UAS, Terrorist Drones, and the Dangers of the Second Drone Age 481**
By Dr James Rogers, UK
Centre for War Studies at the University of Southern Denmark

Part VI – Annexes

A NATO UAS Classification Table 509

B Military UAS Fact Sheets 513
Russia 515
China 539
Iran 555

C Commercial Drones Fact Sheets 565

D About the Authors 573

E Table of Figures 595

F List of Acronyms 601

By Dr Claudio Palestini
North Atlantic Treaty Organization,[i]
Emerging Security Challenges Division,
Countering Unmanned Aircraft Systems Working Group

[i] Contents of this book reflect only the views of the authors and do not express any official position of NATO. JAPCC is providing an independent thought and analysis and the book is intended to initiate and contribute to the on-going discussion about the topic.

Preface

There is no 'Silver Bullet'

If you were attending a conference or meeting about Countering Unmanned Aircraft Systems (C-UAS) in the last three years (and there were a lot), for sure you heard this sentence. However, this used to address only one narrow aspect of the whole problem, i.e. the impossibility of technical providers to propose one single system that would solve the problem in its entirety and forever.

C-UAS is a wicked problem, as it involves a multitude of aspects and problems for which solutions are not trivial or not practical in many typical scenarios. Think about the different legal implications of a C-UAS operation in peacetime within NATO territory, or in an expeditionary conflict; or the incredible pace of development

of the commercial and recreational drone market that makes deployed countermeasures ineffective after only a few months. Think about the ongoing developments of the so-called 'second drone age' in which all competitors, from peers to terrorists and non-state actors, will include drone technologies in their standard tactics and concept of operations, challenging the traditional air superiority in most of the conflicts. Think about the upcoming drone arms race, in which drones and counter-drones manufactures will fight to deploy the smartest and most innovative technologies, bringing the current C-UAS issue to new heights, transitioning towards novel domains and concepts, from electronic to cyber warfare, from kinetic to directed energy weapons.

It is known that wicked problems cannot be solved but can only be tamed. To tame the C-UAS problem, the only possibility is to have a profound understanding, to anticipate trends, to imagine the desired end state and work towards it. I would argue that the famous 'silver bullet' is exactly this: awareness, experimentation, preparedness, cooperation, coordination, and capability to adapt. C-UAS demands for more cooperation at every level: at the technical level, where single solutions are never effective if not integrated in a broader defence-in-depth context; at the tactical level, to make sure that countermeasures are effective against the threat without fratricide and collateral damages; at the operational level, as C-UAS needs seamless integration at the verge of multiple domains; finally, at the strategic level, as a whole of government approach is essential to cope with the threat.

This is what the NATO C-UAS Working Group has been trying to do since its establishment in 2019. In the course of the past two years, it has become a trusted forum where Allies exchange views, cooperate and learn from each other. This is also the ultimate scope of this book: it gives multiple perspectives from different stake-

holders, military, law enforcement, industry and academia, and encourages cross-domain thoughts and mutual understanding.

As this subject is entering a novel level of maturity within NATO, the work collected in this book will certainly help in addressing the future challenges and to provide answers to the many questions that, collectively, will need to be answered.

Dr Claudio Palestini
North Atlantic Treaty Organization,
Emerging Security Challenges Division,
Countering Unmanned Aircraft Systems Working Group

By Lieutenant General Klaus Habersetzer, GE AF
Commander, German Air Operations Command
Commander, Combined Air Operations Centre Uedem
Executive Director, Joint Air Power Competence Centre

Foreword

Dear Reader,

Unmanned Aircraft Systems (UAS) have become an integral part of NATO operations and have advanced into an invaluable asset for Intelligence, Surveillance, and Reconnaissance, as well as for combat missions.

This has not gone unnoticed by both state and non-state actors, which has led to an enormous effort by these players to catch up with or at least mimic the Western level of technology. Over the last decade, China, Russia, and to a certain extent Iran, have considerably advanced the development of UAS, and their latest models seem to have the same performance characteristics as Western models. Russian and Chinese inventories comprise the full range

from small and tactical UAS, through Medium- and High-Altitude Long-Endurance (MALE/HALE) systems, to replicas of US and European stealth prototypes.

At the same time, the consumer drone market is one of the world's fastest growing businesses, making drone technology literally available for everyone. The market for commercial drones with a significantly higher performance than consumer models is also steadily growing. Due to their increased proliferation the number of incidents with drones in the vicinity of airports, public events and military installations has raised the attention and concern of the respective civil authorities responsible for public safety and law enforcement.

Countering UAS and drones is a challenging task, both in the military and civil domain. Therefore, it is important to incorporate all available means and to exploit any vulnerabilities to achieve this task. However, most UAS and drone defence applications are focused solely on the Unmanned Aircraft (UA) itself, rather than exploiting the weaknesses of the entire system, which typically also comprise mobile or stationary remote control equipment, radio communication links, and human personnel.

It is also important to note that countering UAS and drones is already a task in peacetime whereas most military defence applications are intrinsically designed for a conflict scenario. Not to mention that the legal frameworks for operating in peace, crisis, or conflict differ significantly. Hence, adopting civil approaches to this challenge and incorporating the civil authorities is required when the employment of military force is restricted or prohibited.

To stimulate thought on a more comprehensive approach when having to counter UAS and drones, this book provides the reader

with a broad assortment of the different military, civil, and legal perspectives on the subject matter.

I invite you and your staff to read through this book and to critically assess the conclusions and recommendations presented. We welcome any observations you may have with regard to this book or future issues it identifies. Please feel free to contact my JAPCC staff via e-mail: contact@japcc.org for any inquiries and comments.

Klaus Habersetzer
Lieutenant General, GE AF
Executive Director, JAPCC

Part I

Overview

1

By Lieutenant Colonel André Haider, GE A
Joint Air Power Competence Centre

Introduction

Background

In recent decades, Unmanned Aircraft Systems (UAS) have been fielded in every military service, ranging from handheld micro-UAS to medium-sized tactical systems to full-grown 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' in the vicinity of airports, public events and military installations.

Recently, various industries 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, 2, 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[5-11] and by establishing a C-UAS Working Group with a focus on terrorist misuse of UAS.[12]

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 (C2) 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 Global System for Mobile Communications (GSM) network from the operator's mobile phone. These features make jamming either completely useless, since the C2 link is no longer required to navigate, or unavailable, because of peacetime restrictions that prohibit the jamming of frequencies that are in use by the public.

Additionally, a sole focus on the LSS 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 the Alliance. Consequently, NATO has to anticipate enemy use of UAS in the same mission sets as friendly UAS, covering the spectrum from Intelligence, Surveillance & Reconnaissance (ISR) 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 LSS end, although

imminent and essential, is not sufficient to cover all aspects of defence against potential adversary UAS engagements.

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 the 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 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.

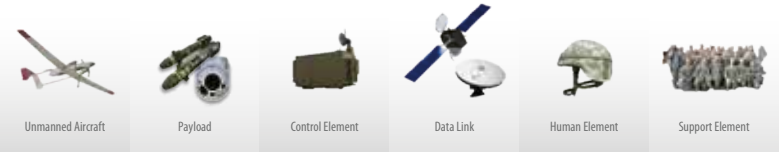


Figure 1.1: Unmanned Aircraft System Components.

As a general rule, the larger the UAS, the larger the requirement for infrastructure such as shelters, runways, airfields or airports. The same is true for the amount of logistics support, 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 in case of larger systems. Higher class military UAS performing collection missions also require a significant amount of Processing, Exploitation and Dissemination (PED) personnel to analyze 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.[13] By comparing 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.

Unmanned Aircraft System Design Principles

Apart from their different classifications as described above, UAS also follow various design principles, according to their application and purpose. Depending on the specific UAS design features, detection and potential countermeasures may be challenged, denied or even not applicable.

Unmanned Aircraft. UA can be fixed-wing, rotary-wing, and some even incorporate stealth designs. Smaller systems (Class I) typically follow the rotary-wing principle, whereas larger systems

(Class III) almost exclusively utilize a fixed-wing design. Tactical systems (Class II) follow both principles. Stealth designs are predominantly found with large HALE aircraft but sometimes also with tactical systems.

Propulsion. Throughout all classes, the majority of UA are propelled by a rotorcraft engine which allows for greater fuel efficiency and therefore longer endurance. However, some UA are equipped with jet engines, trading-in mission duration for faster speeds and larger payloads. Upcoming generations of UA are envisioned to incorporate hypersonic propulsion and may achieve airspeeds faster than Mach 5.

Communications. C2 of a UA is generally conducted via a LOS or BLOS radio link. Depending on the unmanned system's level of

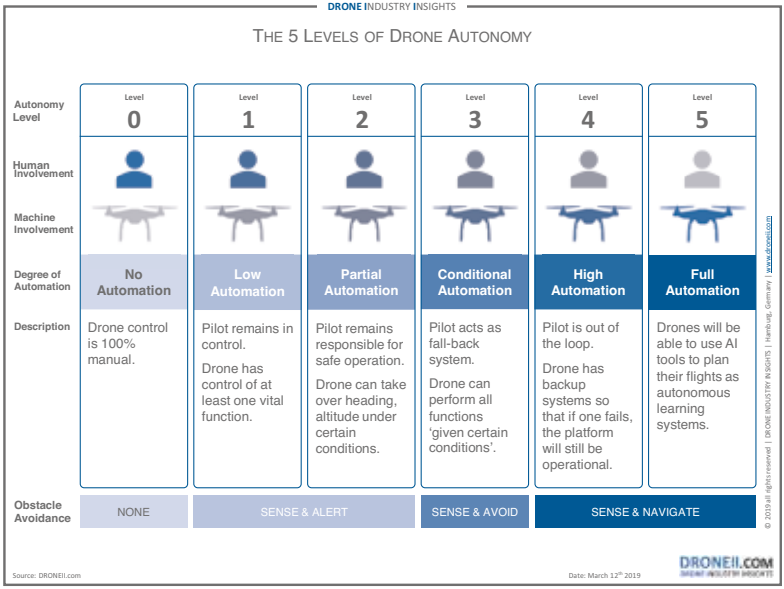


Figure 1.2: Levels of Drone Autonomy.

autonomy (cf. Figure 1.2), this radio link is active either permanently or only on demand. UAS radio links encompass the range from common Wireless Networks up to dedicated satellite communications frequencies in the Ku-Band. The upcoming 5G standard will utilize even higher frequencies and mobile phone applications for command and control of UAS via GSM are already available on the commercial market. It is important to note that a potential adversary will most likely not utilize the same frequency bands as NATO and its partners.

Data Transmission. It can be anticipated that every radio link and every other form of digital communications between unmanned system components will be secured to a certain degree. Even commercially available 'drones' use either proprietary data link protocols or encryption to secure their communications.

A Comprehensive Approach to Countering Unmanned Aircraft Systems

Figure 1.3 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

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 focused on the area which requires protection. Natural and human-made 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

Larger UAS can operate at altitudes of up to 30,000 ft., and in some cases even higher. The Radar Cross Section (RCS) of these UAS is comparable to any other legacy aircraft, hence can be detected and engaged by most Air and Missile Defence (AMD) systems. However,

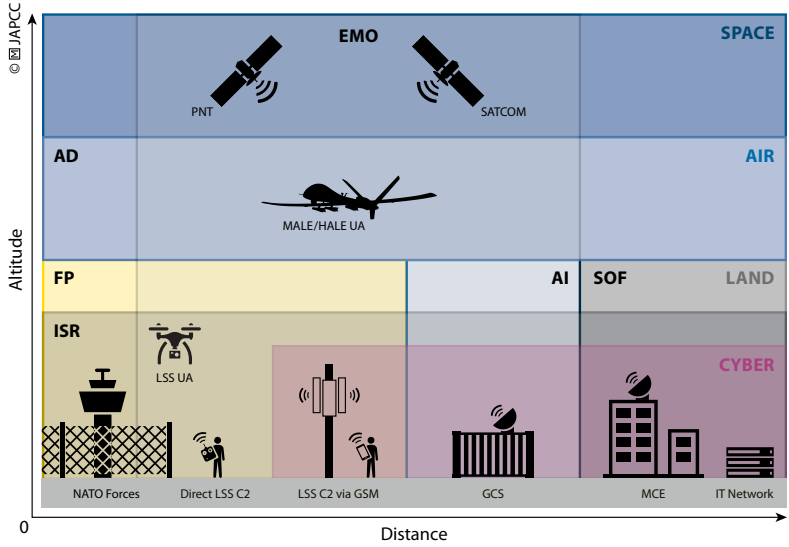


Figure 1.3: Spatial Arrangement of Unmanned Aircraft System Components.

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 (SHORAD), Counter-Rocket, Artillery, and Mortar (C-RAM) systems, and even legacy Anti-Aircraft Artillery may provide an effective, but also efficient, defence against UAS.

Close Air Support and Air Interdiction

Launch and Recovery of larger UAS is typically conducted from a Ground Control Station (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 may not be recovered safely. Thus, AI may disrupt, degrade, deny or destroy an adversary's unmanned capabilities before they can be even used against friendly forces.

Special Operations

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 (SOF) 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 duty.

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 an 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 most 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

C2 of UAS is conducted via LOS or BLOS radio transmissions and typically also reliant on Position, Navigation, and Timing (PNT) signals. Electromagnetic Operations (EMO) 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 (EW) 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 (DEW) such as High-Power Microwaves (HPM) or High Energy Lasers (HEL) may add kinetic capabilities to the EMO portfolio and could be used to render sensor payloads inoperable or destroy the UA itself.[14]

Intelligence, Surveillance, and Reconnaissance

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 the appropriate countermeasures. 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 this information, preferably in real-time, to process a suitable targeting solution.

The Space Domain

SATCOM is 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 the creation of large amounts of debris which could render entire orbits unusable for mankind.

Legal Considerations for the Enforcement 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 versus Wartime

Defending against UAS is not only a wartime requirement. Frequent incidents[15, 16] have already proven that COTS 'drones' can easily be flown into restricted airspace and can 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. airbases, headquarters or military training grounds.

Depending on the country and its domestic laws, which are 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 UA, 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 versus 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 reside only in 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.

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

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 can be employed. Therefore, 'traditional' C-UAS methods which take effect on the spot need to be reviewed, and new approaches such as capturing aerial vehicles and neutralizing payloads should be considered.

Pre-emptive versus 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 adversary computer systems may ensure access to these networks when required and it is probably the only way to be prepared and react promptly to 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 radio frequency. Of course, this will not prevent criminal or terroristic abuse of these systems, but if legislation was in place, any system not providing a transponder signal could be classified as potentially hostile.

Summary

This short introduction was intended to provide an overview of the complexity of having to counter UAS. Different classes, applications and design principles of the Unmanned Aircraft itself challenge or even deny certain types of countermeasures. Moreover, larger unmanned systems may include ground installations, data links, computer networks as well as logistics, support equipment and dozens of personnel. Hence, there is no 'one-size-fits-all' solution to the C-UAS challenge.

Finally, countering UAS requires a comprehensive approach by all the military and also non-military disciplines who can project lethal and non-lethal effects on any of the components of an unmanned

system. Additionally, all these potential countermeasures require review under the different legal frameworks applicable in wartime, but more importantly in peacetime. Typically, in peacetime, military and civil authorities usually own different powers which require close coordination when employing countermeasures.

Endnotes

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 Engagement of Low, Slow and Small Aerial Targets by GBAD', 2013.
8. NATO Industrial Advisory Group (NIAG), 'SG-188 GBAD Sensor Mix Optimization Study for Emerging Threats', 2015.
9. NATO Industrial Advisory Group (NIAG), 'SG-200 Low, Slow, and Small (LSS) Threat Effectors'.
10. NATO Industrial Advisory Group (NIAG), 'SG-220 GBAD Operations in the 21st Century', 2017.
11. NATO Industrial Advisory Group (NIAG), 'SG-238 GBAD Against Cruise Missiles and UAS', 2019.
12. 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.
13. NATO Standardization Office (NSO), 'ATP-3.3.8.1 Minimum Training Requirements for Unmanned Aircraft Systems (UAS) Operators and Pilots', Edition B Version 1, May 2019.
14. 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].
15. Dedrone, 'Worldwide Drone Incidents', [Online]. Available: https://www.dedrone.com/resources/incidents/all. [Accessed 16 Jul. 2019].
16. 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].

2

By Lieutenant Colonel Andreas Schmidt, GE AF
By Lieutenant Colonel André Haider, GE A
Joint Air Power Competence Centre

The Differences Between Unmanned Aircraft, Drones, Cruise Missiles and Hypersonic Vehicles

Introduction

To define the impact of unmanned aerial systems on current and future NATO operations, it is very important to identify which kind or category of threats are included and which are not. This section will try to clarify this definition and will show that a clear classification is sometimes not easy to achieve.

A threat is typically defined as the combination of malevolent intent and the ability to put it into action. Further sub categories of this overarching term exist, such as 'air threat' to better describe the operational environment and to categorize or delineate measures, like 'air defence' to counter the respective threat. The set of all capabilities that qualify as air threats is so diverse and

complex that no singular system can be used to execute air defence. Additionally, the question of what constitutes an air threat is not an easy one. Is an air threat any capability that uses the air as its main or final domain for effect delivery? If that were the case, a projectile from a rifle would be an air threat, which is not the case. However, the defence against larger projectiles like artillery shells or mortar rounds, which are a typical ground threat, finally became part of air defence considerations after Counter-Rocket-Artillery-Mortar (C-RAM) systems had been developed and fielded.

Defining Unmanned Aircraft

Since this document is about the threat of Unmanned Aircraft Systems (UAS), the term Unmanned Aircraft (UA) needs to be looked at. Currently, NATO defines UA as an aircraft that does not carry a human operator and which is operated remotely using various levels of automated functions.[1] UA can be expendable or recoverable and may carry lethal or non-lethal payloads. Of note, cruise missiles are categorically excluded from this NATO definition. As this definition is very broad, the term aircraft needs to be described for a better understanding. The ICAO (International Civil Aviation Organization) defines an aircraft as any machine that can derive support in the atmosphere from the reactions of the air other than the reactions of the air against the earth's surface.[2]

By this portrayal alone, all projectiles that only have initial propulsion and then just follow a ballistic trajectory (e.g. bullets, artillery shells, regular bombs or ballistic missiles) can be excluded from the aircraft category. For the purpose of this paper, also ordnance which uses aerodynamic lift or other interactions with the atmosphere just to extend the ballistic flight path will be excluded from

the UA category as well. This removes threats like gliding bombs or hypersonic glide vehicles from the UA set, although they could be remotely operated and definitely possess automated functions. Emerging technologies (e.g. new propulsions, swarming or Artificial Intelligence) might create fringe threat sets, which generally show UA properties, but are currently not considered as such.

An extended definition proposal of Unmanned Aircraft (UA)

Vehicles that use aerostatic or aerodynamic lift, and overall don't generally fly on a ballistic trajectory can be categorized as an aircraft. These vehicles can be propelled by a motor (e.g. rotary or jet) to create lift and sustain flight. If these aircraft do not house a pilot within the airframe and are operated remotely using various levels of automated functions, they are considered an UA, excluding cruise missiles.

Cruise Missiles versus Unmanned Aircraft

In general, making the distinction between ordnance and UA is not useful, due to tremendous technical progress. These two categories are not exclusive anymore, while not every ordnance is a UA, a UA can be used as ordnance. In times of mass production, innovative propulsion systems and reliable effect delivery without a pilot on board, the idea of using the vehicle as ordnance itself became more prevalent. While the V1 in WWII initially had a CEP (Circular Error Probable) of more than 10 km and most use cases were aimed at producing terror, today´s cruise missiles have a CEP of 10 meters or less. The cost/benefit ratio between losing the UA while creating a certain effect or enabling it to deliver the same effect while remaining retrievable has shifted significantly in times of precise technological options and relatively cheap production cost, especially for small UA.

Drone versus Unmanned Aircraft

The terms 'Unmanned Aircraft' and 'Drone', as well as variations such as 'Unmanned Aerial Vehicle (UAV)'[3] or 'Remotely Piloted Aircraft (RPA)'[4] are often used interchangeably but are actually deliberately defined to reflect certain classes, attributions or certifications of the unmanned systems.

When having to counter these systems, the most relevant factors are overall system complexity and aircraft size. Therefore, this book summarizes the different categories and classes of unmanned systems under the following two terms:

Unmanned Aircraft

The term 'Unmanned Aircraft' describes the overall set of vehicles, as described above. However, this book uses the term 'UA' to address military systems falling into the NATO Class II and III categories. UA are typically part of a complex system that can include dedicated Ground Control Stations, Mission Control Elements, multiple aircrews, military-grade communication systems, as well as dedicated infrastructure for logistics and maintenance. UA are usually operated by well-trained personnel, often qualified pilots, to safely operate alongside other airspace users. When addressing not only the aircraft but also other system components or the system as a whole, this book uses the term 'Unmanned Aircraft System' or 'UAS'.

Drone

The term 'drone' is commonly used and widely accepted in the civil domain for all kinds of unmanned systems. Hence, this book uses the term 'drone' to address all types of consumer and com-

mercial systems, which are generally smaller and less complex than their military counterparts. 'Drone' implies that the system is typically operated by a single, not necessarily qualified individual, from a handheld remote control, in relatively close proximity to the aircraft, and under Line-of-Sight (LOS) conditions. Therefore, this book also uses 'drone' for most military systems falling into the NATO Class I category, as their size and complexity is quite comparable to commercially available consumer models and therefore require a similar approach when having to counter them.

Endnotes

1. 'Unmanned Aircraft', Record #7915, NATO Terminology Database, [Online]. Available: https://nso.nato.int/natoterm/Web.mvc. [Accessed 15 Jul. 2019].
2. International Civil Aviation Organization (ICAO), 'International Standards and Recommended Practices, Annex 6, Operation of Aircraft, Part I', 25 Feb. 2013. [Online]. Available: https://www.icao.int/safety/fatiguemanagement/FRMS%20Tools/Amendment%2037%20for%20FRMS%20SARPS%20%28en%29.pdf. [Accessed 15 Jul. 2019].
3. The term Unmanned Aerial Vehicle (UAV) is no longer in use by NATO but is often still used in the civil and public domain.
4. The term Remotely Piloted Aircraft (RPA) is used to indicate that the UA is required to be controlled by a pilot who has been trained and certified to the same standards as a pilot of a manned aircraft.

3

By Lieutenant Colonel André Haider, GE A
Joint Air Power Competence Centre

Unmanned Aircraft System Threat Vectors

Introduction

The threat imposed by UAS is manifold as these systems come in various sizes, shapes and applications. This chapter outlines the broad range of threats which derive from UAS as well as the different environments where NATO has to anticipate their use. This chapter will also discuss threats which are unique to unmanned systems, provide adversaries with new options to challenge NATO and require innovative approaches when having to counter them. The chapter concludes with recent examples of UAS activities which were able to breach the security measures in place at the time.

Proliferation of Unmanned Aircraft Systems

Consumer and Commercial Drones

Unmanned systems available as Commercial-Off-The-Shelf (COTS) products range from very lightweight drones of just barely 100 g to small UAS of up to 150 kg.

Consumer drones first went mainstream around 2011 resulting in a vibrant market for hobbyists and photography enthusiasts and they have seen exponential growth since. Current beginner systems which can carry a usable payload, such as a small camera, start at less than a hundred Euros and are literally available everywhere and affordable for everyone, to include Non-State Armed Actors (NSAA) and terrorist organizations.

As an example, the number of drones in Germany alone has more than tripled from 162,000 to over 600,000 since 2015.[1] Although the consumer market begins to look saturated, the commercial drone industry is expected to show stages of growth that will continue to accelerate over the next few years. Analysts estimate that the global commercial drone market will grow tenfold from 4 billion USD in 2018 to 40 billion USD in 2024.[2]

With the rise of commercial UAS, it can be expected that these drones will incorporate better and more capabilities than consumer versions currently provide. Some of the estimated main markets for commercial systems are agriculture, transport, security and telecommunications.[3] These applications will likely require improved payload, sensing, and automated flight capabilities, which may also enhance the potential threat if these systems were misused.

This development should raise concern as NSAA and terrorist organizations are highly innovative in identifying and adapting new technologies for their purpose. Broadcasting propaganda of successful attacks on the Internet helps these organizations to make other terrorist groups aware of new technologies and eventually disseminate them even further.

Some examples of NSAA and terrorist organizations using commercially available drones are, amongst many others, The Islamic State of Iraq and Syria (ISIS), The Houthi Movement, and even drug cartels in Mexico and South America.

The Islamic State of Iraq and Syria. The group purchased drones through multiple different companies in more than seven countries and can be seen as the originator of the terrorist drone threat. With their supply chain, technical human resources, and own research and development activities, ISIS modified commercial drones into airborne Improvised Explosive Devices (IEDs). At the end of their drone programme, ISIS was able to construct its own drones with an approximate payload of 5 kilograms of explosives. Although the organization had lost most of its territory in its former core areas in Syria and Iraq, other NSAA have started to use drones in the scope of ISIS' drone strategy.[4]

The Houthi Movement. Houthis are evidently more advanced in using technologies than other NSAA. Apart from employing Unmanned Surface Vessels (USV) loaded with explosives against oil trade routes in the region, they also utilize small UAS, allegedly provided by Iran. It has been observed that the Houthis were able to successfully guide artillery fires and missiles with their UAS and hit targets with a level of precision that used to be credited to regular armed forces only.[4]

Drug Cartels. In Mexico, drones have been extensively used for drug trafficking purposes in the region of the Mexico-US border as their use significantly lowers the risk of being caught. The route of the drone is pre-programmed and due to its autonomous capability, it cannot be blocked by electronic jammers at the border. The cartels in Mexico also use so-called potato bombs – hand grenade-sized IEDs – in attacks on each other.[4]

'Those worried about drone proliferation must face facts. We are no longer in a world where only the US has the technology, and we are not moving toward a future in which the technology is used only in the same way we use it now.'

Peter Warren Singer
Director of the Centre for 21st Century Security and Intelligence at the Brookings Institution

---

Military Unmanned Aircraft Systems

Multiple extensive reports on military drone proliferation have been published in recent years, showing that at least 95 countries now maintain active military drone programmes. This is a 58 percent increase within a decade, and there are currently at least 21,000 military drones in operation around the globe.[5, 6, 7, 8]

Apart from the United States, the United Kingdom and Israel being the long-established market leaders in unmanned technology, there are at least 19 countries currently developing or operating military UAS. Amongst these '2nd generation' of unmanned system producers and operators are China and Russia as well as most of the Middle Eastern countries, including Iran. The increasing export of unmanned technology – not only by these states – also raises

concerns about the need for effective control on the proliferation of armed UAS.[7]

Russia. There has been much speculation and misinformation regarding the Russian development of armed drones. A large number of armed UAS have been designed and prototypes put on display, only for those models to never be heard of again. However, allegedly disappeared prototypes such as the Voron, Chirok, Skat, Altius, Inokhodyets, Dozor 600 and Proryv-U show that Russia is actively pursuing significant improvement of its military UAS inventory. Notable UAS programmes include the 'Forpost', several variants of the 'Altius' system and the 'Okhotnik' UCAV, which is strikingly similar to Western concepts such as Northrop Grumman's 'X-47B', Dassault's 'Neuron' or BAE's 'Taranis'. Zala Aero, which is part of the Kalashnikov Group, offers multiple UAS that cover almost all classes and categories, including systems that are specifically designed to operate in extreme climate conditions such as the Arctic. Furthermore, several Russian UAS are especially adapted to navigating without the use of global satellite-based navigation systems, which are often unreliable in Polar Regions. For that purpose, the drones use a newly developed system, GIRSAM, when GPS and GLONASS are not available.[7, 9, 10]

China. China has risen to become one of the foremost producers and exporters of armed UAS, with over half a dozen states now operating strike-capable Chinese systems. According to the Stockholm International Peace Research Institute's (SIPRI) Arms Transfers Database, exports of Chinese 'Wing Loong' and 'CH4-B' strike capable UAS to Egypt, Iraq, Nigeria, Pakistan, Saudi Arabia and the United Arab Emirates have all been confirmed. Many experts suggest that these UAS are copies of the US 'Predator' and 'Reaper' and that the components are not of such high specification as their US counterparts. However, they are much cheaper and sell for a fraction

of the price of the original US systems, making them attractive for customers in the Middle East and elsewhere, e.g. Serbia. Chinese UAS comprise tactical systems such as the 'CH-3' and 'CH-3A', Medium-Altitude Long-Endurance (MALE) variants such as the 'CH4-B', 'CH-5' and 'Wing Loong' series, as well as High-Altitude Long-Endurance (HALE) UAS, such as the 'Cloud Shadow'. Reportedly, all of these systems have similar capabilities if compared to Western UAS, to include BLOS communications via SATCOM, range, endurance, as well as sensor and weapon payloads.[7, 9]

Iran. Separating actual and on-going UAS programmes from rumoured capabilities and stalled or failed prototypes is difficult. However, despite conflicting reports and regardless of trade sanctions from the international community for a number of years, it can be concluded that Iran has indeed developed and manufactured armed UAS, although there is likely less capability than has been projected by Iran itself. Iran's primary UAS is the combat-proven 'Shahed-129', a roughly 'Predator' sized MALE system. It is primarily intended to perform C4ISR missions but can also be employed in attack roles mainly for deploying air-to-surface munitions. The 'Mohajer-6' tactical UAS is the most mature version of its series and in 2018 Iran announced that it had entered serial production for the Islamic Revolution Guards Corps (IRGC). The 'Yasir' is a small UAS, most likely reverse-engineered from a Boeing 'Scan Eagle' which had been captured by Iran in 2012. According to Iranian military commanders during an interview in 2014, the 'Saeqeh' UAS was developed with technology obtained from reverse-engineering an American RQ-170 Sentinel, which was allegedly captured by Iran in 2011. If the 'Saeqeh' has actual combat capabilities is at least questionable and the system itself may be just part of Iran's propaganda. However, the risk that potential adversaries were able to exploit and reverse-engineer Western technology should raise concerns that need to be addressed in future systems.[7, 9, 11, 12, 13, 14]

Non-State Armed Actors. Low, Slow, and Small UAS are already an inherent part of the arsenal of NSAA and terrorist organizations. The proliferation of consumer and commercial LSS UAS with the potential for misuse by these organizations has already been outlined at the beginning of this chapter. However, non-state actors such as Hamas, Hezbollah or the Houthi forces, have reportedly been provided with larger UAS by Iran and other supportive regimes. Conclusively, NATO has to anticipate the employment of larger UAS beyond the LSS spectrum, not only from peer adversaries but also from NSAA and terrorist organizations.[7]

Threat Environments

In contrast to most military disciplines, the challenge of defending against UAS is not limited to a wartime scenario. Rather, a considerable part of C-UAS work will already have to be dealt with as a peacetime task.

Wartime

Not only in a peer to peer conflict scenario but also during lower tiers of escalation between parties to a conflict, adversarial use of unmanned systems against NATO forces has to be anticipated throughout the entire range of UAS classes and capabilities. Especially in the early stages of a developing conflict, UAS may be the preferred choice as they do not involve the risk of human casualties, hence they lower the potential for escalation. On the other hand, this may also lower the threshold of UAS employment, which in turn increases the need for having to counter these systems early on.

In wartime, NATO forces can utilize the complete range of combat activities to counter UAS, limited only – as every combat action – by

International Humanitarian Law (IHL), the Laws of Armed Conflict (LoAC), and the Rules of Engagement (RoE). This does not necessarily mean that countering UAS in wartime would be easier than in peacetime, but the military portfolio of potential actions is significantly broader – to include targeting UAS ground installations and personnel – and the engagement options are less restricted.

Peacetime

The threat from UAS in peacetime can be almost exclusively narrowed down to consumer and commercial drones whereas at the same time, the threat from larger military systems can be almost neglected, assuming that the regular airspace surveillance is sufficient to deter foreign countries from unauthorized entry into the National Airspace System (NAS).

The main challenge of having to counter UAS in peacetime is not defending the airspace, it is rather the problem of detecting drone threats in the first place, and then securing military installations and critical civilian infrastructure from unauthorized intrusion and potential damage, while at the same time, domestic law typically restricts military activities to a minimum. Depending on the respective national regulations, military countermeasures may not be applicable at all and the entire responsibility may lie with the law enforcement agencies, which, in turn, requires very close civil-military cooperation and coordination.

Finally, the protection and safety of the civilian population takes priority over all defensive measures, which considerably limits the 'traditional' options for defending against flying objects. There is simply no acceptable collateral damage in peacetime. Hence, new approaches are required, e.g., to manoeuvre drones to safe locations or to land them in a controlled manner before the final countermeasures can be taken.

General Threats from Unmanned Aircraft Systems

UAS are basically flying platforms which can be equipped with a multitude of sensors and weapons. Depending on their size, this may range from a simple camera up to a full set of guided ordnance on a military system.

Imaging Sensors

The typical sensor on even the smallest consumer drone is a digital camera. However, even non-military UAS, for example, commercial drones used by farmers to monitor their crops and fields can incorporate sophisticated sensors, such as LiDAR (light detection and ranging) or multi-spectral Electro-Optical (EO) cameras. Some of the most relevant imaging sensor types are:

Electro-Optical/Infrared sensors extend from the ultraviolet (UV) through the visible region to the infrared (IR) spectrum. EO/IR systems are depending on the illumination of the target or the target's emission of light. EO/IR sensors are in general sensitive to the environment and depending on the weather conditions, light may be refracted, absorbed or scattered, reducing the quality of the captured image. However, EO/IR sensors can intensify the light waves received and provide imagery also at night.[15]

Synthetic Aperture Radar (SAR) and **Inverse Synthetic Aperture Radar (ISAR)** provide high-resolution imagery independent of daylight, cloud coverage or weather conditions. Through processing, modern SAR systems convert the captured raw data in real-time and provide a perfect vertical view of the target area. In recent years, SAR units have become smaller and more capable as hardware is miniaturized and better integrated, so even smaller systems like Boeing's 'ScanEagle' can provide tactical SAR coverage.[16]

Light Detection and Ranging (LiDAR) is a remote sensing method that uses light in the form of a pulsed laser to measure ranges to the surface. These light pulses generate precise, three-dimensional information about the shape of the Earth and its surface characteristics. There are a multitude of civil and military applications for LiDAR such as terrain and vegetation mapping, mapping beneath forest canopy or water surface, creation of digital surface and city models, or forest height and density measurement.[17, 18]

Multi-/Hyper-Spectrum Sensors. All materials reflect, emit, scatter and absorb electromagnetic waves in a characteristic way. However, only a small portion of this spectrum is visible to the human eye. Military applications include the detection of disturbed soils, which can be an indicator of a buried IED, or revealing the presence of explosive materials. Image processing software can then process the captured image and make the information visible to the human eye.[19, 20]

All of the aforementioned sensors are not limited to military systems only. Commercial, and to a limited extent also consumer systems, may incorporate these sensor capabilities. Conclusively, NATO has to anticipate that basically every UAS may be capable of capturing thermal signatures, mapping terrain and objects through clouds and beneath forest canopies as well as to detect disturbed soil from, for example, tracked vehicle movements.

The broad accessibility to these sensor capabilities can be considered a game-changer as they transform even commercially available consumer drones into a viable threat to NATO operations.

Weapons

Military UAS such as the Chinese CH-x and 'Wing Loong' series, the Russian 'Altius' and 'Okhotnik', or the Iranian 'Shahed-129' are alleg-

edly capable of carrying air-to-ground, and in some cases also air-to-air ordnance.[7] For example, the Russian 'Altius' is expected to support up to two tons of combat payload,[21] whereas Iran is said to have dropped multiple Sadid-345 guided bombs on the Islamic State in Syria with their 'Shahed 129' UAS.[22] However, little is known about these systems' actual capabilities and NATO should anticipate a level of targeting and precision strike abilities which is comparable to own systems.

Consumer and commercial drones are generally unarmed but can be modified to carry serious amounts of explosives, converting them into an airborne IED. They may also be turned into more nefarious weapons by attaching hazardous material such as a nuclear, biological or chemical payload. Unfortunately, criminal and terrorist ingenuity is almost unlimited and difficult to predict. So even small consumer drones require serious attention as they can have considerable destructive potential if they have been modified accordingly.

Target Acquisition and Indirect Fires

Over the last two decades, NATO and its Allies, especially the United States, have proven the effectiveness of UAS and how significantly these systems contributed to linking sensors and shooters. UAS became an integral part in the sequence of Find, Fix, Track, Target, Engage, and Assess (F2T2EA), also often referred to as the 'Kill Chain'. This has not gone unnoticed, and other countries are now incorporating similar Tactics, Techniques, and Procedures (TTP) into their own doctrine.

For example, Russian forces have acquired the capability to use numerous layered sensors to feed into their target acquisition cycle, to include multiple UAS platforms – even COTS products – which relay target data to artillery systems for action. This has been demonstrated in Eastern Ukraine where Russian forces direct and adjust fires with their unmanned systems. Ukrainian forces

have repeatedly seen a systematic approach by the Russians to acquire a target, determine its coordinates, and adjust their artillery fire with UAS in a total timeframe of about 10–15 minutes.[23, 24]

The Russian example shows that mimicking proven Western tactics is not a question of expensive military technology. It can be done quite successfully with only consumer and commercial products.

Therefore, NATO has to anticipate that future adversaries, symmetric as well as asymmetric, will be able to employ some form of viable ISR and targeting capabilities utilizing unmanned systems. Consequently, every UAS or drone sighting in the vicinity of our own forces should raise immediate concerns about being spotted and targeted.

Electronic Warfare

Since 2008, the unifying themes of Russian Armed Forces reforms have been asymmetry and the recognition that the means and methods of modern warfare have changed. From Russia's point of view, its adversaries would seek dominance in the aerospace and information domains, which exponentially enhances the role of Russian Electronic Warfare (EW) to level out NATO's information superiority.[25]

'Relying too much on high-information and electronic technologies made the course and outcome of combat actions increasingly dependent on the condition and functioning standards of computer information and computing networks, knowledge and databases, systems and assets of radio communication, radar, radio navigation used in systems of state and military control, reconnaissance, and control of weapons, particularly high-precision ones.'[25]

Major General Yury Lastochkin
Chief of the Russian Electronic Warfare Force

Although EW systems are mostly mounted on ground vehicles, some variants of Russian and Chinese UAS are allegedly capable of carrying EW payloads to employ them with more agility and at longer ranges than the systems on the ground.

The Russian 'Orlan-10', for example, can be equipped with an EW suite as part of the Leer-3 EW system, enabling it to disrupt GSM signals within a radius of six kilometres. In addition, the UAS can imitate a cellular base station, forcing connections from nearby devices, analysing their transmissions and locating their position.[26]

The Chinese 'Wing Loong II' appears to come in a SIGINT variant as well. Pictures of a circular antenna array fitted underneath the fuselage indicate that the system could be capable of intercepting communication signals while providing a bearing of the transmitting signal.[27]

Unique Threats from Unmanned Aircraft Systems

Swarming

Unmanned systems are typically cheaper than manned aircraft, especially if consumer and commercial products are taken into account. This price advantage creates the opportunity to acquire multiple times more UAS than manned combat aircraft. Grouping together multiple UAS creates a so-called 'swarm' and depending on their numbers, they are expected to cause significant challenges for current Air Defence systems. For example, in January 2018, an improvised swarm of ten drones rigged with explosives was employed in a coordinated assault against Russia's Hmeimim airbase in western Syria. The drones appeared to have been assembled from a small engine, cheap plywood and a number of small mortar

shells and were allegedly launched from a site more than 50 kilometres away. Although all of the drones were eliminated or forced to land, this incident has proven that the concept of swarming is a viable threat, even when using improvised devices.[4, 28]

Autonomy

True autonomy in terms of having a robot or machine making an informed decision by itself has not yet been achieved. However, the technology to create fully automated systems that use pre-programmed algorithms to process the robot's sensor inputs is readily available. Highly automated systems are typically perceived as 'autonomous' because their behaviour is seemingly unpredictable. In fact, it is not the system but the environment in which it operates which is unpredictable, leading to changing sensor inputs and thus, varying actions by the automated system.[29]

One example of an autonomous UAS is the Israeli Aerospace Industries' (IAI) 'Harpy', an anti-radiation loitering munition that can autonomously home in on radio emissions. The 'Harpy' is designed to loiter over the battlefield for about six hours and attack targets by self-destructing into them or returning home, if no target could be engaged during the duration of the mission. China purchased an undisclosed number of 'Harpy' drones in 1994 and unveiled a reverse-engineered version of the system, the ASN-301, during a military parade in 2017, which appears to be a near copy of the original.[30]

Moreover, even today's consumer products incorporate highly automated functions, such as active detecting, tracking and following of persons and objects, or waypoint navigation with autonomous trajectory calculation and active obstacle avoidance based on the drone's sensor inputs.[31]

Both categories, commercially available drones as well as military UAS, should be considered 'autonomous' in the way that they probably no longer require a permanent command and control link to fulfil their mission. This eliminates many of the current countermeasures which rely on jamming their radio transmissions.

Lower Operational Threshold

Unmanned systems offer three principal advantages over manned systems concerning the operational threshold when projecting military force.

Reduced Risk. Minimizing the risk of losing a human pilot has been the driving factor for developing UAS. Because there is no human on board, there is no casualty if the UA is shot down or captured by enemy forces.

Expendability. Compared to manned aircraft, UAS come at a significantly lower cost. Some tactical UAS, but especially smaller systems, are specifically designed for expendability and some of them are not even considered for reuse.

Less Potential for Escalation. Employing UAS to penetrate foreign airspace and to gather intelligence bears less risk of escalating an emerging crisis as no humans get killed if a UAS is shot down.

These three factors contribute to the fact that the operational threshold for deploying these systems against NATO is likely to be lower than using manned aircraft. Therefore, NATO should anticipate the employment of military-grade UAS already during a developing crisis.

Recent Examples of Unmanned Aerial Threats

Germany, 2013
Drone Crash Landing in Front of German Chancellor

At a campaign rally in Dresden on 15 September 2013, a small quadcopter flew within a few feet of German Chancellor Angela Merkel and Defence Minister Thomas de Maiziere, hovering briefly in front of them before crashing into the stage practically at Merkel's feet. Fortunately, the quadcopter, a Parrot AR drone, was harmless. The person who was operating the drone from a nearby hide-out was quickly located by the police and briefly taken into custody for being accused of disturbing the event.[32, 33]

Great Britain, 2018
Closure of Gatwick Airport

Between 19 and 21 December 2018, hundreds of flights were cancelled at Gatwick Airport near London, England, following reports of drone sightings close to the runway. The reports caused major disruption, affecting approximately 140,000 passengers and 1,000 flights. A Sussex Police spokesman said: 'The incident was not deemed terror-related and there is no evidence to suggest it was either state sponsored, campaign or interest-group led. Through corroborated witness statements, it is established that at least two drones were in operation during this period, and the offender, or multiple offenders, had detailed knowledge of the airport.'[34, 35]

Venezuela, 2018
Alleged Assassination Attempt on Venezuelan President

On 4 August 2018, attackers used two DJI M600 drones, each carrying a kilogram of C-4 explosive, to reportedly conduct an attack

on the Venezuelan President Nicolas Maduro while he was giving a speech at a military parade in Caracas. If confirmed, this had been the world's first known attempt to kill a head of state with a retail drone, purchased online and manually weaponized with military-grade explosives. However, the legitimacy of the assassination attempt is doubted and various countries asked for an independent investigation.[36, 37, 38]

Great Britain, 2017
Drone Landing on British Aircraft Carrier

In August 2017, an amateur photographer flew his DJI Phantom across the Invergordon harbour to take some imagery of the Royal Navy's docked aircraft carrier HMS Queen Elizabeth. When the drone sensed a high wind risk, it landed itself on the flight deck. After taking pictures from the deck, the photographer managed to fly the drone back safely. The pilot was aware he had broken rules on flying too close to the ship and reported himself to armed police guards at the entrance to the shipyard.[39, 40]

Saudi Arabia, 2019
Attack on Saudi Oil Refinery

On 14 September 2019, Saudi oil facilities were severely damaged by a combined UAS and cruise missile strike which led to the interruption of an estimated 5.7 million barrels of the kingdom's crude oil production per day, equivalent to more than 5% of the world's daily supply. The Iranian-backed Houthi rebels in Yemen publicly claimed responsibility for the attack. However, a United Nations' investigation concluded that the UAS and land-attack cruise missiles used in the attack did not have sufficient range to have been launched from Yemeni territory nor had the Houthis been shown to be in possession of the type of UAS used in the attacks.[41, 42, 43]

Summary

UAS and drones have proliferated to such an extent, that their use against own forces must be anticipated literally anywhere, anytime and from any potential adversary. This includes both wartime and peacetime and will occur inside and above NATO territory as well as abroad. The capabilities of even consumer drones have reached a more than sufficient enough level of technology to use them as efficient tools for ISR, targeting and directing of fires. Potential adversaries are actively pursuing to mimic Western UAS designs and their respective warfighting tactics and it would be negligent to underestimate their fast-developing capabilities.

Endnotes

1. German Aviation Association, 'Analysis of the German Drone Market', [Online]. Available: https://www.bdl.aero/en/publication/analysis-of-the-german-drone-market/. [Accessed 27 Feb. 2020].
2. Patrick McGee, 'How the commercial drone market became big business', Financial Times, 27 Nov. 2019. [Online]. Available: https://www.ft.com/content/cbd0d81a-0d40-11ea-bb52-34c8d9dc6d84. [Accessed 27 Feb. 2020].
3. Business Insider Intelligence, 'Commercial Unmanned Aerial Vehicle (UAV) Market Analysis – Industry trends, forecasts and companies', Business Insider, 10 Feb. 2020. [Online]. Available: https://www.businessinsider.com/commercial-uav-market-analysis?r=DE&IR=T. [Accessed 27 Feb. 2020].
4. Serkan Balkan, 'A Global Battlefield?: Rising Drone Capabilities of Non-State Armed Groups and Terrorist Organizations', SETA Foundation for Political, Economic and Social Research, Istanbul, 2019.
5. Aniseh Bassiri Tabrizi and Justin Bronk, 'Armed Drones in the Middle East: Proliferation and Norms in the Region', Royal United Services Institute for Defence and Security Studies (RUSI), Dec. 2018. [Online]. Available: https://rusi.org/sites/default/files/20181207_armed_drones_middle_east_web.pdf.
6. John Borrie, Elena Finckh and Kerstin Vignard, 'Increasing Transparency, Oversight and Accountability of Armed Unmanned Aerial Vehicles', United Nations Institute for Disarmament Research (UNIDIR), 1 Dec. 2017. [Online]. Available: https://www.unidir.org/publication/increasing-transparency-oversight-and-accountability-armed-unmanned-aerial-vehicles.
7. Johanna Frew, 'Drone Wars: The Next Generation', Drone Wars UK, May 2018. [Online]. Available: https://dronewarsuk.files.wordpress.com/2018/05/dw-nextgeneration-web.pdf.
8. Dan Gettinger, 'The Drone Databook', Center for the Study of the Drone at Bard College, 2019. [Online]. Available: https://dronecenter.bard.edu/projects/drone-proliferation/databook/.
9. 'Military Unmanned Systems Market Analysis', Military Unmanned Systems Handbook, no. 27, pp. 4-12, 2019.
10. Nurlan Aliyev, 'Russia's Military Capabilities in the Arctic', International Centre for Defence and Security (ICDS), 25 Jun. 2019. [Online]. Available: https://icds.ee/russias-military-capabilities-in-the-arctic/. [Accessed 2 Mar. 2020].
11. 'Jane's analyses the Shahed 129 and Hamaseh', Jane's, 24 Sep. 2019. [Online]. Available: https://ihsmarkit.com/research-analysis/Janes-analysis-shahed129-Hamaseh.html. [Accessed 2 Mar. 2020].

12. 'IAIO Yasir (Yasseer)', MilitaryFactory.com, 20 Jul. 2017. [Online]. Available: https://www.militaryfactory.com/aircraft/detail.asp?aircraft_id=1331. [Accessed 2 Mar. 2020].
13. Wim Zwijnenburg, 'Sentinels, Saeqehs and Simorghs: An Open Source Survey of Iran's New Drone in Syria', Bellingcat, 13 Feb. 2018. [Online]. Available: https://www.bellingcat.com/news/mena/2018/02/13/sentinels-saeqehs-simorghs-open-source-information-irans-new-drone-syria/. [Accessed 2 Mar. 2020].
14. Jeremy Binnie, 'Iranian army deploys armed UAVs', Jane's Defence Weekly, 18 Jul. 2019. [Online]. Available: https://www.janes.com/article/89947/iranian-army-deploys-armed-uavs. [Accessed 2 Mar. 2020].
15. G. Koretsky, J. Nicoll and M. Taylor, 'A Tutorial on Electro-Optical/Infrared (EO/IR) Theory and Systems', Institute for Defense Analyses, 2013. [Online]. Available: https://www.ida.org/-/media/feature/publications/a/at/a-tutorial-on-e-lectro--opticalinfrared-eoir-theory-and-systems/ida-document-d-4642.ashx. [Accessed 3 Mar. 2020].
16. Microwaves and Radar Institute of the German Aerospace Center (DLR) et al., 'A Tutorial on Synthetic Aperture Radar', IEEE Geoscience and remote sensing magazine, pp. 6-43, 2013.
17. 'What is LIDAR?', National Oceanic and Atmospheric Administration (NOAA), 7 Jan. 2020. [Online]. Available: https://oceanservice.noaa.gov/facts/lidar.html. [Accessed 3 Mar. 2020].
18. 'The uses of LiDAR', LiDAR UK, 2020. [Online]. Available: http://www.lidar-uk.com/usage-of-lidar/. [Accessed 3 Mar. 2020].
19. Philippe Lagueux, Alexandre Vallières, André Villemaire, Martin Chamberland, Vincent Farley and Jean Giroux, 'Chemical Agent Standoff Detection and Identification with a Hyperspectral Imaging Infrared Sensor', SPIE – The International Society for Optical Engineering, Oct. 2007. [Online]. Available: https://www.researchgate.net/publication/258293528_Chemical_agent_detection_and_identification_with_a_hyperspectral_imaging_infrared_sensor. [Accessed 3 Mar. 2020].
20. Bora M. Onat, Gary Carver, Mark Itzler, 'A solid-state hyperspectral imager for real-time standoff explosives detection using shortwave infrared imaging', SPIE - The International Society for Optical Engineering, May 2009. [Online]. Available: https://www.researchgate.net/publication/228727726_A_solid-state_hyperspectral_imager_for_real-time_standoff_explosives_detection_using_shortwave_infrared_imaging. [Accessed 3 Mar. 2020].
21. Karl Soper, 'New UAVs completing Russian state testing', Jane's, 15 May 2018. [Online].
22. Babak Taghvaee, 'Sadid-345 Smart Bomb is now main weapon of the #IRGC Air & Space Force's Shahed-129 UCAVs', Twitter, 27 Jun. 2017. [Online]. Available: https://twitter.com/BabakTaghvaee/status/879694011866525696. [Accessed 6 Apr. 2020].
23. A.W.G. US Army, Russian New Generation Warfare Handbook (U/FOUO), Fort Meade, MD 20755, Dec. 2016, [extracted information is unclassified].
24. Roger McDermott, 'Russia's Armed Forces Rehearse New 'Shock-Fire' Tactics', The Jamestown Foundation, 6 Mar. 2018. [Online]. Available: https://jamestown.org/program/russias-armed-forces-rehearse-new-shock-fire-tactics/. [Accessed 5 Mar. 2020].
25. Roger McDermott, 'Russia's Evolving Electronic Warfare Capability: Unlocking Asymmetric Potential', The Jamestown Foundation, 17 Apr. 2018. [Online]. Available: https://jamestown.org/program/russias-evolving-electronic-warfare-capability-unlocking-asymmetric-potential/. [Accessed 5 Mar. 2020].
26. 'STT Orlan', Jane's, 18 Oct. 2019. [Online]. [Accessed 5 Mar. 2020].
27. 'AVIC Wing Loong series', Jane's, 12 Dec. 2019. [Online]. [Accessed 5 Mar. 2020].
28. David Reid, 'A swarm of armed drones attacked a Russian military base in Syria', CNBC, 11 Jan. 2018. [Online]. Available: https://www.cnbc.com/2018/01/11/swarm-of-armed-diy-drones-attacks-russian-military-base-in-syria.html. [Accessed 5 Mar. 2020].
29. André Haider and Maria B. Catarrasi, 'Future Unmanned System Technologies: Legal and Ethical Implications of Increasing Automation', Joint Air Power Competence Centre (JAPCC), Kalkar, 2016.
30. Elsa Kania, 'The PLA's Unmanned Aerial Systems', China Aerospace Studies Institute at Air University, Montgomery, AL 36112, 2018.
31. 'P4P V2.0', DJI, [Online]. Available: https://www.dji.com/de/phantom-4-pro-v2. [Accessed 9 Mar. 2020].
32. Sean Gallagher, 'German chancellor's drone 'attack' shows the threat of weaponized UAVs', Ars Technica, 9 Sep. 2013. [Online]. Available: https://arstechnica.com/information-technology/2013/09/german-chancellors-drone-attack-shows-the-threat-of-weaponized-uavs/. [Accessed 10 Mar. 2020].

33. Friederike Heine, 'Merkel Buzzed by Mini-Drone at Campaign Event', Der Spiegel, 16 Sep. 2013. [Online]. Available: https://www.spiegel.de/international/germany/merkel-campaign-event-visited-by-mini-drone-a-922495.html. [Accessed 10 Mar. 2020].
34. 'Gatwick Airport: Drones ground flights', BBC, 20 Dec. 2018. [Online]. Available: https://www.bbc.com/news/uk-england-sussex-46623754. [Accessed 10 Mar. 2020].
35. 'People behind drone chaos had 'detailed knowledge' of Gatwick', The Guardian, 27 Sep. 2019. [Online]. Available: https://www.theguardian.com/uk-news/2019/sep/27/gatwick-drone-disruption-perpetrators-detailed-knowledge-airport-police-report. [Accessed 10 Mar. 2020].
36. Nick Paton Walsh, Natalie Gallón, Evan Perez, Diana Castrillon, Barbara Arvanitidis and Caitlin Hu, 'Inside the August plot to kill Maduro with drones', CNN, 21 Jun. 2019. [Online]. Available: https://edition.cnn.com/2019/03/14/americas/venezuela-drone-maduro-intl/index.html. [Accessed 10 Mar. 2020].
37. Christoph Koettl and Barbara Marcolini, 'A Closer Look at the Drone Attack on Maduro in Venezuela', The New York Times, 10 Aug. 2018. [Online]. Available: https://www.nytimes.com/2018/08/10/world/americas/venezuela-video-analysis.html. [Accessed 10 Mar. 2020].
38. Uta Thofern, 'Venezuela on the verge of imploding', Deutsche Welle, 5 Aug. 2018. [Online]. Available: https://www.dw.com/en/opinion-venezuela-on-the-verge-of-imploding/a-44960051. [Accessed 10 Mar. 2020].
39. 'Unauthorised Drone Lands On HMS Queen Elizabeth', Forces Net, 12 Aug. 2017. [Online]. Available: https://www.forces.net/news/unauthorised-drone-lands-hms-queen-elizabeth. [Accessed 10 Mar. 2020].
40. Harry Yorke, 'Drone enthusiast 'amazed' as he lands device on deck of £3bn HMS Queen Elizabeth without being detected', The Telegraph, 12 Aug. 2017. [Online]. Available: https://www.telegraph.co.uk/news/2017/08/12/drone-enthusiast-avoids-detection-lands-vehicle-3bn-hms-elizabeth/. [Accessed 10 Mar. 2020].
41. Ryan Pickrell, 'The devastating attack on Saudi oil plants confirms the worst fears about low-tech drones in the wrong hands', Business Insider, 16 Sep. 2019. [Online]. Available: https://www.businessinsider.com/drones-strikes-in-saudi-arabia-a-wake-up-call-experts-2019-9. [Accessed 10 Mar. 2020].
42. Michelle Nichols, 'U.N. unable to verify that weapons used in Saudi oil attack were from Iran', Reuter, 11 Dec. 2019. [Online]. Available: https://www.reuters.com/article/us-saudi-aramco-attacks-un-idUSKBN1YE2UD. [Accessed 10 Mar. 2020].
43. Michelle Nichols, 'U.N. investigators find Yemen's Houthis did not carry out Saudi oil attack', Reuters, 8 Jan. 2020. [Online]. Available: https://www.reuters.com/article/us-saudi-aramco-attacks-un-exclusive/exclusive-u-n-investigators-find-yemens-houthis-did-not-carry-out-saudi-oil-attack-idUSKBN1Z72VX. [Accessed 10 Mar. 2020].

4

By Lieutenant Colonel André Haider, GE A
Joint Air Power Competence Centre

The Vulnerabilities of Unmanned Aircraft System Components

Overview

Unmanned Aircraft share basically the same vulnerabilities as manned aircraft. However, it is not only the UA which can be subject to countermeasures. Each individual component of an Unmanned Aircraft System (UAS) has unique vulnerabilities and could be targeted to counter the UAS threat. This chapter describes the different system components, their limitations and vulnerabilities, as well as potential countermeasures against them. The countermeasures themselves will then be discussed in the respective subsequent chapters of this book.

Unmanned Aircraft

General Characteristics

Unmanned Aircraft is the overall term for all aircraft that do not carry a human operator and are operated remotely using varying levels of automated functions.[1] However, the prevalent terminology in the civilian domain is 'drone', which is almost always used for the respective consumer and commercial UA variants. For the purpose of distinction, this chapter will use the terms 'Unmanned Aircraft' (UA) and 'Unmanned Aircraft System' (UAS) to indicate military-grade systems, and 'drone' for commercial or consumer products.

Unmanned Aircraft. Most of the current UA share design principles that seek to optimize long endurance and low fuel consumption. The most prominent features are wings with a very high aspect ratio combined with a rear-mounted, fuel-efficient propeller engine. Together, these provide the desired flight characteristics, but also bring with them certain disadvantages. High aspect ratio wings have a fairly high amount of inertia preventing UA from conducting flight manoeuvres with a high roll angular acceleration and G-force.[2] Additionally, the average cruising speed of propeller-driven UA is quite low, e.g. 60 knots for the Russian 'Forpost' or estimated 80 knots for the Chinese Wing Loong.[3, 4] Therefore, the UA is unable to conduct 'last-ditch' manoeuvres and becomes a rigid target compared to manned fighter aircraft.

Drones. Smaller systems are typically rotorcraft which feature four or more propellers to keep them airborne. This design allows for easy take-off and landing, lower airspeeds, and hovering the drone in mid-air. Together with an easy to use remote control, e.g. a mobile phone or tablet computer application, this design enables

consumers such as hobbyists, farmers or photographers to operate drones with ease and without the detailed knowledge and airmanship military UAS require. Drones are generally susceptible to weather conditions, especially strong winds, due to their lightweight and size. However, their size and weight make them also highly agile compared to fixed-wing UAS.

Visibility to Radar Systems

The visibility of an object to a radar system is measured by the Radar Cross Section (RCS). RCS is defined as the measure of a target's radar signal reflectivity in the direction of the radar receiver.[5, 6]

Unmanned Aircraft. Larger UAS like the Wing Loong, an almost exact replica of the MQ-1 Predator design, can be expected to display an average RCS of slightly less than one square meter which is comparable to non-stealth fighter aircraft.[7, 8, 9] Although prototypes such as the Russian Okhotnik seemingly incorporate stealth technology, the vast majority of current systems lack any of these features.

Figure 4.1: Chinese Wing Loong (l.) and US MQ-1B Predator (r.).

Drones. In contrast to UAS, the radar reflectivity of drones is relatively low. Due to their small size, the majority of plastic components and generally lower operating altitude, they challenge most traditional air surveillance radars.

Visibility in the Infrared Spectrum

Hot engine parts, exhaust plumes, the rear fuselage area, and aerodynamically heated skin are the key sources of aircraft infrared (IR) emissions. In general, aircraft with a jet engine have the highest IR intensity.[10]

Unmanned Aircraft. The majority of UAS configurations have a turboprop engine fitted to the back of the UA, dispersing the exhaust through the pusher propeller. Compared to a turbojet-powered aircraft, this design results in a much lower IR signature. However, UAS are not necessarily resistant to attacks by IR-guided missiles. Modern IR-detection technology with its increased sensitivity is capable of detecting IR radiation in a wide enough spectrum to spot lower IR signatures from UAS.[11, 12]

Drones have very low IR emissions due to their typically battery-powered propulsion. However, most objects have a different temperature than the environment they are operating in. Therefore, thermal imaging will most likely reveal the presence of a drone,[13] although not at the longer distance where a hot engine exhaust can be detected. The very low IR signature may also be not sufficient for an IR-guided missile.

Acoustic Detectability

Propeller noise can be measured by ground-based stationary microphones which use the Doppler Effect in the acoustic spectrum to compute an aircraft's altitude, speed and actual revolutions per minute of the engine. Real-time computations on such signals can provide the direction or location of the sound source.[14]

Unmanned Aircraft. Many UAS are propeller-driven and generate a significant amount of noise. Depending on their altitude, the noise emissions can be so strong, the propeller noise alone may attract the attention of ground personnel.[15, 16] However, UAS operating at higher altitudes are typically no longer audible for humans and require dedicated acoustic sensors to be detected.

Drones emit significantly less noise than a UAS equipped with a turboprop engine. However, the noise level is still loud enough to be audible at shorter distances. The typical sound level of a consumer drone is between 70 dB and 80 dB, measured at a distance of one metre. This is comparable to a motorized lawnmower. If the distance to a sound source is doubled, the sound pressure level drops by 6 dB. Figure 4.2 shows this formula applied and how the noise level will fall below the threshold of 20 dB at a distance of approximately 350 m for the 70 dB drone and 1,000 m for the 80 dB drone, which means that the average environmental noise in a quiet rural area will be loud enough to mask the remaining noise of the drone.[17, 18]

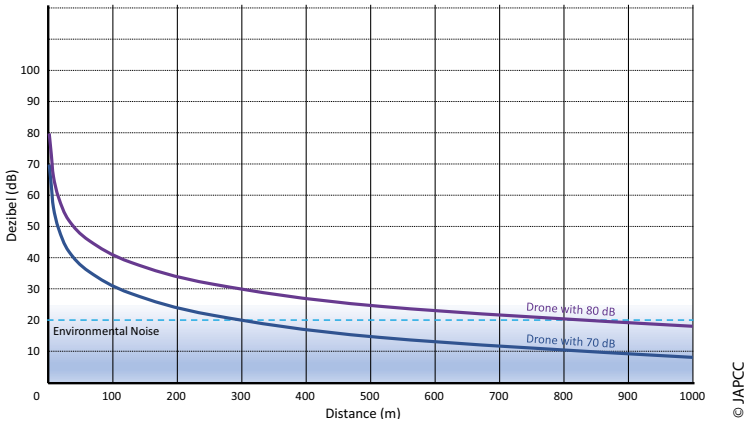


Figure 4.2: Average Consumer Drone Audibility.

Visual Recognition

The range at which aircraft can be detected, recognized and identified varies with the size, shape and colour of the aircraft, viewing aspect, visibility conditions, its motion relative to and contrast with the background and eventually, the visual acuity of the observer. Depending on these factors, the aircraft can be seen at long ranges in clear weather. When there is rain, snow, fog, dust or haze, the visibility range may be reduced to zero.[19, 20]

Unmanned Aircraft. The largest distance at which an aircraft can be seen by the human eye can be mathematically predicted from its size and contrast to the background. Given a perfect black & white contrast, an MQ-9 Reaper sized UAS, like the Wing Loong II, can be visually detected at a distance of almost 10 km, whereas lowering the contrast to 50 % reduces the detection range to roughly half. As military aircraft are typically camouflaged or painted grey to blend in with the surrounding sky, it can be assessed that visual detection of UAS without electro-optical support is limited to ranges of less than 5 km and is unlikely at altitudes above 15,000 ft.[21]

Drones. The challenge with visual detection of drones is their small size and discriminating them from different moving objects such as birds or even a plastic bag caught in the wind. It is most likely, that a drone will be heard before it will be spotted and typically the noise of a nearby drone is the trigger for visual recognition.

Payload

UA and drone payloads consist primarily of imaging sensors and – if applicable – a set of weapons. Payloads also have vulnerabilities, or better labelled 'limitations', which can be

exploited too, for example, disrupting sensors, or misdirecting the UA's weapons.

Sensors

Every sensor has specific characteristics of how it perceives its environment and how it processes that input into a human-readable output. The sensor input is typically limited to a certain type of radiation and its respective wavelength. Disrupting a sensor requires either masking the specific wavelength or using the same wavelength against the sensor to inject false information or blind it.

Chapter 3 (cf. p. 41 ff.) outlines the most prevalent types of UAS sensors and their specific characteristics. Most of the time, it might be more favourable to mask a certain range of wavelengths than to blind the sensor as active countermeasures may draw unwanted attention from the UA or drone. Traditional measures such as camouflage, light discipline, or dispersion of troops may be sufficient to counter an electro-optical camera. Reportedly, the Taliban in Afghanistan mitigated their risk of detection by US Predator and Reaper UAS by simply parking their trucks below trees and covering them with mattresses to suppress IR radiation from the hot engine. More sophisticated sensors, e.g. LIDAR or SAR, definitely require more complex countermeasures to reflect or absorb radiation in their sensing spectrum.

Weapons

UAS can basically carry every type of air-to-air and air-to-ground ordnance, limited only by its Size, Weight, and Power (SWaP) restrictions. It should go without saying that countering a weapon should be the very last option in the overall C-UAS approach.

Modern weaponry is typically guided by some precision enhancing method (Global Positioning System (GPS), internal Inertial Navigation System (INS) or Laser spot tracking). Terminal guidance can be based on imagery, light radiation (IR, Laser), or radar reflections. In general, the same principles about radiation and wavelengths as discussed in the sensor section above apply to guided weapons as well. However, a more active approach is required to misdirect an already released weapon. Laser and radar guidance require clear reflections from their intended target to hit accurately. IR guidance also requires a sufficient contrast between the IR source and its environment. Scattering or delaying reflections in the respective spectrum may induce significant enough error to the guidance system so that the weapon would miss the intended target.

Satellite-aided inertial-guided ammunition utilizes the Position, Navigation, and Timing (PNT) signals provided by at least one of the three respective satellite constellations, i.e. GPS (USA), GLONASS (RUS), and BEIDOU (CHN). The weaknesses and limitations of these systems will be discussed in more detail in Chapter 12 (cf. p. 209 ff.).

Every ordnance, guided as well as unguided, is susceptible to reflecting radar emissions and has a unique trajectory which is clearly distinguishable from natural objects. Depending on their amount of metal components and overall size, radar reflections may be quite low. However, these reflections are still above any LSS drone, and their speed and trajectory can help defenders in discriminating them from the environment and to detect the imminent threat.

Stand-off Limitations

The maximum functional distance of an imagery sensor, and in turn the UA, depends on the operational requirements of the

desired target resolution. A higher target resolution requires a smaller Ground Resolved Distance (GRD), which is, simply put, the smallest surface area a single image pixel can display. The GRD should be at least half of the size of the smallest detail which is required to be measured for the mission. For example, when trying to detect (not identify) persons on the ground, the GRD should be no larger than half of the width of the human body, which equates to roughly 40 cm per pixel.[22, 23] This resolution can be achieved by even legacy cameras at distances of roughly 55,000 ft.[24] However, the average operational altitude of MALE UAS is in the range of 20,000 ft to 25,000 ft to provide sufficient GRD for positive target identification,[25] and, depending on haze, dust and other vision-obscuring conditions, the effective range can be even considerably lower.

The maximum range of non-propelled ammunitions, such as guided or unguided bombs, depends exclusively on the airspeed and altitude of the delivery platform. Current propeller-driven MALE UAS have a maximum speed of about 200 kts.[26] Modern manned fighter aircraft are capable of bomb releases at high subsonic or even supersonic speeds and higher altitudes. The total potential (altitude) and kinetic (airspeed) energy of the weapon at release are the main contributors to its maximum range. Consequently, the same type of non-propelled ammunition will have a shorter range if released from a UA than if released from a manned fighter aircraft.

Limited Situational Awareness

The UAS' sensors are the only direct source of information to build situational awareness. Although the sensor suite can take a very detailed look at a very small area, the viewer has no awareness of anything outside the 'soda straw' field of view of the aircraft's

sensors. Boresight cameras mounted on the UA's nose or tail provide the crew with a broader view of the flight direction, but they still do not receive the kind of cues they get from their proprioceptive senses.[27, 28, 29]

Additionally, UAS sensors are generally not designed for threat detection. In conjunction with the overall limited situational awareness, this is a fundamental vulnerability. The typical mission sets for ISR UAS in the relatively benign environments of the last decade have led to a focus on the improvement of sensor payloads rather than on the development of self-protection capabilities.[30] Although self-protection suites used on manned aircraft are available, few, if any, UAS are currently equipped with them.

Human Element

Although the UA itself does not carry a human crew, there are a lot of personnel involved in the operation of UAS. Hence, attacking the personnel rather than the UA itself may also be a favourable option. UAS personnel can be classified into three categories: The Launch and Recovery Unit (LRU), the Mission Control Element (MCE) and the Processing, Exploitation, and Dissemination (PED) element.

Launch and Recovery Unit

Depending on the UA's effective range, the LRU usually has to be located into or near the Area of Operations (AOO). For smaller UAS, the LRU is most likely deployed inside the AOO. For larger HALE and MALE systems with higher effective ranges and airspeeds, the LRU may be deployed to a neighbouring host nation. Launching and recovering UA requires a Line of Sight (LOS) data

link from a local Ground Control Station (GCS) and suitable airport infrastructure with a decent sized runway. Like for any other military aircraft, additional personnel for refuelling, arming and performing maintenance are needed as well. This infrastructure is likely to be well defended; however, a successful attack on an LRU will disrupt any UAS operations significantly.

Mission Control Element

Larger military UAS are typically capable of operating Beyond Line of Sight (BLOS) after transferring control from the LRU via satellite to a remotely-based MCE, which can be deep inside the enemy's territory. Home-based UAS personnel are subject to the protection of their country's territory, which makes access more difficult than inside or near the AOO.

Processing, Exploitation and Dissemination Element

The data links that enable UAS to be operated BLOS also permit conducting PED from afar, via any network attached to the UAS. Many nations operating UAS use some kind of central 'reach back' intelligence organization to conduct their PED. This is due to the vast amount of imagery and Full Motion Video (FMV) delivered by current UAS. Like the MCE, they also enjoy the protection of their home country's security environment.

Off-Duty Personnel

As briefly outlined above, UAS personnel working in the MCE and PED element are more difficult to access than if they were inside the AOO. However, the perceived threat level and actual level of alert for military installations in the home country may be lower compared to that of deployed forces, which may be exploited for

own countermeasures. Additionally, MCE and PED personnel usually have the option of leaving the protected military environment while off-duty, which, in fact, does not change their status as combatants and legal targets. This provides a window of opportunity to strike when the individual is most vulnerable. Individual targets may be identified by traditional intelligence, but also by exploiting social media and the internet. Additionally, they may be identified by name tags, unit patches, or special insignia which some countries award to their UAS operators.

Control Element

The Control Element consists of its physical infrastructure (hardware) and a non-physical (software) component. Both may be subject to different types of countermeasures. The physical part may be subject to kinetic countermeasures while the non-physical part may be subject to countermeasures in the cyber domain.

External Hardware Components

The Control Element's prominent hardware components typically consist of a shelter or trailer containing the controls to operate the UA and a satellite earth terminal for BLOS communications. Due to their unique size and shape, the hardware components may serve as a means to positively identify them as UAS components. Additionally, their persistent radio transmissions may also reveal their location to electronic reconnaissance.

Non-deployable GCS integrated into existing infrastructure can make them indistinguishable from other multi-purpose buildings; however, roof-mounted communication equipment may reveal the purpose of the building. The most prominent characteristics

Figure 4.3: Potential Satellite Ground Terminals at Hmeimim Airbase, Syria.

of any GCS are the BLOS satellite earth terminals which can have antenna diameters of several metres. Communication antennas of this size are easily recognizable since they require a minimum safety distance from surrounding equipment and personnel due to the radiation hazard. Fixed installations of satellite earth terminals could even be identified by using publicly available satellite imagery.

Software Components

To destroy, disrupt or infiltrate the software portion of the Control Element, potential countermeasures must first gain access to the network, either directly or remotely. The software components necessary to operate a UAS are not limited to the GCS, but also include the aircraft, satellites and ground stations if applicable, as well as support systems for logistics, maintenance or PED. This provides a broad spectrum of possible entry points into the UAS network.[31]

To gain access to these software components, human weaknesses may be exploited. According to the adage, 'a chain is always only as strong as its weakest link', even highly secured and physically separated military networks may be infiltrated through the identification of individual personnel that can be persuaded to support own countermeasures.

Data Link

Data links connect the UA with the GCS which enables operators to remotely control the UA and receive transmissions. Data links can be established either by radio for LOS communications or satellites and network nodes for BLOS communications. The radio transmissions may be subject to attack by EW, whereas the network nodes may be attacked by means of cyber warfare. The UAS' vulnerabilities in the cyber domain have been outlined in the previous chapter. These same tactics also apply to the data link's network nodes used for BLOS communications. Therefore, this chapter focuses on the vulnerabilities of UAS radio transmissions only.

Unmanned Aircraft

UA typically use two or more antennas to maintain the data link between the GCS and the satellite. Antennas to receive signals from the GCS face downwards and may be directional and/or omnidirectional. Antennas to receive satellite signals face upwards and are typically directional.[32] Because the omnidirectional LOS antennas are usually only used for launch and recovery, the timeframe to interfere with the LOS data link is quite short. However, especially during the landing phase, the UA is highly vulnerable to a possible data link loss. The directional antenna for satellite communications can be considered less vulnerable to ground-based

electromagnetic interference than either its main lobe or side lobes which face the ground. Successfully injecting signals into the UA's satellite antenna requires either airborne or space-based EW assets.

Ground Control Station

Like the UA, the GCS uses separate, directional antennas for LOS and BLOS communications. Depending on the position of the UA or satellite, the LOS and BLOS antenna may have to be aimed at shallow angles and in the direction of NATO forces, which exposes the main lobe to electromagnetic interference. Maintaining LOS communication with a low flying UA during recovery makes the LOS antenna even more susceptible to electronic attack. As previously discussed, disrupting LOS communication during recovery operations may result in the loss of the aircraft.

Satellite

Geostationary communication satellites usually cover a large area of the Earth's surface. To disrupt satellite communications, spurious signals could be transmitted from any location inside the satellite's footprint. Military-grade equipment is not necessarily required to conduct an electronic attack on receiving antennas. Any civilian broadcasting station is capable of interfering with the satellite uplink.[33]

Satellite Ground Segments

Countermeasures against the satellite ground segments can disrupt the respective space assets. Critical ground control facilities associated with space systems, both military and civilian, are valid targets if operated in support of an adversary's armed forces. NATO needs to identify those ground facilities which are critical to adversary UAS operations, especially those that are non-redundant.[34]

Positioning, Navigation and Timing Systems

Most UAS use a dedicated PNT data link to determine its precise location, and this link must be maintained to ensure mission success. The PNT signal strength measured at the surface of the Earth is roughly equivalent to viewing a 25-Watt light bulb from a distance of 10,000 miles. This weak signal can easily be jammed by a stronger power transmission in a similar frequency.[35, 36]

Any radio navigation system is generally vulnerable to interference. A typical patch antenna used to receive PNT signals must be able to receive them from virtually the entire sky. The advantage of this omnidirectional design is that even signals from satellites, which are just above the local horizon, can be received. However, this design is susceptible to a broad range of interference and jamming.[37, 38]

Support Element

The Support Element includes all of the prerequisite equipment to deploy, transport, maintain, launch and recover the UA and its associated communications equipment. The Support Element is typically deployed and located in or near the AOO, depending on the UA's effective range. Like manned aircraft, UAS typically require an appropriate logistics footprint, e.g. shelters for refuelling, arming and maintenance. MALE and HALE UAS usually also require an adequate airport infrastructure with a runway of roughly 2,000 m. The exposure of Support Element personnel and equipment is identical to that of the LRU and MCE as already discussed in the 'Human Element' section.

Summary

This chapter outlined the broad scope of potential points of attack when having to counter UAS and drones. Most notably, possible countermeasures are not limited to the air domain, but also include actions against installations and personnel on the ground, interference with the electromagnetic spectrum up to the space domain as well as cyber-attacks in the non-physical realm of the respective computer networks. Consequently, there is also no single solution that is suitable to counter all types of unmanned systems or their components. The following chapters in this book will outline various approaches which can contribute to a comprehensive C-UAS effort that aims at the many potential points of attack against adverse unmanned systems.

Endnotes

1. 'The Official NATO Terminology Database', North Atlantic Treaty Organization (NATO), [Online]. Available: https://nso.nato.int/natoterm/Web.mvc. [Accessed 9 Apr. 2020].
2. John D. Anderson, Jr., Fundamentals of Aerodynamics (5th Edn), 2010.
3. 'IAI Searcher', Jane's Unmanned Aerial Vehicles and Targets, 15 Oct. 2019.
4. Cruising speed taken from U.S. MQ-1B Predator as the Wing Loong is an almost exact replica. 'MQ-1B Predator Fact Sheet', US Air Force, 23 Sep. 2015. [Online]. Available: https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104469/mq-1b-predator/. [Accessed 9 Apr. 2020].
5. US Naval Air Warfare Center Weapons Division, Electronic Warfare and Radar Systems Engineering Handbook (4th Ed.), 2013.
6. IEEE Standard Definitions of Terms for Antennas, IEEE Standards Association, 1993.
7. 'RCS Simulation of the Predator UAV', Efield AB, Kista, Sweden, 2010.
8. 'Radar Cross Section (RCS)', Global Security, 11 Jul. 2011. [Online]. Available: http://www.globalsecurity.org/military/world/stealth-aircraft-rcs.htm. [Accessed 9 Apr. 2020].
9. Allen J. Bric, 'Imaging a BQM-74E Target Drone Using Coherent Radar Cross Section Measurements', Johns Hopkins APL Technical Digest, Vol. 18, no. 3, p. 365–376, 1997.
10. Shripad P. Mahulikar, Hemant R. Sonawane, G. Arvind Rao, 'Infrared signature studies of aerospace vehicles', Progress in Aerospace Sciences, Vol. 43, no. 7–8, p. 218–245, Oct. 2007.
11. 'Gecko-M', Thales Spain, [Online]. Available: https://www.thalesgroup.com/en/gecko-m. [Accessed 9 Apr. 2020].
12. 'Drone/UAV Detection and Tracking', HGH Infrared Systems, [Online]. Available: https://www.hgh-infrared.com/Applications/Security/Drone-UAV-Detection-and-Tracking. [Accessed 11 Mar. 2020].
13. Ibid.

14. S. Sadasivan, M. Gurubasavaraj and S. Ravi Sekar, 'Acoustic Signature of an Unmanned Air Vehicle - Exploitation for Aircraft Localisation and Parameter Estimation', Aeronautical Development Establishment, 28 Feb. 2001. [Online]. Available: http://publications.drdo.gov.in/ojs/index.php/dsj/article/download/2238/1198. [Accessed 9 Apr. 2020].
15. M. Drela, J. Gundlach, R. Parks and A. S. Ehrmantraut, 'System and Method for Reducing the Noise of Pusher Type Aircraft Propellers'. United States Patent 20120292441, 2012.
16. International Human Rights and Conflict Resolution Clinic at Stanford Law School and Global Justice Clinic at Nyu School Of Law, 'Living Under Drones: Death, Injury and Trauma to Civilians from US Drone Practices in Pakistan', Sep. 2012.
17. 'How loud are drones? | Sound Level metering | Testing noise level of DJI's Mavic and Inspire drone', The Introvert Speaks, 11 Jun. 2017. [Online]. Available: https://www.youtube.com/watch?v=V5DYre_EZKU. [Accessed 13 Mar. 2020].
18. 'Lärm – Hören, messen und bewerten', Bayerisches Landesamt für Umwelt, Feb. 2017. [Online]. Available: https://www.lfu.bayern.de/buerger/doc/uw_34_laerm_messen_bewerten.pdf. [Accessed 13 Mar. 2020].
19. Headquarters Department of the Army, 'Visual Aircraft Recognition FM 3-01.80 (FM 44-80)', 17 Jan. 2006. [Online]. Available: https://www.fas.org/irp/doddir/army/fm3-01-80.pdf.
20. Reg Austin, Unmanned Aircraft Systems: UAVS design, development and deployment, John Wiley & Sons Ltd, 2010.
21. Andrew Watson, Cesar V. Ramirez, Ellen Salud, 'Predicting Visibility of Aircraft', PLoS ONE, Vol. 4, no. 5, May 2009.
22. James B. Campbell, Randolph H. Wynne, Introduction to Remote Sensing, 5th Ed., Guilford Press, 2012, p. 103, p. 287 f.
23. 'National Image Interpretability Rating Scales', Federation of American Scientists (FAS), 16 Jan. 1998. [Online]. Available: https://www.fas.org/irp/imint/niirs.htm. [Accessed 9 Apr. 2020].
24. Lockheed Martin, Presentation on UAS EO/IR Sensor Capabilities, 2002.
25. 'Predator RQ-1 / MQ-1 / MQ-9 Reaper UAV', airforce-technology.com, 2013. [Online]. Available: http://www.airforce-technology.com/projects/predator-uav/. [Accessed 9 Apr. 2020].
26. Maximum speed taken from U.S. MQ-9 Reaper as the Wing Loong II is an almost exact replica. 'MQ-9 Reaper/Predator B', General Atomics Aeronautical, 2012. [Online]. Available: http://www.ga-asi.com/products/aircraft/pdf/Predator_B.pdf. [Accessed 9 Apr. 2020].
27. Flight International, 'USAF: Current unmanned aircraft irrelevant in the Pacific', 6 Dec. 2012. [Online]. Available: http://www.flightglobal.com/news/articles/usaf-current-unmanned-aircraft-irrelevant-in-the-pacific-379839/. [Accessed 9 Apr. 2020].
28. Navy Captain Greg Maguire, Exercise Blue Knight, Nellis Test and Training Range, Nevada, 2011.
29. Anthony P. Tvaryanas, William Platte, Caleb Swigart, Jayson Colebank, Nita Lewis Miller, 'A Resurvey of Shift Work-Related Fatigue in MQ-1 Predator Unmanned Aircraft System Crewmembers', Naval Postgraduate School, Monterey, 2008.
30. Robert Haffa Ph.D., Anand Datla, '6 Ways to Improve UAVs', Haffa Defense Consulting, LLC, 2012.
31. Parag Batavia, Ph.D., Rich Ernst, Kerry Fisherkeller, Doug Gregory, Rob Hoffman, Ann Jennings, George Romanski, Brian Schechter, Gordon Hunt, 'The UAS Control Segment Architecture', Raytheon, 2011.
32. Steve Bonter, Diana R. Dunty, Jason Greene, and Dr William Duff, 'Predator UAV Line-Of-Sight Datalink Terminal Radio Frequency Test Report', Alion Science and Technology, Sep. 2004.
33. Pierluigi Paganini, 'Hacking Satellites … Look Up to the Sky', INFOSEC Institute, 18 Sep. 2013. [Online]. Available: http://resources.infosecinstitute.com/hacking-satellite-look-up-to-the-sky/. [Accessed 15 Apr. 2020].
34. Lt Col Karl Ginter, Space Technology and Network Centric Warfare: A Strategic Paradox, US Army War College, Feb. 2007.
35. 'NAVSTAR GPS User Equipment Introduction', Sep. 1996.
36. Jon S. Warner, Ph.D. and Roger G. Johnston, Ph.D., GPS Spoofing Countermeasures, Los Alamos, New Mexico: Los Alamos National Laboratory, Dec. 2003.
37. John A. Volpe National Transportation Systems Centre, 'Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System', Office of the Assistant Secretary for Transportation Policy, U.S. Department of Transportation, Aug. 2001.
38. 'GPS Modernization', National Coordination Office for Space-Based Positioning, Navigation, and Timing, 25 Sep. 2013. [Online]. Available: http://www.gps.gov/systems/gps/modernization/. [Accessed 9 Jan. 2014].

5

By Lieutenant Colonel André Haider, GE A
Joint Air Power Competence Centre

A Methodology for Countering Unmanned Aircraft Systems

Overview

The challenge of Countering Unmanned Aircraft Systems (C-UAS) has been recognized and taken seriously after incidents with commercially available drones showed that even small systems could project a viable threat to political leaders, critical infrastructure and commercial businesses. Chapter 3 (cf. p. 48 ff.) provided some examples of recent incidents and outlined them in more detail.

A multitude of C-UAS systems have since been developed to satisfy the growing need to defend against drones, especially in the low, slow, and small spectrum. In principle, these systems are designed to detect and then engage the threat, and some systems have indeed proven to be quite successful in fulfilling their mission.

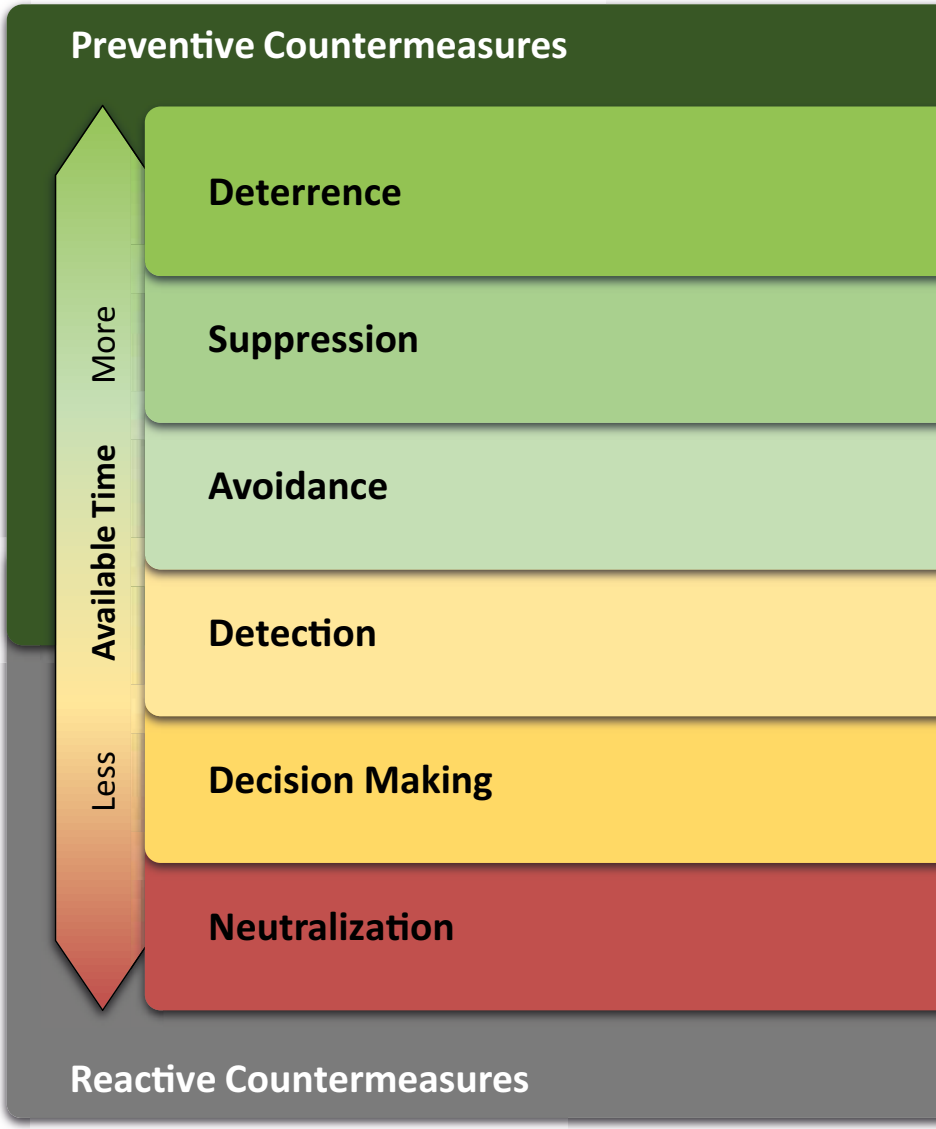
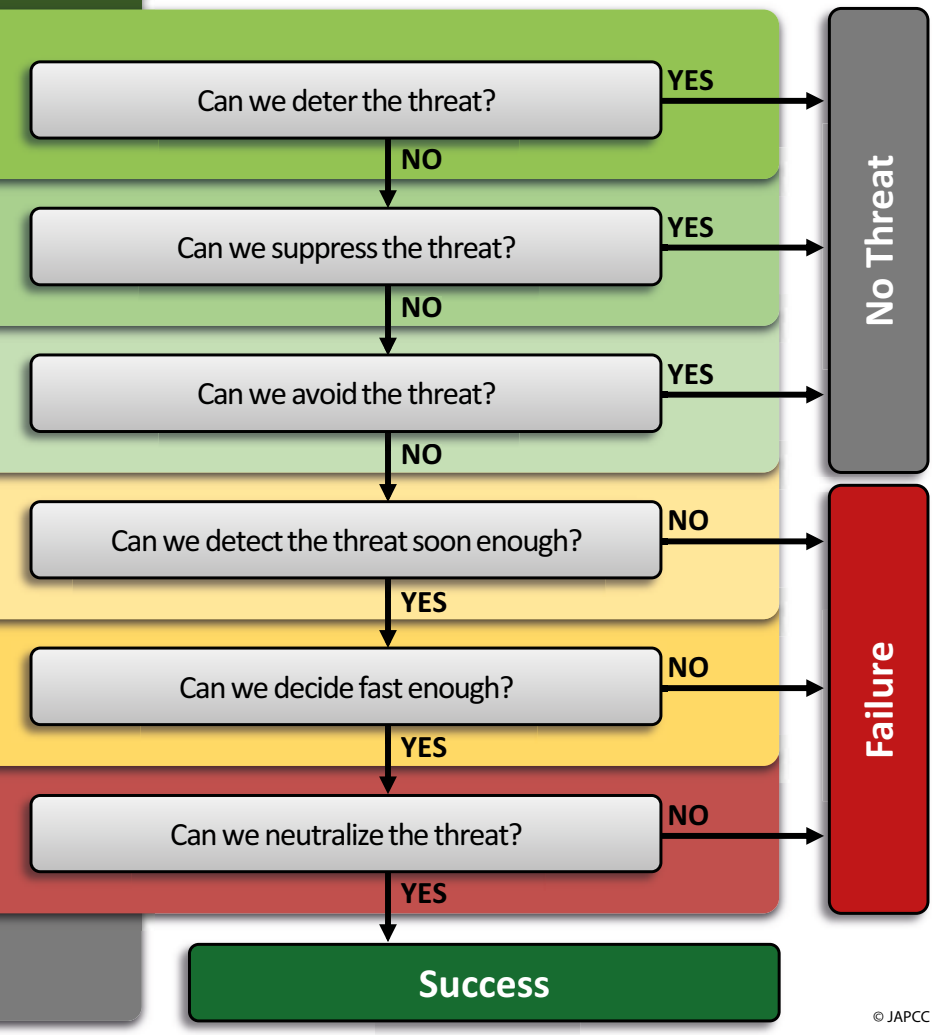


Figure 5.1: C-UAS Methodology.

C-UAS Methodology



However, a comprehensive C-UAS approach must not only rely on reacting to an imminent threat, but it has to include preventive measures as well. Assuming that preventive measures helped eliminate the presence of a drone in the first place, then no active countermeasure would be necessary.

This chapter provides a potential methodology which incorporates preventive as well as reactive countermeasures. The countermeasures are listed sequentially, based on the time available to employ them. The previous two pages portray that approach in general terms, whereas the subsequent sections will describe every measure in more detail.

Preventive Countermeasures

Preventive countermeasures have the advantage, if successfully applied, that a potential threat will not even occur and reactive countermeasures need not be employed. Moreover, they are not subject to time pressure, as preventive measures can be taken well in advance and thoroughly planned.

Deterrence

Successfully deterring enemy forces or civilians from using UAS or drones will negate the threat completely. For deterrence to be effective, enemy forces or civilian drone users have to anticipate such negative consequences that the mere prospect of suffering them is sufficient to refrain from using UAS or drones.

Deterring enemy forces from using UAS is undoubtedly problematic, as these systems offer significant military advantages without putting the lives of their forces at risk. However, the prospect of

losing a high number of UAS to NATO air defences may be a sufficient deterrent if the adversary's military budget is constrained or the availability of UAS is so limited that losing them is not affordable. Strategic Communications (STRATCOM) may also help spread the message that UAS employment against NATO territory or forces will be denied or come at a high cost. Consumers and commercial companies may be fined for unlawful use of their drones. This probably requires dedicated legislation, but at minimum the incorporation of unmanned flight into the national rules of the air. This may not entirely prevent drone incidents, but it may help reduce them significantly and allow the focus on actual threats.

Suppression

If enemy forces or civilians cannot be deterred from using UAS or drones, the next step would be to deny them access to NATO airspace or protected areas and prevent them from achieving their goals.

For military UAS, NATO air defences and Electronic Warfare (EW) are likely the most effective means that can successfully suppress enemy UAS operations. During open conflict, Air Interdiction (AI) and cyber-attacks against UAS ground installations and networks may prevent UAS employment right from the start. EW will also work against consumer and commercial drones; however, peacetime restrictions may limit this option significantly. Again, legislation may be an option to impose obligations for manufacturers that drones adhere to flight restrictions automatically, e.g. incorporating geofencing parameters by default.

Avoidance

If the employment of UAS or drones cannot be deterred or suppressed, the detection or effects from these systems need to be avoided.

Avoiding detection or kinetic effects from the air is not new. However, many traditional measures may not have been sufficiently trained or even forgotten in the last decade due to the war on terrorism and the actual absence of a serious air threat. Long established Tactics, Techniques, and Procedures (TTP) may have to be brought back to soldier's minds, and, if necessary, reviewed and modified for this new type of air threat. Modern sensor technology may be countered by fielding newer materials which are capable of better absorbing or reducing radar reflections or thermal signatures. Protective measures for military installations and critical infrastructure, but also military forces in the open, may require review and modernization to shield them from detection and kinetic effects.

Reactive Countermeasures

Detection

As a prerequisite for any further countermeasures, the existence of a threat must first be identified. Detection is the first action in a series of active measures against UAS or drones, and therefore time is one of the most critical factors. In general, detection must take place at the earliest possible time and the furthest measurable distance.

Intelligence, Surveillance and Reconnaissance (ISR) is the key to detecting and identifying threats from UAS or drones. Most importantly, ISR should not be limited to the UA itself; the detection of any elements or components of an unmanned system could help to increase situational awareness of an imminent adversarial deployment of UAS. Electromagnetic Operations as part of Signal Intelligence (SIGINT) could also contribute to detecting UAS and drone threats as most systems require continuous radio

transmissions to operate. Newer methods of Command and Control (C2) of UAS and drones use cellular networks, and this may require additional cyber tools to help detect this communication. In particular, the use of drones for private and commercial use may require updated regulations and data protocol disclosure to help law enforcement agencies and the military detect and identify drone operations.

Decision-Making

Defending against an imminent UAS or drone threat is the most time-critical. Due to their size and altitude, the detection of Low, Slow, and Small (LSS) drones can be expected to be generally later and the reaction time significantly shorter than for HALE and MALE UAS or fighter aircraft in general.

Established Air C2 and Time-Sensitive Targeting (TST) procedures may require a review to determine if and how to accelerate decision-making processes and probably delegate decision-making authorities to counter this new type of air threat. Countering LSS drones is probably more a question of rapid self-defence at the team or squad level than decision-making at higher echelons. This may require the general incorporation of drone countermeasures into the regular curriculum and training of each soldier. Additionally, countering UAS and drones in peacetime may require close cooperation with law enforcement agencies and the clear delineation of responsibilities.

Neutralization

Defending against UAS or drones not only involves traditional kinetic engagement of the air threat, but may also require actions against other UAS elements and components to be effective. Non-

kinetic measures and activities in the electromagnetic and cyber domain may contribute to a more balanced and proportionate C-UAS approach, if peacetime restrictions apply or fratricide and collateral damage is a concern.

With lesser priority, but certainly worth considering, are the cost-benefit assessments when having to counter cheap UAS and drones. Cheap production and acquisition of drones is an enemy's clear asymmetric advantage, if NATO's options are limited to costly countermeasures only. Legacy AD systems, which are no longer suitable for fighting 5th generation aircraft, could offer excellent potential for a cost-effective C-UAS solution.

Summary

Time is the key factor when having to counter UAS or drones. Most of the currently available C-UAS systems focus on the 'detect, track, and engage' sequence only. Passive measures and preliminary actions to deny adversarial UAS and drone usage right from the start help reduce potential threats, focus on less remaining targets and gain precious time. Once active measures have to be taken, decision speed is decisive. Moreover, C-UAS is not an anti-air activity only but includes actions against all elements of the unmanned system. Non-kinetic and low-collateral damage approaches complete the picture and contribute to a balanced and proportionate C-UAS approach.

Part II

Military Perspectives

6

By Major Giuseppe Valentino, IT AF
By Major Andreas Wurster, GE A
Joint Air Power Competence Centre

Joint Intelligence, Surveillance, and Reconnaissance

Introduction

This chapter discusses the role of Joint Intelligence, Surveillance, and Reconnaissance (JISR) in support of countering Unmanned Aircraft Systems (UAS) and the essential contributions of the different intelligence collection disciplines throughout all phases of the C-UAS methodology described in the previous Chapter. This chapter will also highlight how JISR can support UAS related threat assessments at all levels and it provides an outlook of potential future challenges regarding JISR.

The proposed C-UAS Methodology (cf. Figure 5.1, p. 76) comprises a broad range, from deterrence to neutralization, and from preventive to reactive countermeasures. A prerequisite to successfully

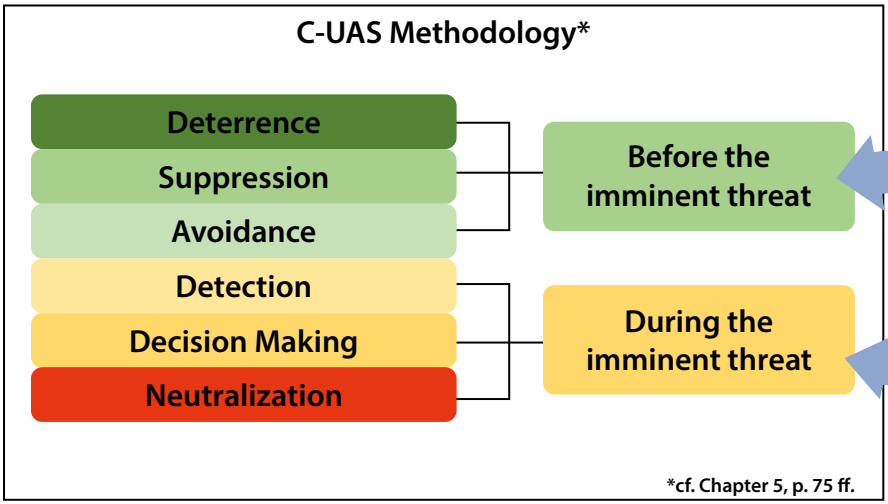
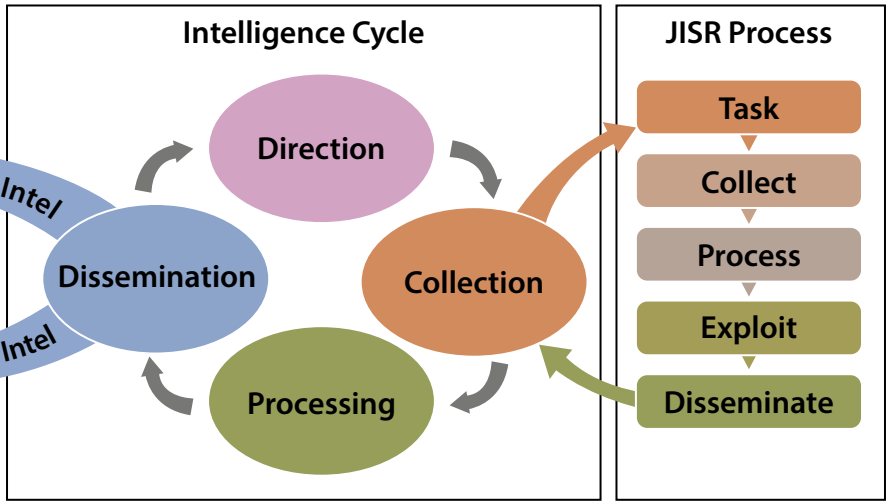


Figure 6.1: Intelligence Cycle and JISR process within C-UAS.

apply this method are defined threat vectors. Although these vectors are not always predictable with absolute certainty, JISR can provide probabilities if a threat exists and how it could evolve, so C-UAS measures can be planned and developed accordingly. Because of this, the intelligence cycle and the JISR process have to start even **before** the described C-UAS Methodology comes into play. Then, once a threat is identified, JISR also needs to continuously accompany and support every single line of effort within the C-UAS Methodology.

Taking Preventive Action: The Joint Intelligence Preparation of the Operational Environment

According to Frank Herbert's famous quote, taking preventive action against a threat requires knowledge of its existence. Hence, the first



step to prepare for countering UAS is to identify how likely a threat is to occur, how it is likely to emerge, and from where it might originate.

'The first step in avoiding a trap is knowing of its existence.'

Frank Herbert
from his 1965 novel 'Dune'

By definition[1] a threat can be described as 'an expression of intention to inflict evil, injury, or damage'. However, this definition covers only the intent of potential adversaries willing to impose a threat, but not the means to do so. To constitute a valid threat, both factors need to be accounted for. Therefore, JISR has to identify the potential adversaries and their intent, as well as their available

means to pursue their objectives. Chapter 3 (cf. p. 34 ff.) describes some potential threat scenarios originating from various actors, ranging from consumer and commercial drones operated by individuals to advanced UAS employed by state-sponsored organizations or regular armed forces. Although the actual countermeasures against these threats may differ, the intelligence requirements and JISR contributions to the C-UAS process as a whole will remain unchanged.

'[…] the establishment of a common threat database […] will enhance identification and classification and will help reduce fratricide. In the case of UAS, everything is enemy – until proven friendly. […] Establishing a common UAS database, with a single intelligence organization responsible for its operation, would provide a considerable advantage for the warfighter.'[2]

Colonel Matthew T. Tedesco
United States Army

With regard to C-UAS, intelligence collection and analysis should be focused on a potential adversary's unmanned systems inventory, these systems' capabilities and anticipated performance, as well as their possible evolution in the future.[3] Therefore, UAS require consideration and implementation in both the intelligence cycle and the JISR process. To develop an effective C-UAS standard, all intelligence activities should take the following information requirements about a potential adversary's drones and UAS into account:[4]

- General System Features and Characteristics;
- Physical Structure of the UAS;
- Sensors and Weapons Capabilities;
- Possible System Adaptations;

- System Interoperability, especially Sensor-Shooter Interrelations;
- Command & Control, especially Radio Frequencies;
- System Vulnerabilities, Resilience and Redundancy;
- Logistic Supply Chain and Contractors;
- Tactics, Technics and Procedures (TTP);
- Potential Chemical, Biological, Radiological, and Nuclear (CBRN) upgrades.

Following collection, the above data needs to be processed and assessed as to whether and how a threat can be deterred, suppressed or avoided. This assessment is provided by the intelligence cycle which is supported by the JISR process. A plain technical analysis of an unmanned system and the deduction of its potential capabilities can already provide a reasonable estimate of its ability to impose a threat on friendly forces. However, as already mentioned, the potential adversary, their intent, and their willingness to inflict harm need to be taken into the equation as well. To do so, there are two possible approaches, depending on how much time and analytical resources are available:

Identify possible actors which pose a threat and then analyze their UAS capabilities. This approach focuses on the potential adversary and has the advantage of significantly reducing the number of UAS to be assessed. Facing clear signs of an emerging crisis or a likely adversary, it is a very efficient way to analyze the threat, especially when time is a critical factor.

Identify all UAS which could pose a threat and then merge these with possible hostile actors if required. Establishing a common threat database of most UAS requires significant time and effort but has the advantage of having knowledge readily available when required. This, in turn, would be significantly beneficial for the first approach, when time is critical.

Both approaches have their own relevance and should complement each other to successfully contribute to the Joint Intelligence Preparation of the Operational Environment (JIPOE).[5] The most relevant intelligence gathering disciplines that can contribute to both approaches and the JIPOE are briefly discussed in the following sections.

Open Source Intelligence (OSINT) can exploit, for example, catalogues and advertisements of different commercial UAS manufacturers, or analyze market trends at commercial and scientific exhibitions and conferences. Like with any other information, these sources must be thoroughly assessed with regard to their credibility and reliability as open-source information is generally vulnerable to falsification and should not be accepted as the main source of intelligence. Many governmental and non-governmental intelligence agencies use open sources to release fake or biased versions of news stories. Chapter 16 (cf. p. 283 ff.) discusses countering disinformation in more detail. Nevertheless, OSINT remains a good source of information to track emerging UAS technologies and the evolution of unmanned systems for civil, public, as well as military applications.

Imagery Intelligence (IMINT) can provide relevant information on an adversary's UAS inventory, the numbers and types of systems, as well as their supporting equipment. Imagery of UAS components, for example satellite ground terminals and ground control stations or dedicated UAS ammunitions and spare parts near an airfield, if visible, can reveal the presence of a UAS capability without having to detect the actual unmanned aircraft. Frequent imagery of suspected or identified UAS locations can help reveal new acquisitions of systems and identify upgrades in UAS capabilities. For example, satellite terminals which were not present before, could indicate a new Beyond Line of Sight (BLOS) capability.

Technical Intelligence (TECHINT) concerns itself with foreign technological developments and the performance and operational capabilities of foreign materials, which have or may eventually have a practical application for military purposes.[6] As UAS technology is a global phenomenon, TECHINT does not necessarily require captured enemy materiel. Technical analysis of common UAS components manufactured in neutral or friendly countries and distributed by a global supply chain (for instance EO/IR sensor chips, microprocessors or engine parts) could provide sufficient insight into a foreign unmanned system's capability.

Human Intelligence (HUMINT). UAS activities always involve people, whether in research and development, production, or deployment. HUMINT can approach these human resources, either overtly or covertly, to gain more specific information than technical systems, like satellites, could provide. However, HUMINT is thoroughly based on the credibility and reliability of the human source targeted.

Acting on the Imminent Threat: the 'S' in JISR

Once a UA is airborne, surveillance as an integral part of JISR becomes relevant. In an operational environment, JISR responds to the Commander's Critical Information Requirements (CCIR)[7] by applying tactics, techniques and procedures to detect, identify, and disseminate intelligence data in support of C-UAS and the operational planning process.

Detecting UA in flight is often the first step in defending against them. Larger UA can be detected even with legacy radar systems, whereas Low, Slow and Small (LSS) drones 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. To provide this reliable identification as a precondition for high confidence real-time decisions, including weapons engagement, all intelligence collecting disciplines have to contribute the necessary data. For example, this includes information about the capabilities and the level of autonomy of the UAS, locations of adversary Launch & Recovery Elements (LRE) and Mission Control Elements (MCE), as well as SATCOM assets and the frequencies used. C-UAS systems must be fed with this information, preferably in real-time, to process a suitable target solution. The most relevant intelligence gathering disciplines that can contribute to surveillance are briefly discussed in the following section.

Acoustic Intelligence (ACINT) collects and exploits acoustic signals or emissions.[8] ACINT has some long-established applications in the maritime environment (sonar) but is also used to locate rocket launch sites or artillery firing positions. Dedicated acoustic detection systems for locating UAS in flight are already developed and available on the market, but their current effective range is limited to less than a few kilometres. At longer distances, the environmental noise will simply mask the sound emissions from the UAS' engine and propeller. Chapter 4 (cf. p. 58 f.) discusses drone and UAS audibility in more detail. However, ACINT systems could be relevant at the tactical level and a built-in database of acoustic drone signatures could support the identification of the detected drone model and manufacturer.[9]

Imagery Intelligence. The vast majority of surveillance is conducted in the optical spectrum, to include not only visible but also infrared and ultraviolet light emissions. IMINT can identify the infrastructure and support equipment necessary to operate larger UAS not only during the JIPOE, as already discussed, but also dur-

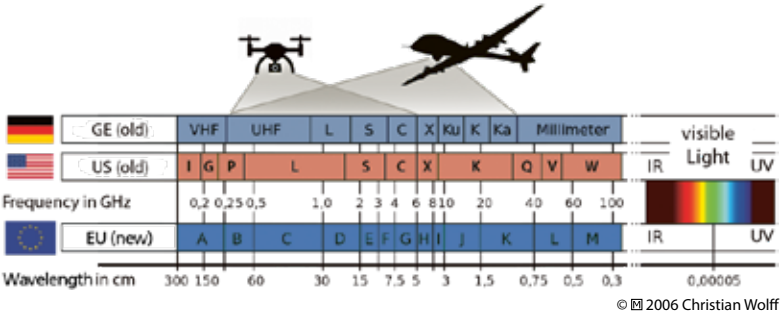


Figure 6.2: UAS Frequency Bands.[i]

ing the Battle Damage Assessment (BDA) process once these targets have been engaged. Moreover, IMINT can actively pursue the identification of temporary UAS launch sites and mobile launch platforms. On the tactical level, dedicated C-UAS systems are typically equipped with an additional EO/IR camera to augment the primary sensor and to support the operator in validating the detected object.

Signals Intelligence (SIGINT) collects and exploits transmissions throughout the entire radio frequency spectrum. If not fully autonomous, almost any UAS relies on electronic communications and one or more data links. Figure 6.2 depicts the frequencies used by the majority of current drone and UAS models. SIGINT can detect and intercept UAS transmissions and analyze the respective signal to identify the drone or UAS. The exploitation of the transmitted data may reveal significant information about the UAS, like its location, planned flight route, engine status, and more. Similar

[i] The most common frequencies used for remote controlling consumer drones are: 900 MHz, 1.2 GHz, 2.4 GHz, and 5.8 GHz. Specialized long-range UHF control systems operate at 433 MHz or 869 MHz and are commonly used to achieve greater control range, while the use of directional, high-gain antennas increases video range. Data links for military UAS encompass the full range from UHF (400 MHz and less) to commercial and military Satellite Communications (up to 30 GHz).

to the recommended audio database for ACINT, it is desirable to implement a comparable approach in the SIGINT domain, to include: UAS data link frequencies, waveforms, protocols, and encryption methods.

Other intelligence disciplines, such as Measurement and Signature Intelligence (MASINT) or Scientific and Technical Intelligence (STI)[10] are required to support this SIGINT approach because they provide the relevant information about the respective UAS and the technical analysis of their radio frequencies.

Human Intelligence. Although HUMINT could not directly contribute to surveillance and countering an imminent UAS threat, it can fill data collection gaps and provide additional intelligence about: locations of temporary launch sites and UAS ground elements, logistic support routes, or regular launch & recovery schedules. Interrogation of captured personnel could provide more reliable information on enemy UAS and their capabilities.

General Reporting Procedures. JISR depends on a continuous flow of information, which does not necessarily only need to originate from the specific intelligence disciplines. The eyes and ears of every soldier are highly valuable sensors to augment the data collection and could help to complete the situational picture. Chapter 15 discusses reporting procedures and the respective requirements for education and training in more detail.

Tasking, Collection, Processing, Exploitation and Dissemination

Drones and UAS require consideration throughout the entire Tasking, Collection, Processing, Exploitation and Dissemination

(TCPED)[11] process to raise awareness on this new type of threat and as a prerequisite for any defensive measures to follow. This is likely to require contributions from all of the aforementioned intelligence collection disciplines and their associated sensors. TCPED needs to develop applications and tools to store drone- and UAS-related technical data and signatures to enable intelligence and C-UAS systems to utilize that information for the identification of the respective drones and UAS. Establishing a common UAS database will likely accelerate the TCPED process with regard to UAS identification and enable more flexible support to ad hoc and dynamic requests. Notably, the sooner information about drones and UAS is collected and analyzed, the more effectively the recommended database could be utilized. Therefore, all intelligence disciplines need to consider pre-emptive data collection of potential adversaries' UAS, but also of dual-use consumer and commercial drones.

Three Considerations for Adapting to the C-UAS Challenge

According to NATO AJP-2.7 'the harmonization of intelligence and operations functions is essential to maximize the efficiency and effectiveness of the employment of JISR capabilities'.[12] In the C-UAS context, three considerations about the key elements of JISR and its associated processes should be made, namely about agility, adaptability and innovation.

Agility

The purpose of intelligence is to gather, analyze and disseminate information to support the decision-making cycle at all levels of operations. Drones and UAS represent a complex challenge as there is a multitude of different models with different characteristics and

capabilities. Larger systems can consist of many different components which are dispersed throughout all domains, to include air, land, space, and even cyberspace. Collecting information about all the different drones and UAS as well as their components and characteristics in all of these domains is likely to result in an 'ocean' of stored data and information. Consequently, the JISR architecture requires a high level of agility in managing this vast amount of information. This agility may only be achieved with the help of automated processes and probably computer-aided analytics and decision-making support.

Adaptability

The recent decades have seen a significant change and evolution of warfare. It shifted from global war against terrorism to a near-to-peer or peer-to-peer confrontation. Nuclear, biological and chemical weapons have been uncontrollably spread to states that should never have been allowed to get their hands on these technologies. In the same way, the ever-accelerating development and proliferation of drones and UAS are enabling potential adversaries to acquire new, previously non-existent capabilities. Hence, JISR needs to adapt to these emerging capabilities and enhance the awareness of the C-UAS challenge. Adaptability might also be required when urgent Collection Requirements (CRs) emerge, and the analysis of adversary UAS receives a high priority in operational planning. NATO doctrine already states that its JISR architecture should be adaptive to 'rapid reconfiguration'.[13] With respect to drones and UAS, this implies the consideration of the different domains in which the individual components of the UAS operate and the geographical region from which they are controlled. It also requires consideration of enemy UAS inventories, including dual-use commercial systems, as well as enemy UAS and drone tactics, techniques, and proce-

dures, to create a comprehensive awareness of how to counter the UAS threat. To highlight the importance of adaptability, Chapter 3 (cf. p. 43 f.) provides an example of how Russian forces directed and adjusted fires in Eastern Ukraine with simple commercial off-the-shelf drones.

Innovation

Innovative technologies and methods offer many opportunities for data collection, processing, and exploitation. JISR should not be limited to classically exploiting information, but rather should initiate an innovative way of thinking how to incorporate the various drone and UAS components into the Collection Task List (CTL). In a complex environment, the use of cognitive analysis tools for the exploitation of high-resolution images and the automatic identification of moving objects are just two examples of potential ways to implement computer-aided analysis support. This may help to reduce the workload of limited, valuable human resources. Eventually, data analytics techniques may be able to automatically generate JISR results,[14] and significantly reduce the required time to deliver reliable information about potential UAS threats.

Conclusion

Drones and UAS are complex systems which do not only consist of the unmanned aircraft. All of the different system components may provide individual opportunities for countermeasures and need discreet consideration in the JIPOE. JISR has to provide the relevant data of enemy UAS and their components. This large amount of information needs to be stored in advance, preferably in a common database, so that it can be made available at the beginning of any operational planning. This database would also help to

feed timely, actionable intelligence into the targeting cycle to support the C-UAS weapon systems embedded in the proposed C-UAS methodology. This may require the design of a more modern and connected intelligence structure and information sharing policy amongst the NATO member states. In this context, it is important that the interfaces between JISR, the intelligence cycle, and the targeting cycle are well defined, synchronized and harmonized. Personnel from the aforementioned disciplines have to be trained in the collaboration between these processes. To further improve cooperation, it is advisable to deepen this during exercises in order to get a routine and common understanding of the processes.

Endnotes

1. 'threat', Merriam-Webster, [Online]. Available: https://www.merriam-webster.com/dictionary/threat/. [Accessed 13 Oct. 2020].
2. Col Matthew T. Tedesco, US Army, 'Countering the Unmanned Aircraft Systems Threat', in Military Review, Nov.-Dec. 2015, Army University Press, 2015. [Online]. Available: https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20151231_art012.pdf. [Accessed 13 Oct. 2020].
3. Vernon Vinge, 'The Coming Technological Singularity: How to Survive in the Post-Human Era', in Vision-21 Interdisciplinary Science and Engineering in the Era of Cyberspace, NASA, 1993. [Online]. Available: https://ntrs.nasa.gov/citations/19940022856. [Accessed 13 Oct. 2020].
4. Jeffrey Lamport, Anthony Scotto, 'Countering the UAS Threat: A Joint Perspective', Defense Systems Information Analysis Center (DSIAC), 2 Nov. 2019. [Online]. Available: https://www.dsiac.org/resources/articles/countering-the-uas-threat-a-joint-perspective/. [Accessed 13 Oct. 2020].
5. Allied Joint Doctrine for Intelligence, Counterintelligence and Security (AJP-2), Edition A, Version 2, NATO, Feb. 2016.
6. NATO Glossary of Terms and Definitions (AAP-06), Edition 2019, NATO, 2019.
7. Ibid.
8. Joint Intelligence, Surveillance and Reconnaissance (AJP-2.7), Edition A, Version 1, NATO, Jul. 2016.
9. Randall K. Nichols, Hans C. Mumm, Wayne D. Lonstein, Julie J.C.H. Ryan, and Candice Carter, 'Counter Unmanned Aircraft Systems Technologies and Operations', New Prairie Press, 2020. [Online]. Available: https://newprairiepress.org/cgi/viewcontent.cgi?article=1031&context=ebooks. [Accessed 13 Oct. 2020].
10. Ibid.
11. Ibid. 8.
12. Ibid. 8.
13. Ibid. 8.
14. Ibid. 8.

7

By Lieutenant Colonel Andreas Schmidt, GE AF
By Lieutenant Colonel Berry Pronk, NE AF
Joint Air Power Competence Centre

Defensive Counter-Air Operations

Introduction

As technology evolves, the technical options and consequently the military applications for unmanned aircraft become more diverse. Theoretically, every manned system could be construed as an unmanned version. But the lack of necessity for a pilot to be in the system gives engineers options, which were not fathomable before. However, from an Air Defence (AD) perspective manned and unmanned aircraft are 'effect delivery platforms' and the delivery of their effects needs to be prevented. This chapter will highlight a lot of the similarities with traditional AD, but will also emphasize the problem's complexities and additional options for dealing with this constantly evolving threat.

Why are Unmanned Aircraft Systems Different to Traditional Air Threats?

The main difference between UAS and regular aerial systems is the fact that the UA itself has no human pilot on board. If this were the only difference, the current requirements for AD would not change. However, the fact that the pilot is not part of the actual airframe or not necessary at all allows for new categories of aircraft and also allows for new ways of using an UA with new or enhanced employment methods.

Not having a pilot on-board allows developers to perform systems engineering with a far more mission-centric mindset than before. Not only does a pilot impose a minimum size requirement for airframes, but it is also a biological limiter, affecting overall dwell-time, system robustness and even expendability. However, according to the principle 'form follows function', UA will have to have a certain size, weight, and flight altitude to fulfil their mission. For example, a 10 kg UA flying at 20 km altitude for 24 hours, carrying high-resolution cameras or air-to-ground missiles is technically not feasible. That means a certain kind of UA can be expected for a certain type of mission.

However, from an AD perspective, the main objective is to prevent the delivery of effects by adversary air threats. For this, the airframe or the payload needs to be targeted in the air, on the ground or its logistic support needs to be negated. For each option, there is a so-called kill chain following the F2T2EA (Find, Fix, Track, Target, Engage, Assess) logic.

Kill Chain

The United States of America developed the F2T2EA kill chain model inspired by General Ronald R. Fogleman.[1] Analysing the six

steps defined by their keywords will shed some light on the question of how the kill chain works, and why there are additional options for UA defence.

Find. This is the initial element to start the entire process. Information collection in regards to Intelligence, Surveillance and Reconnaissance (ISR) to provide a proper Joint Intelligence Preparation of the Operational Environment (JIPOE) is obligatory to be sufficiently informed about the expected threat. In parts, this has to take place long before an actual C-UAS operation, but the theoretical planning process to develop defensive reactions is based on these prerequisites; on a practical note, sufficient surveillance is considered to be obligatory.. Before thinking about any active defensive actions, it is mandatory to 'find' targets. Sensors (e.g. radars, but also optical and acoustic systems) are required to detect any air targets. Sensor requirements for UA, which are similar to known air threats, should be satisfied by existing systems. Although, the smaller the UA and lower the flight altitude, the more complex it will be to reliably execute the first step of the kill chain with Surface-Based Air and Missile Defence (SBAMD) sensors. Therefore, finding UA before they are airborne could significantly enhance SBAMD operations, at least in passive defence terms.

Fix. The meaning of fix in the AD domain is to identify the detected air targets. This will contribute to proper situational awareness (SA) and allow valid and consequent decision-making. This becomes especially problematic, but very important in peacetime, due to the massive increase of private or recreational UA.

Track. Tracking the identified radar contact is mandatory to continue the dynamic decision-making process. In relation to the track history and the current track behaviour, military leaders are capable of prioritizing or retaining attack options. Individual tracks

may be sorted and allocated to weapon systems, which directly leads to the next step.

Target. Final coordination including the reassurance of the correct classification and identification is going to lead into the final approval for engagement under consideration of all applicable laws and Rules of Engagement (ROE).

Engage. The allocated weapon system is ready to fire and will receive the engagement order. Like with other air threats against UAS, this process will work in all modes of operation, depending on the individual situation and UA.

Assess. The last step in the kill chain is the assessment of engagement success. The outcome of this assessment could be an all-clear, a re-engagement or the alerting of threatened sites.

Additional Options to Counter Unmanned Aircraft Systems

As previously mentioned, for regular manned air threats the kill chain can be aimed at the aircraft, the payload or the logistical

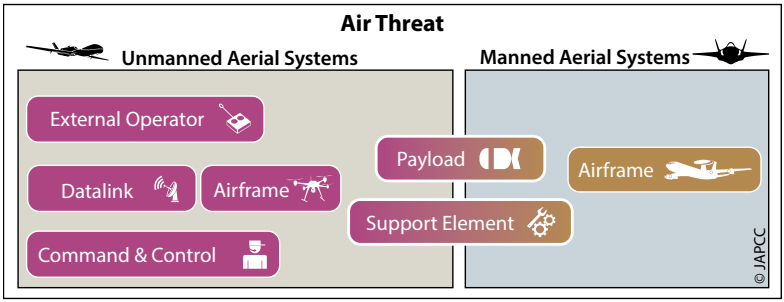


Figure 7.1: Difference between Manned and Unmanned Aerial Systems.

backbone. When dealing with UAS, three more target options arise. These are the control element, the human operator or the control link/mechanism.

Every individual target option requires an additional kill chain, which enables the suppression of the UAS' mission, in several cases even without physically destroying the aerial vehicle itself. Also, smaller UA might only have a very short-range and therefore will be launched well inside of any SBAMD sensor envelope, reducing available time for SBAMD systems to react. In this case, the initial act of finding an UA before it ever becomes airborne is critical. However, there are also options in how SBAMD systems can support these potential kill chains with existing or potentially added capabilities, which will be described later.

Surface-Based Air and Missile Defence Role in Countering Unmanned Aircraft Systems

The role of SBAMD can be defined in various contexts. SBAMD systems are part of NATO´s Defensive Counter-Air (DCA) strategy. DCA consists of all active and passive AD operations to detect, identify, intercept and destroy or render ineffective, adversary air and missile forces attempting to attack or penetrate friendly airspace.[2] As part of DCA, NATO employs the NATO Integrated Air and Missile Defence System (NATINAMDS), which is very important for controlling NATO's airspace and protecting against ballistic missiles. NATO IAMD has four pillars; Active Air Defence, Passive Air Defence, Surveillance and Battle Management, Command, Control, Communications and Intelligence (BMC3I). In both constructs, SBAMD forces can be used in a pre-planned defence design or a more reactive self-defence centric role (e.g. protecting manoeuvring forces). Another distinction of SBAMD forces is the

characteristics of the 'to be protected' asset. The main differences are between area and point defence and stationery versus moving assets. Every SBAMD system is a combination of Sensor, Shooter and Command and Control (C2) elements. Two facts that have to be considered are, not every track that can be seen can be engaged and not every track that is in engagement distance for the effector can be seen. The resulting effective space, where a SBAMD unit can deliver its effect, is called battlespace. However, it is imperative that the C2 mechanisms, the underlying ROE, and the delegated rights to execute the kill chain (including engagement/neutralisation) are readily available and appropriately delegated. In the overall scheme of deterrence, SBAMD means can be used to deny the adversary their ability to deliver effects with UAS, but as will be shown later, they can also be used to inform other means of mitigating the UAS threat.

The picture emphasizes, that SBAMD, as part of active AD, is mainly aimed at the UA or potentially larger payloads (e.g. missiles or bombs) while inflight is only one way to interrupt the application of the entire UAS. However, SBAMD should not be seen in isolation. Through an optimized system of overarching BMC3I, the effectiveness and efficiency against UAS can be optimized.

To describe the role of SBAMD systems and the necessary framework, it is essential to identify the function of the SBAMD force and the anticipated threat. In NATO, UA are classified into three categories.

- Class I: Small UA less than 150 kg; Mini UA less than 15 kg
- Class II: Tactical UA up to 600 kg
- Class III: HALE/MALE[i] larger than 600 kg

[i] High-Altitude Long-Endurance, Medium-Altitude Long-Endurance.

Figure 7.2: The Role of SBAMD in Threat Mitigation.

These are categories based only on one parameter, but for a large part of UA, weight can directly correlate to size, possible lift, propulsion and therefore maximum altitude, payload, speed and function.

Class III

A significant subset of Class III UA is basically 'regular aircraft' without a pilot in the airframe, hence they can be mainly dealt with within the framework of available AD. Since current Class III UA like the MQ-1 'Predator' or RQ-4 'Global Hawk' are very large and relatively slow, finding them in the airspace with available sensors should not be more complicated than finding comparable manned aircraft. Also identifying them is possible with already available means (e.g. IFF, Airspace Control Means). As targets, they are well within the capabilities of available interceptors or Medium-Range (MR) and Long-Range (LR) SBAD units. Some Class III UA might be harder to intercept than others, e.g. rotary UA in comparison to Global Hawk, but the qualitative difference to comparable regular air threats seems minimal.

Also, existing threats like some Cruise Missiles (CM) seem to fulfil the criteria of Class III UA. These threats were never manned but developed to outmanoeuvre the battlespace of existing SBAMD systems. The battlespace is the volume of airspace, where a SBAMD system can intercept a target, mainly based on the sensor, interceptor and threat characteristics. It is commonly depicted as a half sphere, which is somewhat idealistic since it rapidly decreases with the flight time of the interceptor. With increased agility of the target, the intercept probability will decline significantly. The best way for a threat to penetrate a battlespace is to have a combination of parameters, mainly speed, altitude and Radar Cross Section (RCS), for which the SBAMD system is not designed. CM employ very low or very high flight profiles with manoeuvring capabilities to minimize contact time with SBAMD battlespace. By removing the pilot from the aircraft, the biological limitation to physical forces by the human itself is not present, so for a UA, this will be even easier to achieve. Also, heavy attrition of the airframes without a pilot becomes less of a problem and having the UA as an ordnance, like a cruise missile, becomes more of a benefit. This creates UA employment options which could significantly weaken SBAMD defence designs.

Newer UA concepts like 'pseudo satellites', which are by dimension comparable to Class III UA, but can by weight be in all three classes, fly at an altitude above 60,000 ft. Most of the SBAMD effectors might be significantly challenged to reach such altitudes. Also, such interceptors are relatively expensive, so the cost-benefit ratio has to be considered.

Class II and I

For most systems below Class III UA, there are no manned equivalents. Here, we can find relatively new types of threats, which create new challenges for existing SBAMD systems and ideas. UA can

be much smaller and can have different forms/formats than conventional manned threats. This puts stressors on all links of a potential kill chain.

As mentioned before, every sensor works within an anticipated framework of threat parameters which are mainly RCS, speed, altitude and manoeuvrability. Designing unmanned systems allows these parameters to be challenged, which might create a requirement for new sensors, effectors and C2 structures/processes.

RCS: Having the opportunity to miniaturize systems, also allows for a significant reduction of the RCS. Shapes of aircraft without pilots on board create better RCS design options as well. Indeed, mission requirements with impact on the RCS, like range or altitude, will have to be considered in UA design, but it still allows for more flexibility for the developers.

Speed, Altitude and Manoeuvrability: Of course, the human in the system is a significant limiting factor of how the system can behave in the third dimension. High altitudes require life support systems, which can make such a system too expensive or large. Due to high G-forces, a manned system cannot perform flight patterns beyond certain speeds or manoeuvre thresholds. These are not limiting factors for UA.

Every SBAMD system needs to find, fix and track a potential threat before it can be targeted and engaged. The smaller the RCS of a UA gets, the harder this process will be and the closer a target needs to come to the sensor to produce usable signal returns. Airborne sensors might be considered for area UA surveillance, but in general measuring against the ground, especially small targets in possibly congested environments can prove very difficult. However, RCS only speaks to radar energy and is very frequency dependant, so

there might be other means of successfully sensing or supporting existing sensors. Optical sensors in the visual, infrared (IR) and ultraviolet (UV) bandwidth might be able to detect UA. Additionally, acoustic sensors might support RF (radio frequency) or optical sensing. Both acoustic and optical sensors have relatively short-ranges compared to radar sensors. Class II and I UA are normally not long-range systems and the smaller the UA, the lower the flight ceiling. This means that due to their operations at lower flight levels, possible stop-and-drop flights and very agile flight paths, these classes impede C-UAS area defences. The lower a UA flies, the more impact the surrounding environment has on the sensor coverage, especially sensor data that could lead to a successful engagement. The same issue generally applies to helicopter defence within typical AD scenarios. The effective reach a C-UAS effector has for Class I and a large subset of class II is very limited; therefore, the launching point will be relatively close to the intercept point. (Specific ranges are heavily dependent on the individual UA.) The result is a reduction of the ability to execute area AD with shrinking UA size, leading to a potential reduction to pure point defence. In regular AD, the term 'point' refers to individual assets that need protection, which in this case could be an individual person. This consequently results in the requirement for a very high number of C-UAS sensors and effectors, or at least a rigorous prioritization of the assets that need protection. Also, concepts of extended self-defence, where individual units assist each other in the exercise of self-defence, become more complicated.

Surface-Based Air and Missile Defence Components

In NATO terminology SBAMD systems are divided into long, medium, short and very short-range systems. This separation was made having air and layered defence in mind. The lower the

effective range of the specific system, the more often it can be found in a mobile, self- or asset defence role. Currently, there are no universal AD systems to cover all air threats. The overall functionality is mainly defined by the available sensors, effectors, and C2 systems. Since SBAMD systems are designed to cover specific subsets of the known or emerging air threat, it needs to be identified how much UA are included and where new solutions need to be found.

Sensors

The longer the range AD systems have to survey, the larger the overall volume of airspace they need to cover. Therefore, modern systems have sensors with very sophisticated volume management to optimize surveillance and tracking in accordance with their specific mission. Some systems have separate surveillance radars or rely on other external sensor sources, which cue the tracking/engagement radars to reduce the overall workload and decrease reaction times. This improves the chance a target gets acquired in a timely manner and that the system can maintain the track over time. In general, targets need to be within a certain spectrum of altitude, speed, RCS and manoeuvrability for a sensor to be able to handle it. Modern surveillance and tracking radars are scanning the air volume in a 'smart' way, meaning the volume gets searched in accordance with the likelihood of a target being present. Also, tracking is supported by a flight path prediction of the individual target. This requires knowledge about the airframes to develop these supportive algorithms. UA, when supported by Artificial Intelligence (AI) guidance and on-board sensors, can lessen the benefits of these sensor algorithms. This will make it harder to search and track targets until the algorithms are updated in accordance with reliable UA threat data, which highlights the need for accurate intelligence data about the UA threat.

As with other air threats, certain UA require specific sensors. Class III UA like High-/Medium-Altitude Long-Endurance (HALE or MALE) UA fly relatively high between 15,000 ft and 60,000 ft with a moderate speed and a large RCS. For long-range surveillance or tracking sensors (e.g. PATRIOT, S-400) this class of UA should not be a challenge to detect. Even for modern medium-range sensors, these airframes should be easy to acquire and track, but at a reduced range. However, since Class III incorporates all UA with a weight over 600 kg, larger rotary-wing designs are included. Hence, the same problems as with helicopter defence for medium and long-range SBAMD units occur. Rotary-wing aircraft can use topography to deny or hinder sensor acquisition and tracking. Also, successful guidance of an interceptor to the target gets more complicated due to terrain masking and RF signal interference with the surface. Short-range sensors very likely do not have the range to be used for HALE or MALE but are sufficient for lower flying UA of Class III, since the RCS is significant and the short-range limits the effect of topography in relative terms.

Below Class III UA, sensors will have a much harder time acquiring and maintaining a track. Of course, the lighter the UA gets, the smaller the RCS could be, especially because larger fractions of smaller UA can be made out of materials that are less RF reflective. Also, the smaller the UA get, the lower they will fly, which reduces the effective range a sensor could acquire and maintain a track. This is especially true for rotary-wing designs, in which a stop-and-drop or rapid direction-changing flight pattern make it harder for regular AD radars to maintain a track. The later a sensor can produce a consistent track that could potentially be engaged, the smaller the protected areas become and the more point or self-defence centric the SBAMD capabilities will be used.

Modern AD radar sensors are extremely capable and their search patterns are software definable, which would allow their use against smaller UA when programmed accordingly. However, the smaller the UA and the shorter the range, the more reasonable and inevitable it becomes to use specifically designed UA sensors for target detection. These systems will be smaller, cheaper and far more flexible for use, especially in a self-defence environment. Also, in this short or very short-range scenario, other sensors (e.g. optical and acoustical) can be employed to support a potential kill chain or to warn military or civilian personnel.

Also, the wavelength, pulse compositions or dwell times of radar sensors needs to be looked at as well. Current AD sensors are optimized against known air threats. It needs to be analyzed, in which subsets of UA they are effective against as well. UA will introduce the possibility of using swarming techniques for attacking targets. Analysis should be conducted in order to identify which kind of sensors are capable of providing adequate SA of large UA swarms, flying close to each other. Also, these sensors need to be capable of delivering fire solutions for suitable interceptors or other means of engagement.

However, emitting RF energy also increases the vulnerability of the SBAMD unit itself. As can be seen in the development of the Israeli Harpy UA family, which uses RF emissions of SBAMD sensors as guidance for their targeting. While the Harpy UA only had an RF seeker to target active radar sensors, the Harop and Mini Harpy both have optical (electro-optical and IR) sensors, which allow them to target even non-radiating systems. Modern systems increase their survivability by frequency management, agility and diversity, as well as the use of dispersion or various camouflaging measures in the optical and IR spectrum. This emphasizes the need for a comprehensive approach to emissions control, passive defence measures and non-radar sensors.

When dealing with small Class I UA, flying relatively low and slow, personal self-protection might also rely on human visual detection and tracking or acoustic orientation to find air threats. Of course, this capability is less precise and less stress-resistant than technical solutions but can provide needed support in close range. However, this 'last resort' option might play a very important role in passive defence and alerting surrounding personnel.

Interceptors

After the detection of potential targets and the provision of a fire solution, an interceptor has to execute another link of the kill chain. The interceptor needs to be capable of denying the UA the ability to deliver effects, like reconnaissance or ordnance delivery. To effectively deny a UA access to an area, a SBAMD interceptor needs to deliver sufficient physical stress on the structure of the UA to render it non-operational.

Regular SBAMD interceptors, from the long–range PATRIOT to the very short-range MANTIS (Counter-Rocket, Artillery, Mortar (C-RAM)) can in theory cover a large subset of UA as well. The distinction should be made between Line-of-Sight (LOS) and Beyond-Line-of-Sight (BLOS) interceptors. BLOS interceptors for SBAMD purposes are missiles, and LOS interceptors can, in addition, be projectiles, directed energy or even simple nets. BLOS interceptors must be equipped with an active seeker or must be capable of receiving target information from a different sensor source.

Long-range interceptors, like a PATRIOT missile, are very well suited for HALE and MALE UA. These targets fly very high, relatively slow and are not very agile, so chances of evasive manoeuvres or hiding behind topography are non-existent. Medium-Range inter-

ceptors like NASAMS missiles[3] are capable of targeting MALE UA, but might lack capabilities to reach all HALE UA. In general, SBAMD interceptors are capable of intercepting UA which operate in their battlespace and where the SBAMD system has created a fire solution. However, as with other air tracks, this becomes more complicated when the targets fly low or can execute evasive manoeuvres before the actual intercept.

The chance of a sensor losing track of very low flying UA due to topography increases with the distance the missile has to bridge. This can easily lead to unsuccessful engagements and the wasting of missiles. Missiles with active seekers will most likely engage low-flying UA from the above, which is a problem for many seekers, due to background noise and signal reflections from the ground. This could also lead to unsuccessful engagements. In general, engaging rotary-wing UA designs over long distances shows little promise, due to their ability of rapid descends and generally very low flight altitudes.

Just because an UA could be engaged by SBAMD systems, does not mean it is a good idea to do so in general, outside of a last resort self-defence situation. SBAMD interceptors, especially long-range missiles, are very expensive, very limited in stock and take a long time to replace. Engaging potentially mass-produced, relatively cheap, easy to replicate UA with a multimillion-dollar missile does not seem cost-effective. Adversaries might otherwise use this tactic to deplete our resources to reduce our overall control of the airspace. Especially in the case of UA swarm operations, where attrition is a calculated factor, the right choice of the interceptor is crucial. Long or medium-range SBAMD missiles will not be able to deliver a reasonable cost-benefit effect on UA swarms and will likely result in the waste of missiles that are possibly needed for other threats.

LOS systems like C-RAM seem very capable of intercepting UA in their respective battlespace. However, since the bullets are not guided, and C-RAM systems were designed to counter targets with steady flight paths, the general effectiveness of such systems looks promising but needs to be evaluated. Most systems fire numerous shots with airburst munitions to increase the chances of hitting the target. An adequate shot doctrine for dedicated UA needs to be identified. Another LOS solution is based on laser technology. Numerous nations (e.g. the Unites States[4] and Germany[5]) are working on fielding short-range laser systems within the next few years. A Laser is less susceptible to target manoeuvring. Although the travel time for the light to the target is neglectable, the laser beam has to stay on the target for a certain amount of time to be effective. This highlights the challenge of precision beam steering.

There is still a significant subset of UA in all three classes that current SBAMD interceptors cannot engage. Also, since the battlespace of current AD interceptors, especially against smaller UA, won´t look like the perfect half sphere, as it is always depicted, the overall airspace that can be covered is quite limited and the intended defended area of longer-range systems becomes more of a point or self-defence scenario. This tremendously increases the need for more systems, otherwise, NATO will be significantly more vulnerable from these kinds of threats.

Command and Control Requirements

Every SBAMD system has a C2 element. This allows for SBAMD units to be integrated into a bigger AD system (e.g. NATO IAMD System) and to locally execute the ordered mission to control the air space. There can be active tasks, embedded in a planned defence design or reactive tasks in the form of self-defence or extended self-defence.

It needs to be assured that a SBAMD unit has all necessary ROE to execute the kill chain in a timely manner. For self-defence, this is always guaranteed by Article 51 of the United Nations Charter. For any other possible scenario, NATO and the nations have to provide a feasible legal framework in the form of ROEs for each unit/command/mission. This becomes more complicated when a SBAMD unit is deployed in a foreign nation, especially prior to a possible conflict. In this case, the legal framework for using military force and executing effective C2 needs to be coordinated and deconflicted with the host nation. Self-defence with application of military force is an appropriate response to an occurring armed attack, even in peacetime. However, UA can be used to prepare such an attack without posing a direct threat to anyone. Here, the so-called 'Caroline Criteria'[6] could be used to justify anticipatory self-defence against an imminent threat. With a clear military purpose for higher-class UA, the declaration of imminence should be less critical, but with the abundance of civil/recreational use of Class I UA, this will be an issue that needs a robust solution.

Also, the process from detection to engagement needs to be fast enough to be effective against a UA threat. High flying Class III UA are no different than regular air threats. However, the timelier a decision needs to be taken, the faster the C2 element needs to be, concerning the technical procedures and the engagement authorization.

In NATINAMDS, SBAMD units can be in various modes of operation (i.e. centralized, decentralized or autonomous), which puts the engagement authority on the appropriate level to optimize the air battle. Self-defence is always autonomous, but with UA defence the terms for extended self-defence and the embedding of UA defence in the overall air battle needs to be clearly defined to

maintain control where possible and be flexible when necessary. However, the more time-critical an engagement decision is, especially with shrinking UA sizes, the more likely it is that the decision has to be taken in an autonomous mode of operation.

The use of UA can be enhanced by employing higher levels of autonomy or AI. This will allow, for example, intelligent swarming and highly reactive single systems. Any counter UAS C2 system will have to be able to make decisions at the speed of relevance. This will most likely force the integration of AI or at least smart algorithms in our own C2 systems as well. The ideas of a human-in-the-loop, human-on-the-loop or totally autonomous operations for C-UAS systems have to be clearly defined.

The integration of other services in a comprehensive approach against UA also needs to be considered. Therefore, the information/data from SBAMD systems which is necessary to feed these other processes, such as offensive targeting, must be identified. Also vice versa, other services might be able to provide intelligence/data to optimize the SBAMD battle. These interfaces and requirements need to be analyzed and perfected.

System Summary and Future Ideas

SBAMD systems are designed to cover certain threats within a defined spectrum. A lot of UA have similar characteristics with these threats. Therefore, SBAMD systems can be used to defend against some UA as well. The performance of SBAMD systems against this identified subset of air threats will be sufficient and reliable for defensive planning purposes. Some small procedural adaptations of SBAMD employment methods might even increase the overall effectiveness and efficiency of the entire AD system. However, a lot of UA do not fall in the categories of known threats or SBAMD

systems can only cover a particular subset of UA. This has several consequences.

- Similar to Ballistic Missile Defence (BMD), UA defence cannot be looked at in isolation. A BMD capable system is always vulnerable to other air threats as is a SBAMD system to ballistic missiles. This means, when using SBAMD systems in a NATINAMDS context for UA defence, the UA have to be part of the layered defence design considerations with all other air threats, areas to be protected, and critical assets or critical infrastructure. Also, a clear gap analysis of active defence systems against the whole threat set needs to be compiled, to optimize mitigation efforts and to better protect the SBAMD systems themselves.

- Considering the capability gap of longer-range SBAMD systems against small UA at close ranges, C-RAM systems have an excellent potential to also serve as protective means for these SBAMD units. If a SBAMD unit is threatened by UA which they cannot engage, C-RAM is possibly the last and only resort. The concept of mixed/layered defence designs becomes even more critical with the added UA threat. This puts significant constraints on a defence design since the numbers of C-RAM systems are very limited. Either the deployment with SBAMD systems hampers the C-RAM mission or the AD design is restricted by C-RAM deployment locations. To maintain operational flexibility, either more systems need to be procured, or other means for UA protection need to be acquired.

- SBAMD systems are responsible for intercepting targets in the air, although some systems incorporate surface-to-surface operations within the limits of their interceptors (e.g. currently SM-6, or NIKE Hercules in the past). With modern, highly capable

radar sensors, this idea might be worth studying, for immediate targeting or providing targeting data to other kill chains.

- For the past 30 years, the force protection community has been arguing that one of the biggest threats to SBAMD systems is not Anti-Radiation Missiles (ARM) but rather a team of Special Operations Forces (SOF), which can easily take out the radar and render any SBAMD unit non-operational for a significant amount of time. Today, the small Class I UA might be a good tool to be used by SOF as well. SBAMD means, even in a mixed/layered defence design, cannot adequately address this threat and protective measures have to be organized more like force protection than AD. This idea holds true for all Class I UA, which are capable of penetrating a C-RAM coverage. Adequate defence solutions need to be identified.

- A comprehensive defence strategy from wide-area airspace to individual personnel or system protection needs to be created. Defence gaps and mitigation measures need to be identified. To achieve that, the threat and threat perspective needs to be unanimous. The following questions need to be answered before creating any defence design:

Which UA are to be expected in the area?

- How will these UA most likely be employed?
- Which UA can and need to be taken care of by SBAMD means?
- Which UA threaten SBAMD systems?
- Which UA can be taken care of by other means?
- Which information is needed from SBAMD systems to achieve this mission?
- What needs to be covered by passive defence measures to reduce consequences?

- What is the remaining risk for the SBAMD systems that needs to be calculated or addressed?

Insufficient answers to these questions will lead to uncertainties in defence planning and increase the risk of failure. This needs to be clearly addressed before preparing optimized leadership decisions. Realistically, there will always be a risk, especially with new threats, but risk mitigation requires the best possible SA.

Some future capabilities might help with mitigating the UA threat and take the stress from SBAMD systems or the overall defence design.

- Airborne sensors could help in various aspects:
  - SA and cueing of SBAMD sensors.
  - Potentially helping SBAMD sensors to remain mostly 'silent'.
  - Possibly identifying UA launch points, for smaller UA.
  - Supporting passive defence measures with SA.
  - Overhead, airborne sensors will have the problem of measuring against the surface, which increases clutter and other unwanted signals. This might hamper the detection and tracking, especially of very small and low/slow flying UA. Nevertheless, it should be analyzed, to determine whether these airborne sensors can help with the UA threat.

- Passive Sensors will play a significant role in UA defence. UA with a bi-directional guidance link or UA that transmit collected data will have a strong RF signature, which can be used by passive sensors for SA and warnings. Future developments might allow this data to be used for effective fire-solutions. Also, passive RF sensors might be able to locate the UA operator as well, if he uses a RF remote control. This would allow passive detection beyond visual range. For visual distances, optical sensors

can be used for surveillance, tracking and possibly engagements. In even shorter ranges, acoustic sensors can support SA as well.

- Some UA are reliant on Global Positioning System (GPS) navigation. It should be analyzed how localized GPS jamming or spoofing could support the protection of SBAMD units.

- Airborne UA interceptors, employed with a yet to be identified concept of human-in-the-loop, human-on-the-loop or even AI-supported higher levels of autonomy might help in reducing reaction times and give an overhead advantage. A similar approach can be found with Destruction of Enemy Air Defence (DEAD) UA like HARPY or HAROP. Maybe this concept can help to mitigate the UA threat as well. As a low-tech variant of this idea, the use of birds to hunt drones as is used in the Netherlands[7] needs to be mentioned.

- BMD distinguishes between Hit-to-Kill (HtK), where the ballistic missile or the re-entry vehicle is completely destroyed, and a mission kill, where the target gets sufficiently affected to the point where it is unable to fulfil its mission. The same idea can be applied for UA defence. Depending on the structural integrity of the UA, an incoming interceptor (as described below) will either completely destroy a target or at least render it non-operational, which would be like HtK. However, since the kill chain can be applied to several links of an UA operation, SBAMD sensor data can be used in a multi-domain approach as well, to support other kill chains, e.g. targeting the pilot or cyber-hacking the control link. This would constitute a 'mission kill'.

- Some Class I UA, potentially targeting SBAMD systems, might be controlled by regular RF remote controls. It should be analyzed, if additional equipment with sensors covering the

respective frequencies for general awareness or triangulation of the operator are beneficial. Other UA might be controlled by regular cell phone connections. Here it should be investigated if RF and cell phone jammers can be incorporated in SBAMD units to add additional protection. Their use before conflict will have to be in accordance with standing laws and regulations.

- UA might be controlled through satellite relays. Since upper-tier interceptors developed to engage ballistic missiles in their mid-course phase are able to reach altitudes of some satellites, the use of SBAMD units for targeting the satellite control link might need to be looked at as well.

The trend of multi-domain threats is becoming more common. Therefore, the approach of looking at UA defence in isolation no longer applies. The defensive idea needs to be layered and must cover as many threat vectors as possible. This calls for more system interoperability, and due to very short decision timelines, more interconnectivity. The overall system needs to be able to provide timely information to the individual units, so that mission execution and SA for passive defence are optimized. Also, defensive weaknesses and capability gaps need to be known so that other mitigating measures can be planned.

Conclusion

Unmanned Aircraft cannot be considered emerging technology anymore, as they are a current reality. Due to their potential effectiveness, relative ease of employment and affordability, they are prone to evolve much faster than regular air threats. Also, it is far more likely to find wide-spread use of UA by our adversaries in upcoming NATO missions than the use of other new technologies,

like hypersonic missiles. This is especially true for missions against non-peer opponents.

Therefore, the following issues/factors need to be considered:

- Stringent incorporation of UA defence in regular AD planning.
- Proper awareness of:
  - Potential Red UA capabilities;
  - Capabilities of Blue SBAMD against Red UA;
  - Realistic capability gap and vulnerability analysis against UA;
  - Addition of UA defence in force protection measures;
  - Adapting Passive Defence measures to counter UA effects.

Since the capabilities of UA will evolve quickly, the field of counter-UAS needs to be on the cutting edge of current developments as well, otherwise NATO will have a clear and decisive disadvantage in upcoming missions.

Endnotes

1. General Ronald R. Fogleman served as Chief of Staff, Headquarters U.S. Air Force, Washington, D.C from Oct. 1994–Aug. 1997.
2. Allied Joint Doctrine for Air and Space Operations (AJP-3.3), Edition C, Version 1 (Draft), NATO.
3. 'NASAMS Norwegian Advanced Surface to Air Missile System', Army Recognition, 13 Aug. 2020. [Online]. Available: https://www.armyrecognition.com/norway_norwegian_army_missile_systems_vehicles_uk/nasams_norwegian_advanced_surface_to_air_missile_system_technical_data_sheet_pictures_video_12712158.html. [Accessed 13 Oct. 2020].
4. Jen Judson, 'Northrop and Raytheon to compete to build laser weapon for short-range air defense', DefenseNews, 1 Aug. 2019. [Online]. Available: https://www.defensenews.com/land/2019/08/01/northrop-and-raytheon-to-compete-to-build-laser-weapon-for-short-range-air-defense/. [Accessed 13 Oct. 2020].
5. 'HEL on wheels - Rheinmetall's high-energy laser effectors get moving', Rheinmetall Defence, [Online]. Available: https://www.rheinmetall-defence.com/en/rheinmetall_defence/public_relations/themen_im_fokus/rheinmetall_hel_live_fire/index.php. [Accessed 13 Oct. 2020].
6. Matthew Waxman, 'The Caroline Affair in the Evolving International Law of Self-Defense', The Lawfare Institute, 28 Aug. 2018. [Online]. Available: https://www.lawfareblog.com/caroline-affair. [Accessed 13 Oct. 2020].
7. Sam Thielman, 'Eagle-eyed: Dutch police to train birds to take down unauthorised drones', The Guardian, 1 Feb. 2016. [Online]. Available: https://www.theguardian.com/world/2016/feb/01/dutch-netherlands-police-birds-unauthorized-drones. [Accessed 13 Oct. 2020].

8

By Major Osman Aksu, TU AF
Joint Air Power Competence Centre

Offensive Counter-Air Operations

Introduction

Technology is transforming our lives every day. Although it provides many advantages, it can also be utilized to develop an effective or deadly weapon by potential adversaries. Among these technological advances are Unmanned Aircraft Systems (UAS) and the corresponding systems to defend against them. Both technologies, UAS as well as Counter-UAS (C-UAS) systems, are increasingly proliferated and potential adversaries develop or acquire these modern warfare technologies. The threat posed by UAS and C-UAS can be very high, hence the goal should be to counter their negative effects on friendly forces, preferably before these systems can unfold their full potential. In order to reduce the undesired effects of new threats on friendly forces, these

threats may need to be addressed as new and highly sensitive targets within the scope of the Air Interdiction (AI) operations which are defined as a core counter-land mission to obstruct or destroy adversaries' capabilities. With AI operations, basic components of UAS (such as UAS ground components, mission control elements, humans, airfields etc.) and C-UAS (especially some Air Defence systems used for C-UAS) can be disabled or rendered ineffective before battle. This chapter outlines how AI can support countering UAS in an early stage of their deployment by attacking their ground components, personnel, and logistics. This chapter also provides an excursion on how to challenge the enemy's C-UAS systems and highlights some examples from recent Turkish warfighting experiences about how to enable operations of friendly UAS in an AI role.

Air Interdiction Fundamentals

By definition, AI is an air operation conducted to divert, disrupt, delay, degrade or destroy an adversary's military potential before it can be brought to bear effectively. It is preventively directed against enemy targets that are not yet an immediate threat to hinder their later engagement against friendly forces. If total prevention is impossible, the enemy should at the very least arrive at the battle late, fatigued, with depleted logistics and low on ammunition and supporting systems.[1]

Physical destruction of the enemy surface force, supporting elements and supplies is the most direct of the aforementioned AI objectives. However, even the enemy's perception of its imminent destruction can achieve substantial delay and diversion of resources, which can be as effective as physically destroying the target.[2]

It is crucial to concentrate the effects of counter-land operations against critical and sensitive targets, since AI assets are generally limited in numbers. AI targets should be determined based on importance, then prioritized based on operational campaign goals. To make the targeting decision sensible, air planners must have timely and accurate intelligence regarding the enemy's capabilities. To accomplish effective AI, intelligence is a key consideration and indispensable to success. During target development, each targeting process must relate specific targets to objectives, desired effects, and accompanying actions. Interdiction should focus on those systems that will provide the greatest payoff and achieve the objective. Appropriate coordination of AI with other joint force components helps preserve friendly freedom of action.[3] Hence, economy of force will be employed by expending minimum effort and forces for AI, and it paves the way for supporting efforts to allocate assets to other military objectives. Chapters 6 and 9 discuss the role of Joint Intelligence, Surveillance, and Reconnaissance (JISR) as well as the targeting process in more detail.

Air Interdiction Considerations for Adversary UAS Technologies

UAS and C-UAS technologies require consideration in the AI target development process, given the undeniable contributions they have already made on the battlefield. UAS are playing vital roles in battlefield operations and becoming an increasingly dangerous threat against forward-deployed troops. Some technological developments have recently emerged to protect friendly troops on the ground from potentially lethal small unmanned aircraft. This section provides some brief examples where adversaries used UAS against friendly or allied forces.

Air Interdiction against UAS Workshops of Armed Groups and Terrorists

During Operation EAST MOSUL, often referred to as the 'Battle of Mosul', Iraqi government security forces, and international Operation Inherent Resolve (OIR) forces retook the city of Mosul from the Islamic State of Iraq and the Levant/Dawlah al-Islāmiyah Irāq wa-as Shām (ISIL/DAESH). Over the nine months of warfighting, more than ten ISIL/DAESH workshops producing and modernizing Unmanned Aircraft (UA) were identified. Even under intense pressure, the ISIL/DAESH continued to develop these technological innovations.

Intelligence revealed that the ISIL/DAESH had a systematic procurement and development strategy for converting commercially available drones into weapons. Additionally, they managed and planned their activities through the establishment of an air operation and observation unit. As a result of the broad possibilities and capabilities offered by UAS technology, the capability portfolio of

Figure 8.1: ISIL/DAESH Drones Captured during Operation EAST MOSUL, Iraq.[4]

the ISIL/DAESH increased exponentially in both offensive and defensive operations, thus posing a serious threat to friendly and allied forces as well as the civilian population.[4]

Furthermore, the other violent armed terrorist organization, the Kurdistan Workers' Party-PKK has had the chance to capture small-sized armed UA from ISIL/DAESH left over after OIR Raqqa operations and used them in their attacks against the Turkish Armed Forces. In the city centre of Hakkari, an armed (carrying a grenade) small drone used by PKK terrorists to attack a military base was shot down by Turkish Armed Forces in 2016. As some other attacks were examined, C4 type explosive material reinforced with nails was used and carried out in different regions close to Hakkari. It was assessed by Turkish Armed Forces that those small-sized UA were produced as deadly weapons in an isolated workshop close to Syria.[5]

These small-sized UA can create severe problems for friendly forces on the ground. Their size, small radar and electromagnetic

Figure 8.2: PKK Drones Captured in Hakkari, Turkey.

signatures, and quieter operation capability make them difficult to detect and track. This challenge remains the same, and comprehensive threat analyses have been conducted under C-UAS technologies programs. However, these drone workshops are counted as potential AI targets. Identifying the location of the terrorist workshops that produce UA of small size, but with large weapons impacts and their rapid destruction within the scope of AI will allow the friendly ground forces to continue their activities without facing these complex threats on the battlefield. In future Alliance operations against an asymmetric enemy, consideration should be given to attacks against drone workshops like those in the previous examples.

Air Interdiction Against UAS of Peer Adversaries

In contrast to the aforementioned UA workshops of non-state armed groups and terrorist organizations, larger systems offer considerably more attack surfaces for AI operations. Larger armed (detectable and trackable sized) UA are game-changers and force-multipliers on the battlefield. As UA are increasing in physical size and technical capability, the number of inevitable impacts they can create on the battlefield is also increasing. Apart from the UA itself, larger UAS typically include Launch and Recovery Units (LRU), Ground Control Stations (GCS), Communications Equipment, Logistics and Supporting Systems, as well as their respective personnel. These systems are highly critical capabilities for adversary UAS operations. Considering their importance during AI target development phase, these core UAS components might need to be prioritized above other threats. Basically, an interdiction target is one that is worth destroying either during the early suppression period of a battle or by direct engagement of the threats to provide disruptive effects. Accordingly, they need to be defeated well in advance of AI operations to significantly affect

the course of adversary operations. Disabling or neutralizing any of the mentioned system components will at least disrupt the associated UAS' operations.

Targeting Unmanned Aircraft on the Ground: Although UA are predominantly Air Defence targets when airborne, destroying UA on the ground is a viable and arguably better option and well in line with the AI definition of destroying an adversary's military potential before it can be brought to bear effectively. Like any manned aircraft, larger UA require an airfield infrastructure to host their significant logistical footprint. Intelligence has to provide the basing locations of enemy UAS units, which should be part of the regular Intelligence Preparation of the Operational Environment (IPOE) anyway. However, if strike assets are limited and targets have to be prioritized, focusing on the UAS elements discussed in the subsequent sections may be the more efficient option. It is important to note that even though the destruction of the UA on the ground is a more difficult targeting option, it may be an undeniable AI operational task in terms of its contributions to the overall campaign.

Targeting Launch and Recovery Units: Launch and recovery of UAS are the most critical and demanding phases of the aircraft's operation. Large fixed-wing UA require an airfield with a paved runway of sufficient length for take-off and landing. Small to medium-sized fixed-wing UA have significantly fewer infrastructure requirements and the LRU is typically more mobile by using a catapult or other vehicle-mounted systems for take-off and landing. Nevertheless, the equipment necessary to launch and recover the UA, as well as its personnel are highly vulnerable during this phase and can be targeted by friendly AI missions.[6] Successful destruction of launch and recovery equipment and personnel or the airfield's runway with anti-runway penetration bombs will cause the UA to remain grounded until the runway is repaired or

LRU has been replaced by a redundant system and backup personnel. Notably, it is common practice that multiple UA are purchased with a single set of launch and recovery equipment, so the redundancy of LRUs is likely lower than the availability of backup aircraft, which makes the LRU an even more valuable target. Those UA using runways can be disrupted by an effective AI attack which creates craters on the runway surface. This kind of runway or LRU AI attacks result in indisputable functional and/or possible physical damage to adversary UA during ongoing flights. This target diversity of AI attacks actually has the same effect on the adversary UAS operations.

Targeting Ground Control Stations: The portion of the Control Element, where the aircraft's pilot and payload operator are physically located, is referred to as the GCS. The physical location of GCS can vary greatly from near the Area of Operations (AOO) to far away and deep inside enemy territory, depending on whether Line of Sight (LOS) or Beyond Line of Sight (BLOS) communications are established. The physical destruction of a GCS will likely disrupt the current operation of all UA linked to it if no redundant system is in place. In the same way as with the LRU, usually multiple UA rely on a single GCS, which makes it a highly valuable target.[6] The GCS location will be important in AI target prioritization and AI force allocation.

Targeting Communications Equipment: UA are highly dependent on connection with ground stations for command and control data links. Radio communications between the UA and its remote pilot is a vital component of any UAS. The respective communications equipment for UAS operating in LOS is usually attached to the GCS or can be found near its location. As the mode of operation indicates, radio antennas do in fact require LOS to the UA, hence they have to be placed quite openly and on elevated positions, making

them lucrative targets for AI missions. UAS operating in BLOS mode typically utilize large satellite ground terminals with diameters of several metres. These ground installations are usually located at a great distance from the AOO, inside enemy territory or a host nation, so they are less accessible to AI missions. However, the large dimensions of the satellite antennas make them vulnerable to identification by any aerial or space imagery. An array of satellite antennas may indicate a nearby Mission Control Element (MCE) for multiple UA and targeting either the antenna array or the suspected MCE buildings could significantly disrupt enemy UAS operations on a broad scale.[6] Depending on the location and type of the GCS, the satellite terminal may vary and the primary satellite equipment which enables the MCE to control the UA's operation will be far away from the AOO. Home-based UAS control elements may not be identified. Therefore targeting expeditionary enemy personnel, LRU and related logistical supplies at a forward operations base close to AOO might be the best option. Again, it is very difficult to attack and destroy Command and Control (C2) systems linked to such technology. Subsequently, a peer adversary may have a well-developed remotely controlled UAS, and this is especially true with the proliferation of more effective C2 and data link technologies. Even though the destruction of the GCS and C2 systems causes a delay in the mission of the enemy UA, they may recover their effectiveness with the introduction of redundant GCS and link systems. In this respect, AI assets need to strike LRU or UA on the ground before the MCE takes control of UA during remote split operations.

Targeting the Logistics and Support Systems: UAS logistical support refers to UAS lifetime operational support; scheduling issues; delivery of goods and services; maintenance, testing, and fielding of UA; design and operation for reliability, safety, availability, and maintainability; logistics for ground station support and mobile

UA platforms; and potentially human operator support. Although a UA does not require a crew on board, it is a kind of flying platform, which requires nearly the same logistics support as most manned aircraft. Thus, UAS logistical support should cover the required support for all subsystems of the UAS including LRU, GCS, MCE, and data link or communications equipment. The UAS logistical support system depends on many different parameters including the type of the UAS, its operational requirements, and its operational environment. For a small hand-launched UAS, relatively little logistical support is required, while larger UAS usually need more logistical support.[7] Destroying logistics and support systems of the UAS components is a solid hit on an adversary's force employment and readiness. It is kind of like cutting off the oxygen that allows UAS military function to operate properly. The destruction of a tactical logistics chain has deep effects and its effects might not be seen in the short-term, but cause inevitable challenges to UAS life cycle management. However, this all depends on where logistical support facilities of UAS are located. Those centres might be embedded into the main airfield's logistics system, or they may be isolated from the main process. UAS logistics facilities, convoys, or supply chain elements are considered to be in safe areas, targeting logistics and support systems are mainly dependent upon precise intelligence.

It should not be forgotten that these candidate target sets are most likely to be protected by highly integrated air defence systems. The ability to locate and destroy these systems before the AI flight is a big challenge. First, a huge issue is the control of the air in the area of interest. All AI operations are tied to the degree of control of the airspace around the target. Historically, control of air has been a crucial factor in modern air operations' success, because it prevents enemy actions directly against friendly assets and facilitates the freedom of action and movement of friendly joint forces. Any

modest degree of air superiority permits friendly air operations to function without prohibitive interference by the adversary. These operations aiming to destroy UAS components may be used to shape the operational environment or to directly support ongoing military operations by isolating the enemy clearly within the AI target group. Additionally, the effectiveness of AI missions is also dependent upon the joint targeting and tasking cycle fed by timely and precise intelligence regarding the operational environment. This kind of AI operation actually permits AI to be considered as a C-UAS capability of friendly forces. With AI operations, the main actions of AI such as 'delay the time of arrival of enemy capabilities and the destruction of enemy forces' will be managed to prevent the peer adversaries' attacks against friendly forces. Ultimately, successful AI creates a negative psychological effect on the adversary's morale.

Countering the Counter-Systems: An Excursion

In cases where air operations should utilize UA, air operations planners must research which enemy troops have Air Defence (AD) systems used for C-UAS operations or what type of C-UAS systems they may possess. In terms of the effectiveness of the operations by the armed or unarmed UA, it will be crucial to detect and destroy the enemy C-UAS capabilities embedded inside their AD within the scope of the AI campaign plan. Simultaneously, neutralizing the enemy's AD systems will also be key to supporting and establishing air superiority over the battlefield. It is nearly impossible to achieve success during the counter-land and air operations without air superiority. After air superiority is gained, all offensive counter operations, including C-UAS operations with AI will be easier for friendly forces. Subsequently, the aforementioned purpose of AI, to delay, disrupt, or destroy enemy forces or supplies en route to the battle area before they can harm friendly forces will be

achieved. If the enemy ground force presents a lucrative AD (used for C-UAS operations) target, AI can be conducted to significantly degrade the enemy's fighting ability. How to achieve a sufficient level of control of the air, which allows for friendly AI operations is, of course, outside the scope of this chapter. The following brief excursion will, therefore, assume that air missions in denied or contested airspace may be primarily tasked to friendly UA in order not to expose manned aircraft to unreasonable risks. In this context, the following section discusses the use of friendly UA against adversary C-UAS systems to enable manned and unmanned AI operations against the target sets discussed earlier in this chapter.

Current Adversary C-UAS Technologies

In late 2017, Syrian non-state militants launched a drone swarm to attack Hmeimim airbase. (cf. Chapter 3, p. 45) In response to the attack, Russia sought to improve its defences against drone systems by working on several models of anti-drone weapons to improve the military's protection.[8] Subsequently, Russia's Ground Forces were augmented by the introduction of units specially formed to combat enemy UAS. Their primary focus was initially to detect and cause interference against UAS. However, it is planned to eventually equip these units with more direct means to destroy UA. The Russian C-UAS units are equipped with dedicated radars and electronic interference systems to jam the drone's communications and navigation systems.[9]

Another system used for C-UAS is the Russian Pantsir-S1, which was originally designed to provide point air defence against aircraft and helicopters and to provide additional protection for AD units against enemy air attacks employing precision munitions, especially at low to extremely low altitudes. These characteristics make the Pantsir-S1 perfectly suited to also counter the complete

spectrum from small to tactical UAS and to close the gap between the dedicated C-UAS systems against large-sized UA and drones in the regular air defence units, which are directed against larger medium- and high-altitude long-endurance UA.

A Successful Example of a Tactical UAS versus a C-UAS System

For the first time, Turkey used armed UA as the primary element in Operation Spring Shield (2020) in Idlib. In the mentioned case, Turkey extensively employed armed UA which struck multiple targets in and around north-western Syria, adjacent to Turkey's southern border. To provide safety for ground troops, these Turkish-made armed UA were hitting and destroying a broad range of military targets from tanks to air defence systems, howitzers, and military bases which demonstrated the efficacy of such devices in a Close Air Support (CAS) role.[10]

Figure 8.3: Russian-Made Pantsir S-1 Air Defence System.

In addition, there was one active Russian-made Pantsir S-1 air defence system deployed inside Idlib for C-UAS. This was a time-sensitive target, posing a real danger to the supporting UA and it needed to be destroyed immediately. The Pantsir S-1 was mounted on its eight-wheel-drive truck sitting placidly as the mini smart ammunition projectile, fired from Bayraktar TB2, proceeded toward it. The Pantsir S-1 active system failed to detect the drone (due to intensive Electronic Warfare operations) and incoming missiles that were flying within range of the radar.[11]

The above example illustrates how an enemy AD system used as a C-UAS capability was destroyed by friendly UA during part of counter-land attack operations. Without having more AI assets, direct destruction of this C-UAS capability of the non-friendly groups had the desired effects on adversary combat power both physically and psychologically. The destruction of these high pay-off

Figure 8.4: Bayraktar TB2 Armed UA.

targets was perceived as critical for accomplishing the objectives. NATO might need to evaluate using tactical UA to neutralize adversary C-UAS systems. Some critical takeaways might be transferable to NATO to improve the operational effectiveness of the alliance against peer adversary C-UAS and evolve current abilities to adapt to threats and the changing character of armed conflict.

Conclusion

Any adversary using emerging technologies, like UAS or C-UAS, may have the potential to be a force multiplier that can play a decisive role on the battlefield, and also change the balance of

Figure 8.5: Air Interdiction Targets.

power. Considering how rapidly these technologies are developing, it should be understood that this prediction is an inevitable reality. The military role of both technologies is growing at unprecedented rates. As the capabilities grow for all types of UAS and C-UAS, nations should maintain a focus to ramp up their research and development efforts, leading to further advances and enabling them to fulfil the widest variety of missions. As a result, the battlefield environment has changed, and our adversaries have shifted their capabilities. The evolving security environment and its dynamics will impact the need for the development of future Alliance capabilities. The respective required technologies need to be assessed using innovative ideas to keep our military edge while conducting real-time analysis of NATO current operations.

According to those examples depicted above, both UAS and C-UAS are currently a part of adversary capabilities and future perspectives. C-UAS systems which are collocated with existing weapon systems, such as counter-mortar and surveillance platforms, are growing threats to friendly forces on the battlefield and need to be neutralized before friendly forces enter the theatre of operations. The widespread use of all types of UAS by both adversary nations and non-state actors increase the threat intensity level and have potential impacts on friendly battlefield operations. When the adversary systems targeted under AI are reviewed, it is clear that these adversary UAS and C-UAS capabilities should also be evaluated as a new target vulnerability and added to the existing target lists when generating target and threat assessments for AI.

The ability to pinpoint and destroy these systems prior to launch remains a challenge for effective counter-land operations. However, the destruction or partial neutralization of the C-UAS and UAS systems on the ground will lead friendly elements to have both physical and psychological advantages over the enemy. With

ongoing and successful AI operations against these new targets, adversary groups will suffer some level of physical and psychological disruption. Sometimes psychological superiority can quickly change the course of the conflict. For instance, attacking and destroying any high-value UA acting as massive surveillance platforms can affect the sensitivities of an adversary's military morale. Psychologically disruptive effects may prove to be an added benefit to AI objectives. The detailed target risk assessment processes and desired effects should determine the setting of objectives and AI operation flow. We are all dependent on each commander to effectively employ military capabilities to achieve planned AI objectives.

Endnotes

1. Allied Joint Doctrine for Air and Space Operations (AJP-3.3), Edition B, Version 1, Apr. 2016, NATO, 2016.
2. 'Annex 3-03 Counterland Operations', in Joint Publication 3-30 Joint Air Operations, US Joint Chiefs of Staff, 2019. [Online]. Available: https://www.doctrine.af.mil/Portals/61/documents/Annex_3-03/3-03-D11-LAND-Interdiction-Obj.pdf. [Accessed 13 Oct. 2020].
3. Ibid.
4. Serkan Balkan, 'Daesh's Drone Strategy - Technology and the Rise of Innovative Terrorism', SETA, Istanbul, 2017. [Online]. Available: https://setav.org/en/assets/uploads/2017/08/Report88.pdf. [Accessed 13 Oct. 2020].
5. Serkan Balkan, 'A Global Battlefield? Rising Drone Capabilities of Non-State Armed Groups and Terrorist Organizations', SETA, Istanbul, 2019. [Online]. Available: https://setav.org/en/assets/uploads/2019/12/R146En.pdf. [Accessed 13 Oct. 2020].
6. André Haider, 'Remotely Piloted Aircraft Systems in Contested Environments', JAPCC, Kalkar, 2014. [Online]. Available: https://www.japcc.org/portfolio/remotely-piloted-aircraft-systems-in-contested-environments-a-vulnerability-analysis/. [Accessed 13 Oct. 2020].
7. K. Valavanis, K. and George J. Vachtsevanos (Eds.), 'Handbook of Unmanned Aerial Vehicles', Springer Netherlands, 2015.
8. 'Russia Developing Anti-Drone Weapons', aerospace.com, 14 Jan. 2020. [Online]. Available: https://www.defense-aerospace.com/articles-view/release/3/208927/russia-developing-anti_drone-weapons.html. [Accessed 13 Oct. 2020].
9. Roger McDermott, 'Russia's Ground Forces Introduce Mobile Counter-UAV Units', The Jamestown Foundation, 12 Feb. 2020. [Online]. Available: https://jamestown.org/program/russias-ground-forces-introduce-mobile-counter-uav-units/. [Accessed 13 Oct. 2020].
10. Alen Lepan (Ed.), 'Ankara's drone air force puts forth new military doctrine, receives wide media coverage', Daily Sabah, 6 Mar. 2020. [Online]. Available: https://www.dailysabah.com/business/defense/ankaras-drone-air-force-puts-forth-new-military-doctrine-receives-wide-media-coverage. [Accessed 14 Oct. 2020].

9

By Adam Jux, UK
Civilian Targeting Consultant

Targeting

Introduction

Targeting is the means of selecting targets to meet a commander's intent and prioritizing them systematically so that the most important are prosecuted first. It includes both a lethal and non-lethal approach by which to prosecute targets and is dependent on the campaign and the intent of the commander. Targets will differ in each campaign.

There are many different ways to organize a nation's or an alliance's targeting approach. The US Joint Publication 3-60 (Joint Targeting), for example, outlines a targeting cycle that supports the Joint Force Commander's (JFC's) joint operational planning and execution with a comprehensive, iterative, and logical methodology for employing the ways and means to create desired effects

that support the achievement of objectives.[1] A representation of this targeting cycle is outlined in Figure 9.1 below.

NATO follows a similar methodology, which is based on an approach that prioritizes targets based on strategic and operational value. It is unlikely that Unmanned Aircraft Systems (UAS) would feature highly in the prioritized list of targets where issues of contested airspace, freedom of manoeuvre or denied areas are prevalent. Both large and small drones would not be appropriately targeted from a strategic or operational point of view, similar to individual tanks or aircraft, but their systems and the overall effect they may be having could be targeted, again, depending on the campaign and its objectives.

It should also be noted that targeting and defending are two different categories which do not systematically meet. One is focused on enemy forces and their destruction whereas the other concentrates on friendly forces' assets and their protection (i.e. a Defended Asset

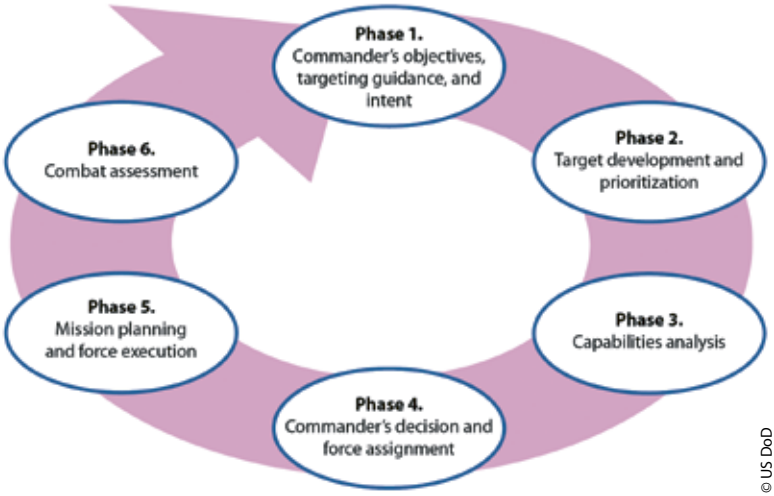


Figure 9.1: Phases of the Joint Targeting Cycle.

List (DAL)). By knowing how to defend against or conduct Counter-Unmanned Aircraft System (C-UAS) operations, one could argue that those systems can be analyzed to target an enemy's UAS inventory. The offensive targeting of those assets, once the campaign has reached an appropriate point in the conflict to do so, is the focus of this document.

Application of UAS

One of the earliest uses of drones in combat was during the Yom Kippur War of 1973, when Israel launched drones that had traditionally been used as airborne targets, to trigger the Egyptian forces into launching their entire arsenal of anti-aircraft missiles. The Egyptian defences were degraded as a result.[2] One could argue that this success is seen as the genesis point for Unmanned Aerial Vehicles (UAV) and UAS in what is now a common feature in most modern militaries.

There are many military applications for drones, and they were primarily exploited for further development after seeing their military advantage during the 1973 conflict. In more modern times, UAS have become more common, and their civilian application from emergency service surveillance to photography and recreation, and even online shopping delivery have been tested and practised. The commonality of drones in society today allows very easy access to something that can be weaponized by those who would use them for terror purposes. There have been several examples of non-formed (non-military) units using them to disrupt modern society. Drones used in terror activities do not need to be packed with explosives to have a significant effect. Examples vary from airport disruption resulting in monetary loss[3] to psychological threats to society's well-being. Although no major attack has been carried

out, the threat remains and therefore has a non-lethal effect on a target/population/society, forcing them to take preventive action and, depending on the effect you wish to achieve, having just as effective an outcome.

With NATO's current focus on 'near-peer' studies, as stated by the Supreme Allied Commander Europe (SACEUR) in a recent US Department of Defense Article,[4] then it would be reasonable to primarily focus on freedom of manoeuvre and countering Anti-Access Area Denial (A2AD) and applying offensive-drone employment against that type of threat where practicable.

The layered defences that near-peer adversaries have developed through technological advances and networked, integrated systems are the new advancement in area denial which has successfully countered the conventional metal-on-metal fight that would be expected if it came to a conflict. It is unlikely that a modern military force would seek to employ a non-traditional drone attack on major systems as described, let alone utilize a vulnerable offensive military UAS.

The more informed reader would also note that the targeting of systems associated with A2AD, in a contested environment, would need to include everything from personnel, finance, logistics, cyber as well as Command and Control (C2) nodes (a Multi-Domain Operations (MDO) approach), as a head-on attack would yield little success.

It would be reasonable to 'pigeon-hole' C-UAS or offensive UAS as a prioritized system for targeting when conditions are set to do so in the battlespace, and not in the early stages of a conflict under the threat of air defence systems. Whilst this is an important area to manage within a conflict, those strategic targets such as A2AD, Inter Continental Ballistic Missiles (ICBM) Threat, etc.

would clearly have a commander's attention at the outset of hostilities as opposed to countering the drone threat. That argument notwithstanding, this is a forum for 'outside-of-the-box thinking'. What if proxy or Special Forces had small UAS in their arsenal and remotely attacked a sensitive part of an A2AD structure to disable it enough for a conventional attack to be successful? It would require modern western forces to change a dated mindset and accept that the development of these systems outside the norms of modern conflict, and an ever-changing battlespace is an investment well spent.

Unmanned Aircraft System Types

Types of UAS could be viewed in two categories: those which are part of a formed-military unit and reflect the capabilities one would see in a modern, western military force, or those which are off-the-shelf, modified, and utilized for quick, hybrid-type and unattributable attacks by personnel whose actions would be more related to terrorist, militia or even organized crime groups.

From a targeting standpoint, the breaking down of systems that contribute to the output of the UAS, a Target Systems Analysis (TSA), would highlight those contributing systems and their vulnerabilities which, in turn, could then be exploited by a prioritisation of targets through the targeting process.

The targeting process mentioned above would identify fixed infrastructure that houses or supports the operations of larger UAS (e.g. hangars, data links, communications nodes, etc.), whereas the process for dealing with smaller UAS would be more reactive and rely on indications and warnings (intel) and would be dynamically driven as their location and appearance could not be positively identified at

the beginning of the targeting cycle. It could be argued that through intelligence-led targeting of these systems and the tracking of personnel integral to the operation of these UAS, one could derive the most effective means of offensively targeting this type of UAS, tracking their whereabouts, identifying their workshops/home base or identifying Tactics, Techniques and Procedures (TTPs).

Target Systems Analysis – General

Target Systems Analysis (TSA) is a system to identify and rank specific targets and their elements so that attack resources can be efficiently used and the most vulnerable element or critical link within a system can be targeted to neutralize the system or unit. Should the TSA determine that the data link is the most vulnerable element, for example, in the analysis of the overall system of larger military UAS, then this would be a focus area for intel gathering and planned attacks on that particular element of the overall system. Should the analysis determine that data links are the focal point for neutralizing the UAS threat, then there will be many factors considered (i.e. vulnerability of satellite links, the satellites themselves, remotely stationed satellite receiver stations, the mitigated risk against one's own forces in attacking this particular element, whether lethal or non-attributable non-lethal action is required, recuperability, etc.)

There are many examples of how to conduct an analysis and the CARVER method is just one example. CARVER is an acronym for attributes used to evaluate a particular target and help in identifying critical elements:

- Criticality. A measure of how critical a node is.
- Accessibility. The ability to physically access and egress from a target.

- Recuperability. The ability of a system to recover from an attack.
- Vulnerability. The ease of accomplishing an attack.
- Effect. The amount of direct loss from an attack.
- Recognizability. The ease of identifying a target.

From its origins during World War II as a method of quantifiably selecting possible targets for interdiction, it has since been refined and was used extensively by the US Special Forces during Vietnam.

Example CARVER Methodology for Larger UAS

Element	C	A	R	V	E	R	Total
Satellite Downlink	1	1	3	4	2	1	12
Aircraft	3	2	1	2	2	1	18
Control Elements	2	3	1	2	2	1	11
Data links	5	8	4	6	5	7	35
Support Personnel	7	8	4	10	4	10	43
Pilots	9	9	7	8	6	9	48

Figure 9.2: An example of the CARVER methodology based on UAS discussion.

The figures are an example only, but the weighting against the system as a whole by targeting the pilots as a vulnerability, would be suggested. Where do the figures come from and what do they represent?

To develop this thought further and to highlight the difference between the different types of UAS, from a targeting perspective, the following targeting details could be considered:

Value	C	A	R
5	Loss would be mission stopper	Easily accessible. Away from security	Extremely difficult to replace. Long downtime (1 year)
4	Loss would reduce mission performance considerably	Easily accessible outside	Difficult to replace with long downtime (< 1 year)
3	Loss would reduce mission performance	Accessible	Can be replaced in a relatively short time (months)
2	Loss may reduce mission performance	Difficult to gain access	Easily replaced in a short time (weeks)
1	Loss would not affect mission performance	Very difficult to gain access	Easily replaced in a short time (days)

Figure 9.3: Notional CARVER Value Rating Scale given as an example.[5]

Larger Drones / Formed Military Units

Conducting a TSA on larger drones would focus on the reliant support elements, support staff, data links, communications, susceptibility to electronic attack and the protection of the physical UAS themselves. These elements make up the system of the UAS/unit which could be systematically exploited through several means, and the targeting

V	E	R	Value
Special operations forces definitely have the means and expertise to attack	Favourable sociological impact. OK impact on civilians	Easily recognized by all with no confusion	5
Special operations forces probably have the means and expertise to attack	Favourable impact. No adverse impact on civilians	Easily recognized by most with little confusion	4
Special operations forces may have the means and expertise to attack	Favourable impact. Some adverse impact on civilians	Recognized with some training	3
Special operations forces probably have no impact	No impact. Adverse impact on civilians	Hard to recognize. Confusion probable.	2
Special operations forces do not have much capability to attack	Unfavourable impact. Assured adverse impact on civilians	Extremely difficult to recognize without extensive orientation	1

process determines which element is the most critical and/or takes the longest to reconstitute, whilst minimizing risk to friendly forces.

Target Systems Analysis – Larger Drones

There are many different types of drones, but many of them have similar components that make up their ability to operate (i.e. the

aircraft, the payload, control elements, data links, their human operators and support elements). These are not exclusive, nor does every element relate to every drone, but they serve as common reference points from which to build a defence against such technology, from a targeting point of view, and will also suffice as a focal point to start offensive operations. Countering UAS relates to defence from UAS rather than the targeting of them, but there are aspects of offensive action that can be taken against those systems. The methodology to be applied should recognize that whilst there are many drone systems, there are also many similarities that can be exploited or protected against. These include:

- **Aircraft** have always been most vulnerable when taking off and landing. They are less manoeuvrable, slower and easier targets. Countering drone attacks at this point can easily identify hangars and aircraft parking areas for conventional targeting. The TSA would identify aircraft/hangars as an element of the overall system and weigh the benefits of targeting these facilities. Failure to target these facilities when their location is known and the capability exists would be a wasted opportunity. Factors will be considered which include reconstitution time, and it will measure the effectiveness of the reduction of the overall force should this element of an enemy's UAS be destroyed.

- **Control Elements** are integral to all remotely piloted systems. The disruption of the signal that controls UAS systems is where this section is focused. Hacking into systems is not unusual, rather it is a low-attributable offensive act that is becoming more of a remote battleground in the 'grey area' of operations. While it could be argued that modern military systems are well protected from hacking, there is a lot of information to the contrary. Only last year (2019), at the Def Con Cybersecurity Conference in Las Vegas, a team of highly-vetted hackers succeeded

in hacking and sabotaging the flight system of a US military fighter jet.[6] This 'grey area' of counter-military operations is effective when targeting a known source or threat, but this is not always the case.

Control elements include both the C2 elements in addition to the actual controlling stations. A TSA will identify these and weigh the pros and cons of an attack against this element, but it might also have a different weighting dependent on the means of attack.

Formed-military units and the location of control elements/C2 elements would expect to be sourced through intelligence for an attack to take place. However, this could result in a conventional or cyber-attack, which would have a different weighting within a TSA. For larger UAS, employing cyber is not without precedent. The US RQ-170 Sentinal UAS, which was captured by Iran in 2011 was 'supposedly tricked into landing where it thought its actual base was in Afghanistan, but instead, it was made to land in Iran'.[7] The Iranians allege 'reverse engineering techniques that they had developed after exploiting less sophisticated American drones captured or shot down in recent years. They were able to figure out how to exploit a navigational weakness in the drone's system'.[8] The inclusion of mobile targets, such as a UAS would be complicated within a deliberate targeting cycle. Tacticians may never know where UAS will be in advance, but a dedicated operation to capture something, similar to the example above, by a land unit would be dependent upon having local tactics to execute.

- **Data Link** is an area that also involves the control elements. Communications are essential to the control of UAS and have been targeted in the past, primarily due to the vulnerability of the link itself. There are many instances where data links have

been targeted to gain control or bring down a drone. From a military perspective, an electronic attack on a known location could be an avenue for C-UAS targeting. While the technology is in its infancy, there is the potential for an Electro-Magnetic Pulse (EMP) aimed at disrupting data links for UAS as a means of defeating a threat. Conversely, there is nothing to prevent the same technology from defending critical infrastructure. Drone Defender Technology from Battelle[9] and Epirus, Inc.'s Leonidas[10] are examples of such technology.

EMP causes electric potential to build up in exposed circuits, and because of its power, Electro Magnetic (EM) shielding does not help protect a UAS design. Induced electric potential is a very high negative charge and travels as an electric current through conductors where the current is high enough to knock out electronic components in its way. As Commercial off-the-Shelf (COTS) drones necessarily use sensitive low-power electronics and require an antenna to function, an EMP will likely destroy all the drones' electronic circuits. The small proportion that are not destroyed outright would potentially be incapacitated by having their radios destroyed. Whether an EMP would have the same effect on larger UAS is a matter for further investigation.

- **Support Personnel.** For military UAS pilots, their lengthy and high degree of training makes them equally vulnerable to multiple threats. This can range from coercion and other non-lethal threats through to individual lethal targeting. The vulnerability of personnel, who have freedom of movement is well known and tracked by foreign intelligence services. Anywhere along the path of daily life could be a potential location for a conventional attack, but coercion is becoming more of a weapon against individuals who have something to hide or be embar-

rassed about. Even the fact that they have been approached is potentially exploitable as it pits one person's word against another as to what has been discussed and agreed, or not.

Smaller Commercial off-the-Shelf UAS

Smaller COTS UAS have a limited range and are small enough to go undetected by regular radar defences. They are made up of a controller and a drone, are highly manoeuvrable, and can appear without notice. All of these factors highlight a wholly different area of focus for C-UAS than that which would be considered for larger drones. The targeting of these systems requires a different approach.

UAS have developed considerably in recent years. So much so that the smaller types are becoming more affordable and are more readily available for use by non-State groups, organized crime syndicates and terrorists. This will increasingly become a matter of concern for all countries and alliances when considering threats to personnel and infrastructure. There have been numerous attacks of this nature that have had varying levels of success, but one thing has been constant regarding the nature of this offensive thinking, and that is the limited development in the way of a defence against low and slow UAS threats from a military standpoint.

Target System Analysis Smaller Drones

In conducting a TSA against this type of UAS, different factors would be considered. It should be noted that:

- **Electronic Defences.** Many modern drones have been built with digital 'gaps' that can be easily exploited, with security often

overlooked in the struggle to satisfy public demand for drones. If the threat against modern-military systems is so easily purchased 'off-the-shelf', then these vulnerabilities will be commonplace amongst those threats.

A study by Johns Hopkins University identified three successful hacks that were easily achieved on a common hobbyist drone.[11]

- The first hack focused on bombarding the UAS with thousands of wireless connection requests asking for control of the airborne device, overloading the Central Processing Unit (CPU) and causing it to shut down.
- The second hack sent the UAS an exceptionally large amount of data exceeding the capacity of the buffer in the aircraft's flight application.
- The last focused on sending repeated signals to the drone's controller, telling it that it was the drone itself. Eventually, the controller started to believe that this was the drone and severed contact with the actual drone.

Whilst these hacks were conducted in a controlled environment, one can easily see how these hacks could be further exploited with little additional effort. Identifying the location of the UAS control station and the ranges required to have an effect notwithstanding, it is an area that could potentially focus on countering inexpensive, COTS UAS threat that is present today.

- **Control personnel** are a vulnerable element of a UAS system and would often be hidden from sight or acting remotely when carrying out a drone attack. Distances vary, but with smaller cheaper systems, it is reasonable to assume that there would only be a small radius of operations from the controller to the drone. Constant Hawk[12] is a Wide-Area Motion Imagery System

> and feeds intelligence data collected in order to understand the environment. It is not a new system and, as the article explains, was used extensively since 2006 in both Iraq and Afghanistan to counter roadside Improvised Explosive Devices (IEDs). More than just Full-Motion Video, monitoring an area surrounding a vulnerable target using this technique has the potential to capture an area of approximately 100 sq. km for constant surveillance. In either real-time or when reviewed at a later stage, following the footage back from an identified launch point/impact point can lead authorities to the location or origin of the actors involved, the building that they operated from for example. Those control personnel can then be individually apprehended or targeted through the normal targeting cycle.

The legalities of this type of targeting would be considered at the time, but the differences between legal targeting and self-defence against this type of threat will be an area for consideration, especially when the perpetrator is a local civilian, and you cannot argue self-defence unless an attack has taken place. The thing we are countering is the perceived attack itself. With that legal issue notwithstanding, and with the example of Constant Hawk in mind, there is a means through intelligence to positively identify and track offenders who may otherwise blend into and hide within local society.

There is a very noticeable difference in the countering of these two different types of UAS, where one is detailed and planned action against a known system that has had a vulnerability identified, while the other is reactionary to a hybrid-type threat to critical infrastructure or personnel. In the case of the latter, then an analysis of the known factors surrounding these types of attacks and utilizing a full coverage of Intelligence, Surveillance and Reconnaissance (ISR) will best enable a defence, along with

indicators and warnings, to this growing threat. Having completed a TSA, regardless of the type involved and analyzed what primarily needs to be targeted in a UAS threat would then form the basis of a defence.

Recommendations

The threat to governments and businesses in modern times is so substantial that there are companies that specialize in C-UAS technology, not only for the military and the terrorist threat that exists in modern-day warfare, but in the civil sector itself. One such company, for example, is the German-based Frauenhofer whose Chairman states '...drones that can carry explosives, self-sufficient delivery drones, self-learning drone swarms – and the materials required are available in every hardware store'.[13]

Many readers with interest in this subject will be aware of the Slaughterbot demonstration on Youtube of autonomous drones searching for targets. Their parameters are defined by facial-recognition technology and social media. It is a fictional demonstration of what potentially could be utilized should drone technology be used for terrorist purposes or even uncontrolled-military purposes.[14] The video was released by autonomousweapons.org and Stuart Russell, a Professor of Computer Science at the University of California, who speculate on the potential of Artificial Intelligence (AI) and in particular, drone technology. If what the Chairman of Fraunhofer states is true, then this technology is available and awaiting exploitation. Utilising drones from an offensive point of view was clearly demonstrated by Stuart Russell and it would be reasonable to expect that it is only a matter of time before this type of attack is commonplace.

Conclusion

It is clear that we are breaking new ground when it comes to countering this type of threat to a modern military force. There are many threats to protect against and many aspects with potential for exploitation. If this new and emerging technology is to be recognized for the threat that it is, particularly the more frequently used non-traditional and hybrid means, then it could be argued that there should be doctrine to give guidance for the protection and future development of C-UAS. This is a cheap, affordable, non-attributable means of conducting a stand-off attack against infrastructure and personnel of importance. The examples thus far of dedicated lethal attacks are limited, but as the technology develops further, the capabilities of newer threats may leave us feeling more vulnerable than we first thought. The reluctance of governments to accuse third parties, due to this non-attributable means of attack, will only bolster and encourage future exploitation through these means.

Endnotes

1. 'Joint Targeting (Joint Publication 3-60)', Joint Chiefs of Staff, 31 Jan. 2013.
2. Spencer C. Tucker and Priscilla Mary Roberts, 'The Encyclopedia of the Arab-Israeli Conflict: A Political, Social, and Military History', Vol. 1, ABC-CLIO, 12 May 2008, p. 1054 f.
3. Gwyn Topham, 'Gatwick drone disruption cost airport just £1.4m', The Guardian, 18 Jun. 2019. [Online]. Available: https://www.theguardian.com/uk-news/2019/jun/18/gatwick-drone-disruption-cost-airport-just-14m. [Accessed 27 Mar. 2020].
4. David Vergun, 'NATO's New Strategy Will Better Protect Europe, Top Commander Says', US Department of Defense, 4 Oct 2019. [Online]. Available: https://www.defense.gov/Explore/News/Article/Article/1981374/natos-new-strategy-will-better-protect-europe-top-commander-says/. [Accessed 30 Mar. 2020].
5. Eric Barnes, 'CARVER Matrix: Tactical Target analysis', Gaijinass, 11 Mar. 2010. [Online]. Available: https://gaijinass.com/2010/03/11/carver-matrix-tactical-target-analysis/. [Accessed 14 Oct 2020].
6. Joseph Marks, 'Hackers just found serious vulnerabilities in F-15 fighter jet', The Washington Post, 14 Aug. 2019. [Online]. Available: https://www.stripes.com/news/us/hackers-just-found-serious-vulnerabilities-in-f-15-fighter-jet-1.594248. [Accessed 30 Mar. 2020].
7. Nancy Owano, 'RQ-170 Drone's Ambush Facts Spilled by Iranian Engineer', PhysOrg, 17 Dec. 2011. [Online]. Available: https://phys.org/news/2011-12-rq-drone-ambush-facts-iranian.html. [Accessed 15 Apr. 2020].
8. Ibid.
9. 'DroneDefender® Counter-UAS Device', Battelle Memorial Institue. [Online]. Available: https://www.battelle.org/government-offerings/national-security/payloads-platforms-controls/counter-UAS-technologies/dronedefender. [Accessed 7 Apr. 2020].
10. Mike Ball, 'Electromagnetic Pulse Capability Integrated into Counter-UAS System', Unmanned Systems News, 21 Jul. 2020. [Online]. Available: https://www.unmannedsystemstechnology.com/2020/07/electromagnetic-pulse-capability-integrated-into-counter-uas-system/. [Accessed 28 Jul. 2020].
11. 'Johns Hopkins Team Makes Hobby Drones Crash to Expose Design Flaws', Johns Hopkins University, 8 Jun. 2016. [Online]. Available: https://releases.jhu.edu/2016/06/08/johns-hopkins-team-makes-hobby-drones-crash-to-expose-design-flaws/. [Accessed 7 Apr. 2020].
12. John Marion, 'Wide Area Motion Imagery Systems: Evolution, Capabilities and Mission Sets', in 'RUSI Defence Systems', Vol. 19, RUSI, 5 Jan. 2017. [Online]. Available: https://rusi.org/publication/rusi-defence-systems/wide-area-motion-imagery-systems-evolution-capabilities-and-mission. [Accessed 30 Mar. 2020].
13. 'Defense against drones – the danger on the radar screen', Fraunhofer, 2020. [Online]. Available: https://www.fraunhofer.de/en/research/current-research/defense-against-drones.html. [Accessed 30 Mar. 2020].
14. Stop Autonomous Weapons, 'Slaughterbots', 12 Nov. 2017. [Online]. Available: https://www.youtube.com/watch?v=9CO6M2HsoIA. [Accessed 30 Mar. 2020].

10

By Lieutenant Colonel (ret.) Panagiotis Stathopoulos, GR AF
Joint Air Power Competence Centre

Electromagnetic Operations

Introduction

The Electromagnetic Spectrum (EMS) comprises the span of all electromagnetic radiation, which is divided into many sub-ranges and separate frequency bands due to their different physical properties. The Electromagnetic Environment (EME) is the geophysical environment, influenced by such factors as terrain, weather and atmospheric conditions, which supports the radiation, propagation, and reception of electromagnetic energy across the entire EMS. To put it simply, the EME is the physical realm which bridges all warfare domains of operation,[1] including Unmanned Aircraft Systems (UAS). Since most UAS depend on the EMS in order to operate, degrading or denying their use of the EMS has the potential to prevent many UAS from conducting effective operations. Electronic

Warfare (EW), the traditional warfighting element of the EME, has been rapidly expanding its capability to include advanced and joint Electromagnetic Operations (EMO) in the EME. This article will discuss how UAS operations could be countered through EMO, concentrating on detection, classification, and engagement.

Detecting and Classifying Unmanned Aircraft Systems

Especially considering the emerging technologies in Low, Small, and Slow (LSS) UAS, detecting and classifying UAS and drones has never been more challenging or critical. Features such as very low Radar Cross Section (RCS)[2] and difficult discernibility in many other spectrums, along with very low flight altitudes and slow speeds can combine to present extremely difficult environments in which to detect these threats. The two ways of detecting UAS using the EMS is through active and passive systems. The main difference between the two is that an active system sends out a signal, and the return signal is analyzed. For passive detection, the detecting system remains silent on the EMS and uses active or passive emissions from the target for analysis.

The active and passive detection and classification techniques that should be considered to accomplish this task are discussed in the following section.

Active UAS detection

Radio Detection and Ranging (Radar) sensors are currently NATO's main option for active air surveillance, target tracking and potentially subsequent engagement guidance. Active radar systems emit Radio Frequency (RF) signals and analyze the backscattered energy from a potential target. Hereby, the architecture, composition and

used frequency of a radar is dependent on the use case and the anticipated targets. Different frequencies have different properties like range, resolution, atmospheric attenuation or accuracy. Very low frequencies could be used for 'Over-the-Horizon' or 'Anti-Stealth' detection, but the respective systems tend to be quite large, and their resolution is significantly lower than systems radiating at higher frequencies. On the other hand, very high-frequency microwave radar systems have an outstanding resolution and accuracy even for very small targets, but have only a very limited range due to atmospheric attenuation. Therefore, most radar systems are designed for a specific purpose in accordance with the anticipated target load and the necessary track quality and a 'One-Size-fits-All' solution does currently not exist.

Radar systems have evolved quite a lot since their inception in 1886 by Heinrich Hertz and they are capable of tracking a wide array of aircraft, satellites or ballistic missiles. To see, how capable existing systems are in coping with Unmanned Aircraft (UA) and drones, they need to be compared to the target types already covered by these systems. In general, four factors primarily influence a radar's capability of detection, namely RCS, altitude, range and speed. The RCS describes the anticipated RF energy reflection of an object from a certain angle and in a certain frequency. When the RCS is large enough to produce an evaluable signal to noise ratio for a sensor, the object is detectable. It needs to be able to distinguish between naturally small RCS (e.g. micro UA) and artificially shrunk RCS like in stealth aircraft (e.g. F-35). The use of low frequencies might help to discover stealth aircraft, but they might not have the resolution and accuracy to detect a small Class I UA or drone. In this case, higher frequencies in the upper centimetre or even millimetre-wave regime can be beneficial. The wavelength specifications need to support the target detection requirements. Once the right frequencies are identified, the signal needs to be

optimized for the target as well. Signal length, pulse composition or pulse compression are just a few parameters or techniques to support detection and tracking.[3] Some target parameters can be identified by analysing changes within the return signal itself. The well-known Doppler Effect can be used to identify the relative velocity of a target towards the sensor since the frequency of the return signal will be shifted accordingly. However, the Micro-Doppler Effect will cause an effect on the return signal due to micro-vibrations or movements of the target. For example, rotor motion can be picked up and analyzed to identify UA and drones and distinguish them from other unwanted targets like birds. This functionality is frequency-dependent, so for very small intra-target motions, high-frequency sensors are needed.[4]

The following figure is a general comparison of RCS from UA and drones with other objects. It shows that a typical Medium-Altitude Long-Endurance (MALE) UAS has an RCS similar to existing fighter aircraft.

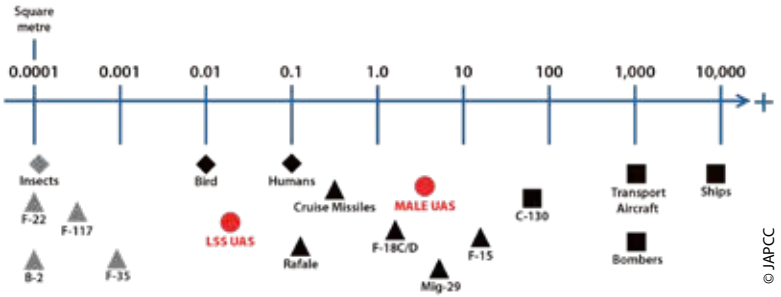


Figure 10.1: Comparative RCS values of various platforms on indicative purposes. These values have been collected from open sources and are referring to controlled and certain factors, conditions and frequencies during real world trials and/or computation, which are not always addressed.

With the radar sensor as the constant in this equation, it can be assumed that the smaller the RCS of an object, the closer it needs to get to the receiver to produce a usable return signal or the more RF energy that needs to be radiated. RF energy output of all systems is limited, so the distance becomes the variable. The detection distance may become even less due to the potentially very low flight paths of small UA and drones, which prevents a line of sight detection independent of the RCS. The short detection range makes these threats a high risk for NATO in general, and it becomes amplified with the employment of small UA and drones in swarms or with high levels of automation.

Most air surveillance/defence sensors are designed to cover very large volumes of airspace in a threat optimized fashion. This means that sub-volumes with a higher likelihood of target presence will be looked at more frequently to increase the probability of detection. This is normally prioritized by the threat/risk-level of the targets, in order for the highly threatening objects to be detected first. Large Class II or Class III UA can easily be incorporated in this calculation and the available sensor mix should suffice. Smaller UA and drones are not only highly threatening but also especially challenging due to their late detection and short engagement distances. Several facts make it infeasible to incorporate these targets into the load for a large volume sensor:

- Every air defence radar has a minimum distance for detection, which might be longer than the UA distance to the sensor.
- A concentration of radar dwell time in the anticipated Class I UA airspace volume will negatively impact the radar's performance in its originally anticipated mission.
- A longer-range sensor might be capable of sensing small UA that pose a risk to itself, but may be challenged to provide coverage for extended self-defence of other entities, due to terrain feature coverage.

This leads to the circumstance that, as with any other air target, an appropriate sensor for the threat has to be identified and most likely this network of various sensors will bring benefits as well. The sensor has to satisfy at least the following needs:

- Cover the target-specific range and altitude band.
- Provide sufficient update rate and accuracy.
- Provide sufficient agility for the mission.

Next to radar sensors using RF signals, other wavelengths of the EMS are being looked at for 'ranging and detection'. In addition to radar, Light Detection and Ranging (LiDAR) can be used for distance, angular and speed measurements of distant objects. LiDAR sensors are often used for 3D mapping of the environment but have also found their way into automation applications, like unmanned cars. Due to their high accuracy and fast update rates, their application in the detection and tracking of small UA and drones is being researched.[5]

Passive UAS Detection

Aside from active detection, where an artificially produced signal is being used and the return analyzed, there are passive options for detection and tracking. Here, the active and passive EMS signatures of an object are used for further processing. The most obvious option is to use deliberate RF emissions like data links, voice-radio emissions or on-board radar sensors. These signals are meant to be received by a dedicated system, so the signal is strong enough to cover relatively large distances. However, every system that is using electronic circuits has a noticeable EMS signature. Here, the unintentional transmission output is far lower, so it cannot be received over large distances. A third option is to basically use a variant of a bi- or multi-static sensor, so-called passive coherent

location radars.[6] In this case, the receiver uses target backscatter from unrelated, but known emitters (e.g. television broadcasting, cellular networks or radio stations) as the source of analysis. Since all of these capabilities are mostly based on the concept of triangulation, arrays of passive sensors are needed for this concept to work. In all three cases, adversary systems can install measures to reduce the applicability of passive detection. Internal circuits can be shielded, so their unwanted transmissions are minimized. RF absorbing coatings or RF energy scattering designs can be used, which are nearly impossible for lower frequency bands. The onboard transmitter can have a very high directionality, with minimized side-lobes, use strong frequency agility/diversity or use very high frequencies that get attenuated by the atmosphere more quickly. However, all these options are more likely to be found in Class III UAS and not the small Class I size or drones. In general, higher levels of automation reduce the need for RF links to a control station, which impedes passive detection as well. Despite these possible countermeasures, the passive detection of Class I or small Class II targets or low RCS Class III UA is a plausible alternative or augmentation to active detection, especially since larger active sensors have weaknesses in short distance detection.

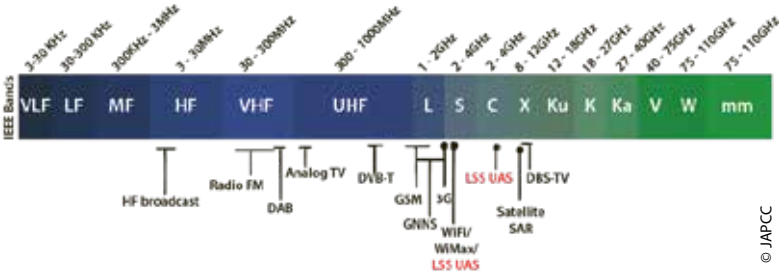


Figure 10.2: Commercial applications in the radio spectrum, whose waves can illuminate a LSS UAS to a passive sensor.

In addition, fielding friendly passive C-UAS detection systems provide excellent concealment against detection by opposing Electronic Support Measures (ESM). Since these friendly passive radars are not emitting energy, they cannot be detected and targeted by EW and SEAD[i] aircraft or UAVs (such as the Israeli 'Harpy' or 'Harop' UAS). Aside from being highly mobile and detecting small or stealthy UA, passive radars can operate in congested EM environments such as urban centres where adversaries will likely employ such UAS.

RF analyzers can be used to identify the frequency of a specific RF transmission or follow complex frequency hopping patterns. These analyzers can detect the control or video signals over the RF (including Wi-Fi[ii] or cell phone signals) employed for UAS operations and can be easily carried on mobile platforms. Once the dedicated frequencies are identified, the controller and drone locations (when actively emitting) can be triangulated by the aforementioned passive radar systems. RF analyzers are a valuable tool to support passive detection of Class I UAS. However, the effectiveness of analyzers can be reduced in highly congested RF environments due to saturation.

Passive sensors and RF analyzers are typical tools in support of ESM. This is the traditional military discipline of EW within the reconnaissance and surveillance systems, to sense and passively collect EM emissions and information to detect, locate, identify, record and analyze radiated EM energy for threat recognition and long-term operational planning. ESM information can be assessed through intelligence products such as Signals Intelligence (SIGINT),

[i] Supression of Enemy Air Defence

[ii] Wi-Fi is a family of wireless network protocols which are commonly used for local area networking of devices and Internet access.

Communications Intelligence (COMINT) and Electronic Intelligence (ELINT). Consequently, this EW function may report the detection of UAS EMS emissions and could contribute to the generation of an Electronic Order of Battle (EOB), which usually includes critical electronic information on threats depicting the likely locations of UAS components such as ground stations. ESM is not usually producing real time data, but it is a good source in support of C-UAS real time operations. Technological advancements have promoted the evolution of tools such as CESMO[7] (Cooperative ESM Operations) that can triangulate and share electronic emitter information within networks almost in real-time and increase the opportunities for UAS detection and C-UAS operations.

Electro-Optic and Infrared (EO/IR). A promising passive method of UAS detection is through the use of Electro-Optic (EO) and Infrared (IR) light sensors. EO includes the visible light and Ultraviolet (UV) light spectrum of wavelengths. The spectrum of these three wavelengths is shown in Figure 10.3.

The detectability and classification of objects through the use of systems utilizing these wavelengths is highly dependent on the reflectivity and emissivity of the object compared to the apparent background, including environmental effects. The designed function of the system will often determine what spectral band is best to achieve detection. For instance, if an object is flying in an

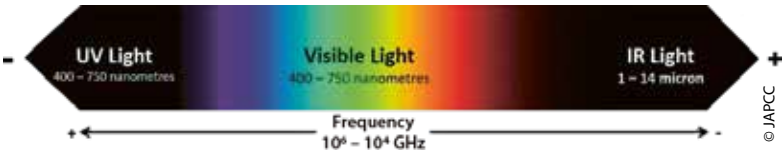


Figure 10.3: Electro-optics and Lasers Spectrum.

environment with little visible and UV light present (such as during the night), IR sensors may be the best solution to trace the IR radiation (heat) emitted by the UA.[8] By contrast, in environments with ample visible light and UV present (such as during the day), EO sensors may be more suited for detection and classification, depending on many variables. Since reflectivity and emissivity of a material changes based on the wavelength of energy being analyzed, the environmental conditions greatly affect wavelength transmission.[9] The use of multi-spectral sensors that can fuse UV, IR, and visible light has great potential to detect UA across a wide range of conditions.

Night Vision Devices & Low Light Cameras. These systems primarily collect ambient visible light and intensify the image by using photocathode technology to produce electrons from the photons in the incident light. They may also integrate IR illuminators to increase their range for detection and classification, making them both a passive and an active system. If the object is emitting or reflecting even a small amount of energy in the visual spectrum, these systems have great potential to be an effective method of detecting UAS at considerable ranges. However, since these low light systems operate with visible light, they have poor performance in twilight conditions and are negatively affected by environments with high humidity, fog or smoke, not unlike other EO systems.

Acoustic Detection

In addition to the IR and EO spectrums, the noise produced by UA can be detected. Microphone arrays can be deployed to detect sound waves and triangulate the origin of the acoustic emission. However, detection ranges of acoustic sensors are very limited and may only support detection of Class I UAS and drones.

Chapter 4 (cf. p. 58 ff.) discusses the acoustic detectability of UA in more detail. Depending on the background noise, detection ranges vary greatly and can be expected to range up to 1,000 m in a quiet rural area, but are limited to only a few hundred meters in a noisier urban environment.

Action Against UAS Within EMS Context

Once the UAS is detected and classified with enough fidelity to determine the appropriate response, effects will need to be applied to the UAS to meet the commander's intent. This section will discuss the many ways EMO can be used to affect an UAS.

Active and Non-lethal EW Actions Against UAS

Traditional active measures for EW are jamming and deception[10] of the signal for UAS control. For jamming, a large enough amount of RF energy (in the previously identified frequency, frequency spectrum or frequency sets) is directed towards the UA's receiving antenna to mask the UAS RF control or data signals. Hence UAS operations are likely the target for denial or disruption. Deception is more complex since it is target and even content-sensitive. Therefore, more information than just the operating frequencies is needed. A signal with a new or altered content to manipulate UAS behaviour gets fed into the UA or control station to interfere with the UAS' mission. Terms like spoofing[iii] or meaconing[iv] are being

[iii] GPS spoofing is the transmission of interfering signals that imitate the GPS signal. In contrast to the GPS jammer, it generates and transmits formally valid but incorrect position data. These jammers are also called pseudolites because they are usually operated on the ground and imitate the signal from satellites. Both civil and military receivers are affected.

[iv] Meaconing is the interception and rebroadcast of navigation signals. These signals are rebroadcast on the received frequency, typically, with power higher than the original signal, to confuse enemy navigation. Consequently, aircraft or ground stations are given inaccurate bearings.

used in this context as well. The advent of UAS has accelerated the development of portable or mobile special jamming/deception systems to counter drones by neutralizing them through EW techniques. Jamming and deception can be done reactively, but also pre-emptively, for example by flooding the anticipated frequencies with RF noise, emitting altered GPS[v] signals or spoofing/hijacking cell tower signals. Such jamming/deception modules can be installed on existing infrastructure like cellular network antennas which would affect UAS signals within a wide geographic area and particularly where UAS Class I and II are likely to operate. These are non-kinetic solutions, which work effectively at close distances against Class I and II UAS rather than Class III UAS that are typically flying at higher altitudes.

Directed Energy Weapons

Although research in the field of lasers for use in military applications has been conducted for over 50 years[11], only recently have laser systems been able to be used to counter air threats such as UAS. Directed Energy Weapons (DEW) systems are designed to provide a focused beam of energy in order to disable or disrupt the target. DEW defensive systems have many possible advantages to traditional kinetic systems, including the capability to perform speed of light engagements, the ability to adjust output energy, the access to potentially unlimited number of shots (limitless magazine), and cost savings when compared to many traditional systems. DEW systems are already being employed for C-UAS on ships and surface vehicles.[12] The primary DEW weapons being employed are discussed next.

[v] The Global Positioning System (GPS), originally NAVSTAR GPS, is a satellite-based radio navigation system owned by the United States government and operated by the United States Space Force.

High Energy Lasers. Since lasers designed to cause blindness in humans were banned by the United Nations in 1995,[13] military lasers have primarily been used to provide precise targeting information to guided munitions and 'dazzle' targets for incoming IR-guided munitions. High Energy Lasers (HEL) have had little success until fairly recently due to rapid technology improvements, whereas having to counter LSS UA was one of the main driving factors for these developments.[14] There are currently multiple HEL systems being deployed by NATO members to combat zones to determine their efficacy in combating small UA.[15] Systems fielded by the US Air Force, Army, Navy, and Marine Corps have all had broad success in the C-UAS mission during recent 'real-world' trials.[16] These trials bode well for the future of HEL to fill the critical role to counter LSS UA now, with larger HEL weapons systems being developed to have increased ranges to counter much larger and capable UA (in addition to other targets).[17]

Electro-Magnetic Pulse and High-Power Microwaves. These types of weapons are capable of disabling or destroying electronic components inside a UAS, instead of hitting the surface of the object with a laser. Electro-Magnetic Pulse (EMP) weapons can be delivered to disrupt radio links and the electronic circuits of the UAS. Even though EMP technology is not yet fully mature, it has been added to many C-UAS systems as another means to provide non-kinetic C-UAS effects.[18] One of the primary benefits of EMP is that it has great potential to be used to counter swarm attacks, in addition to being employed with more focus at individual threats. When focused, it also has good potential to be employed at farther ranges than traditional HEL weapons, however, EMP weapons must be thoroughly tested and employed very carefully since they have the potential to cause significant collateral damage to friendly electronic assets, as well.

Passive EW Actions Against UAS

Passive defence, i.e. the mitigation of radiation propagation throughout the EMS should always be an integral part of countering UAS. It may encompass long-established techniques such as camouflage, sheltering or radio discipline to avoid being detected by an airborne sensor. Chapter 15 (cf. p. 269 ff.) discusses these measures in more detail.

Summary

The combination of UAS features, that may include a wide range of physical sizes, types of missions and payloads, including potential for swarming and full autonomy, lead to the conclusion that there is no single defence method able to counter all classes of UAS. Due to these vast differences, a multi-layered, tailorable, overlapping array of sensors and effectors is required. Mobility, weather and light conditions, network capacity and availability, atmospheric attenuation, the battlespace environment, and technological advancements are all paramount considerations that need to be properly planned to ensure the effectiveness of these sensors and effectors. The challenge of implementing this multi-layered Counter-UAS system of systems array is creating a command and control system able to merge the vast amount of incoming data to present a clear and accurate picture enabling the employment of the most appropriate UAS countermeasures. Managing and controlling sensor data collection through artificial intelligence applications may significantly contribute to creating an adaptable and effective UAS kill chain. Once a UAS is sensed by the network of sensors, an artificial intelligence application could task sensors in the area to gather the needed information to classify the system and then either provide recommended actions to a human response centre or operate autonomously to neutralize the threat.

Endnotes

1. NATO recognizes the following domains of operations: Land, Maritime, Air, Cyberspace and Space.
2. The Radar Cross Section (RCS) is a measure of the radar reflection characteristics of a target. It is equal to the power reflected back to the radar divided by power density of the wave striking the target. For most targets, the RCS is the area of the cross section of the sphere that would reflect the same energy back to the radar if the sphere were substituted. From 'Electronic Warfare and Radar Systems Engineering Handbook', 4th Ed., Naval Air Warfare Center Weapons Division, Point Mugu, CA, Oct. 2013.
3. Christian Wolff, 'Radar Basics', radartutorial.eu, [Online]. Available: https://www.radartutorial.eu/index.en.html. [Accessed 14 Oct. 2020].
4. Victor C. Chen, Fayin Li, Shen-Shyang Ho, and Harry Wechsler, 'Micro-Doppler Effect in Radar: Phenomenon, Model, and Simulation Study', IEEE Transactions on Aerospace and Electronic Systems, Vol. 42, no. 1, Jan. 2006. [Online]. Available: http://www.geo.uzh.ch/microsite/rsl-documents/research/SARlab/GMTILiterature/Ver09/PDF/CLHW06.pdf. [Accessed 14 Oct. 2020].
5. 'LiDAR-based detection and tracking of small UAVs', Fraunhofer Institute of Optronics, System Technologies and Image Exploitation (IOSB), [Online]. Available: https://www.iosb.fraunhofer.de/servlet/is/42689/. [Accessed 14 Oct. 2020].
6. 'Passive Coherent Location (PCL)', GlobalSecurity.org, 2011. [Online]. Available: https://www.globalsecurity.org/military/world/stealth-aircraft-vulnerabilities-pcl.htm. [Accessed 14 Oct. 2020].
7. Erik Bamford and Malte von Spreckelsen, 'Future Command and Control of Electronic Warfare', JAPCC, 2019. [Online]. Available: https://www.japcc.org/future-command-and-control-of-electronic-warfare/. [Accessed 14 Oct. 2020].
8. Georgia Lykou, Dimitrios Moustakas and Dimitris Gritzalis, 'Defending Airports from UAS: A Survey on Cyber-Attacks and Counter-Drone Sensing Technologies', Athens University of Economics & Business, May 2020. [Online]. Available: https://www.mdpi.com/1424-8220/20/12/3537/htm. [Accessed 26 Aug. 2020].
9. G.M.Koretsky, J.F.Nicoll, and M.S. Taylor, 'A Tutorial on Electro-Optical/Infrared (EO/IR) Theory and Systems', Institute for Defense Analyses (IDA), Jan. 2013, p. 20. [Online]. Available: https://fas.org/spp/military/program/track/eo-ir.pdf. [Accessed 26 Aug. 2020].
10. 'Fundamentals of Naval Weapons Systems', US Naval Academy, Weapons and Systems Engineering Department, [Online]. Available: https://fas.org/man/dod-101/navy/docs/fun/part11.htm. [Accessed 14 Oct. 2020].
11. 'Directed Energy Weapons: Counter Directed Energy Weapons and High Energy Lasers', Office of Naval Research, [Online]. Available: https://www.onr.navy.mil/en/Science-Technology/Departments/Code-35/All-Programs/aerospace-science-research-351/directed-energy-weapons-cdew-and-high-energy-lasers. [Accessed 14 Oct. 2020].
12. Sam LaGrone, 'Marines Took Out Iranian Drone for the Cost of a Tank of Gas', U.S. Naval Institute (USNI), 19 Jul. 2019. [Online]. Available: https://news.usni.org/2019/07/19/marines-took-out-iranian-drone-for-the-cost-of-a-tank-of-gas. [Accessed 14 Oct. 2020].
13. International Committee of the Red Cross (ICRC), Protocol IV to the Convention on Certain Conventional Weapons (Protocol on Blinding Laser Weapons), 13 Oct. 1995.
14. Iain McKinnie, 'High-Energy Laser Weapon Systems', Aerospace & Defense Technology Magazine, 1 Jun. 2020. [Online]. Available: https://www.aerodefensetech.com/component/content/article/adt/features/articles/37108. [Accessed 14 Oct. 2020].
15. Thomas Gnau, 'The Air Force just fielded its first high-energy laser weapon overseas', Dayton Daily News, 6 Apr. 2020. [Online]. Available: https://taskandpurpose.com/military-tech/air-force-laser-weapon-fielding. [Accessed 14 Oct. 2020].
16. John R. Hoehn and Kelley M. Sayler, 'Department of Defense Counter-Unmanned Aircraft Systems', Congressional Research Service (CRS), 29 Jun. 2020. [Online]. Available: https://fas.org/sgp/crs/weapons/IF11426.pdf. [Acessed 14 Oct. 2020].
17. Nancy Jones-Bonbrest, 'Scaling Up: Army Advances 300kW-class Laser Prototype', US Army Rapid Capabilities and Critical Technologies Office, 3 Mar. 2020. [Online]. Available: https://www.army.mil/article/233346/scaling_up_army_advances_300kw_class_laser_prototype. [Accessed 14 Oct. 2020].
18. Mike Ball, 'Electromagnetic Pulse Capability Integrated into Counter-UAS System', Unmanned Systems Technology (UST), 21 Jul. 2020. [Online]. Available: https://www.unmannedsystemstechnology.com/2020/07/electromagnetic-pulse-capability-integrated-into-counter-uas-system/. [Accessed 14 Oct. 2020].

11

By Lieutenant Colonel Paul MacKenzie, CA AF
By Major Fotios Kanellos, GR AF
Joint Air Power Competence Centre

Cyberspace Operations

Introduction

It has been stated that Unmanned Aircraft Systems (UAS) are 'reshaping the cyber security world'.[1] While this claim might seem overstated, there's little doubt that the advancement and proliferation of UAS worldwide present many challenges to the cyber security community as UAS increase in sophistication and defenders scramble to keep up with the growing threat. However, while adversaries in possession of UAS exploit their capabilities and invent new avenues for attack, the UAS themselves are 'highly exposed technical systems'[2] and increasingly vulnerable to capabilities operating in and through cyberspace. Indeed, it has also been claimed that, in reference to countering UAS, 'cyber or electronic attack on UAV [sic] may constitute one of the most direct and immediate

ways of implementing cyber power'.[3] A general understanding of the elements of Cyberspace is an important piece as it pertains to the multi-domain, whole of government approach to countering the UAS threat. The aim of this chapter is to provide an overview of Counter-UAS (C-UAS) concepts as it pertains to Cyberspace. This chapter outlines the Layers of Cyberspace, the Cyber Kill Chain, what is meant by 'Counter', Attack Surfaces, Vectors and Tools and includes a special note on the relevance of 5G technology.

UAS are 'reshaping the cyber security world'.

Layers of Cyberspace

Familiarization with what constitutes the Cyberspace Domain is important to understand how capabilities can be brought to bear when C-UAS missions are being considered. At first glance, an UAS might be considered for the airborne platform itself (i.e. Unmanned Aircraft or UA) and only as a part of the Air Domain. However, taking into account the UAS in its entirety, and not the vehicle alone, it becomes clear that this first impression is over-simplified; the entire UAS consists of elements accessible through the Cyberspace Domain. The Cyberspace Domain can be described as comprising primarily three interconnected layers: a physical layer, a logical layer and a cyber-persona layer.[4, 5, 6] The physical layer comprises the Information Technology (IT) hardware, the equipment and networking infrastructure for processing, storing and transmitting data. The logical layer includes inter-related but abstract elements such as data, operating systems, applications, network operations and protocols. The cyber-persona layer is a digital representation of an actor or identity created by the data and rules of the logical

layer. A cyber-persona can be a person, multiple users, an alias, an entity or a machine. When considering C-UAS, all three layers should be assessed as possible attack surfaces.

Cyber Kill Chain

Generating effects in and through Cyberspace varies significantly in degree of difficulty depending on the target and desired effect, but the processes involved are similar. The progression from conceptualization through to achieving the desired effect is referred to as the Cyber Kill Chain and one of the industry's more recognized models[i] was created by Lockheed Martin (LM).[7] The steps in this process include Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control and Actions on Objectives. Each phase presents unique challenges requiring varying degrees of sophistication and investment of time and resources, normally in direct correlation to the value (monetary or strategic) and the level of security afforded the target.

What Do We Mean by 'Counter'?

C-UAS activities can be categorized into three distinct elements, 'detection, non-interactive measures, and interdiction'.[8] Detection activities employ a variety of sensors including 'acoustic, thermal, radar, visual or radio frequency (RF)'[9] to identify the presence of a UA. Non-interactive measures are those employed in response to reduce the impact, such as warning and/or evacuating personnel

[i] Since Lockheed Martin created this model in 2011 various versions have been released, some with 18 steps, including the 'APT Kill Chain' (AIRBUS), 'Internal Cyber Kill Chain Model' (AT&T) and the 'Unified Kill Chain', each with their own pros and cons. The Lockheed Martin Model steps best meet the purposes of this review.

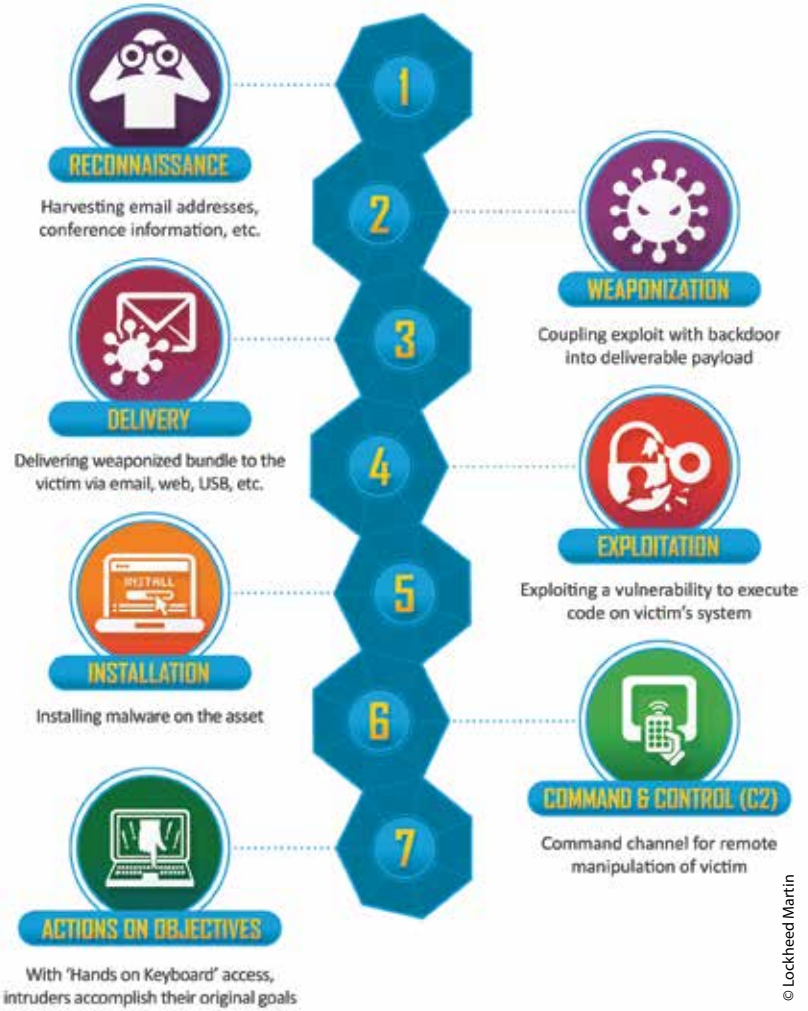


Figure 11.1: Cyber Kill Chain.

from the area. Finally, interdiction refers to action taken to actively engage and influence a UAS. Therefore, C-UAS in this chapter is not referring to passive, defensive measures (technical and/or administrative) to protect our networks, data and critical IT infrastructure from attacks (i.e. firewalls, intrusion detection systems, antivirus applications, etc.) in order to preserve freedom of action. Rather, C-UAS in this chapter refers to active measures implemented to project capabilities in order to defend against UAS threats. Note that NATO, as a defensive Alliance, does not possess resources within either its command or force structure to conduct Offensive Cyberspace Operations, but its operational commanders are able to leverage sovereign cyber effects provided voluntarily by Allies, a process entitled SCEPVA[10]. How effects are generated in and through Cyberspace for C-UAS measures, and what transpires in each step in the Cyber Kill Chain, is ultimately determined by the objective, whether it is to capture, to exploit[ii] or to destroy UAS components.

Capture

Capturing an airborne UA might well be considered the ultimate C-UAS response. Seizing an adversary's high visibility asset not only eliminates it from their inventory and provides a source of intelligence about their capabilities, it can also have a significant impact on morale, improving morale of friendly entities and negatively impacting the morale of the antagonists. Capturing a UA may be achieved by spoofing GPS signals to direct the UA off course to an area where it can be retrieved by associates. One of two popular theories of how Iranian forces came into possession of a US RQ 170 Sentinel in 2001 was that the GPS satellite signal was

[ii] Exploit may be expressed differently in other doctrines or concepts, for example Disrupt, Degrade, Deceive, Manipulate or Influence. See 'Additional References' 1, 2, 3, and 4.

'overlaid by a spoofed GPS-signal originating from a local transmitter with a stronger signal'[11] which created a false indication of the UA's position.[iii] Capture can also be achieved by intercepting the communications links in order to take control of the UA. With autonomous systems malware would have to be introduced before the flight to enter a new flight path and landing coordinates.[12] It is possible to gain access (by keystroke logging[iv]), and change authorizations or access permissions which will make it possible to alter permissions, privileges and authorization and take over and capture the UA. A keylogging virus was detected on US Predator and Reaper UASs at Creech Air Force Base in Nevada in September of 2003 'logging pilots' every keystroke as they remotely fly missions over Afghanistan and other War zones'.[13]

Exploitation

An adversary's UAS might be exploited by leveraging its operation in order to help achieve one's own mission goals, and ideally without the operator's knowledge. UAS can be exploited through intercepting the sensor data, such as the video images to be able to view what an adversary is seeing and to analyze and interpret this for intelligence and force protection purposes. Another possibility is to 'compromise the keys and capture the communications' (eavesdrop/passively monitor) or even 'modify or fabricate information',[14] in other words, intercept what an adversary is communicating and assess it for intelligence purposes (traffic analysis, forensics, location tracking) or change the content (identity Spoofing, Man-

[iii] GPS Spoofing has more commonly been associated with capabilities in the Space and/or EW Domains. In this context, spoofing is achieved via cyber-attack on a ground system, so is included as a C-UAS activity accomplished in large part, if not entirely, through Cyberspace. The subject of the merging of the Cyberspace and EMS Domains is beyond the scope of this study. See 'Additional References' 5 and 6.

[iv] Brief descriptions of Cyberspace Terms are provided in the glossary.

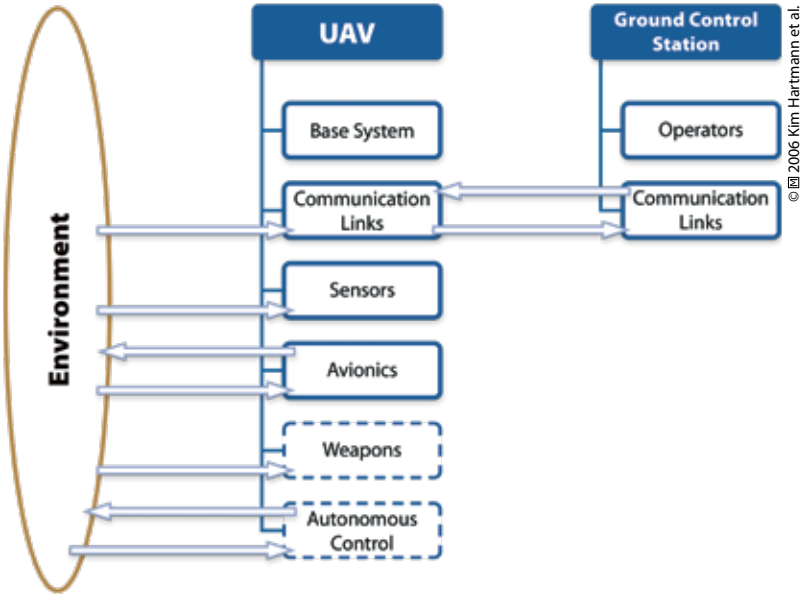


Figure 11.2: Block Diagram of a Typical UAS.[2]

in-the-Middle attack, Message Forgery, Replay Attack) in order to deceive/mislead and influence their decision-making as part of an Information Operation or Deception campaign. Creating a Rogue Access Point would facilitate, depending on the Class and Type of System, accomplishing a Man-in-the-Middle attack, for example. Another, though highly sophisticated approach, would be to conduct a firmware replacement attack, the most opportune time in which to accomplish would be when a UAS is undergoing maintenance, particularly when software or firmware upgrades are taking place. Replacing the firmware with a malicious variant supports installing a back door to allow ongoing access to sessions with the UAS for continuous exploitation.[15] Furthermore, having malware installed would permit influencing the performance, which, in

turn, would enable increasing fuel depletion rates, decreasing the time of operation and reducing the length of a mission.[16]

Destruction

Destroying an enemy UA may be the most probable and more easily achieved C-UAS measure from the perspective of Cyberspace operations. Attacks to influence on-board sensors and alter data regarding (one or more of) location, altitude, speed, pitch, roll and heading etc., in order to cause the UA to either malfunction and crash, to self-destruct by flying outside its own flight envelope for maintaining structural integrity or to fly directly into the ground or another object and be destroyed are all plausible courses of action. Destructive attacks also have a better likelihood of avoiding detection or at least permitting plausible deniability considering that, historically, UA accident rates are 100 times greater than for manned aircraft.[17]

Attack Surfaces

UAS vary a great deal in size and complexity. There is a wide array of UA according to their construction (e.g. the size, weight and payload), their operational capabilities in speed, range and endurance, and their electronic and mechanical design. Such differences result in a large field of UA with a wide variety of flight envelopes, degree of autonomy, level of sophistication and functionality. Regardless, whether small and designed for amateur use, or large and complex, designed for national defence purposes, all UAS are comprised of the same basic components (cf. Figure 11.2, p. 189) and are founded on similar principles. Additionally, the many types of UA should be considered as complex aerial vehicles and exceptionally sensor-driven assets.[18]

Most UAS operations require interaction in a three-dimensional environment under the continuous guidance of the operator and, therefore, require multiple on-board control sensors. Maintaining reliable and synchronized communication channels between these sensors assures the real-time data transfer and control of a UA. The main control elements consist of 'physical infrastructure (external hardware), computer systems (internal hardware) and non-physical software'.[19] Other principle elements common to UAS include the payload, operator, data links and support elements.

During flight, even when in autonomous mode (when applicable), several data links may be established forming a UAS network among one or more Ground Control Stations (GCS), ground-based antennas, Mobile Ground Units or many other UA (e.g. in the case of swarming). A communication link may consist of a continuous and dedicated data link connection, a partly-continuous and semi-dedicated connection, (such as Wi-Fi or Bluetooth), or 'discrete connections', based on pre-programmed flight plan uploaded to the UA through direct access to the hardware from external data storage devices, such as USBs and DVDs.[20] Similar to any other IT network or operating system, UAS networks are crucially dependent on the information flow through the sensors, the links, the avionics and the hardware infrastructure.

The more complex and sophisticated the system elements, the more attack surfaces and number of potential entry points to exploit. By implementing common attack vectors against these surfaces, such as backdoors in a network perimeter, software vulnerabilities, manipulating output data to actuators, compromising input data to controllers, Man-in-the-Middle attacks, database attacks and communications hijacking, it is possible to challenge the Confidentiality, Integrity, and Availability (CIA) of the data flow and, hence, interdict and influence the UAS.[21] These forms of attacks are

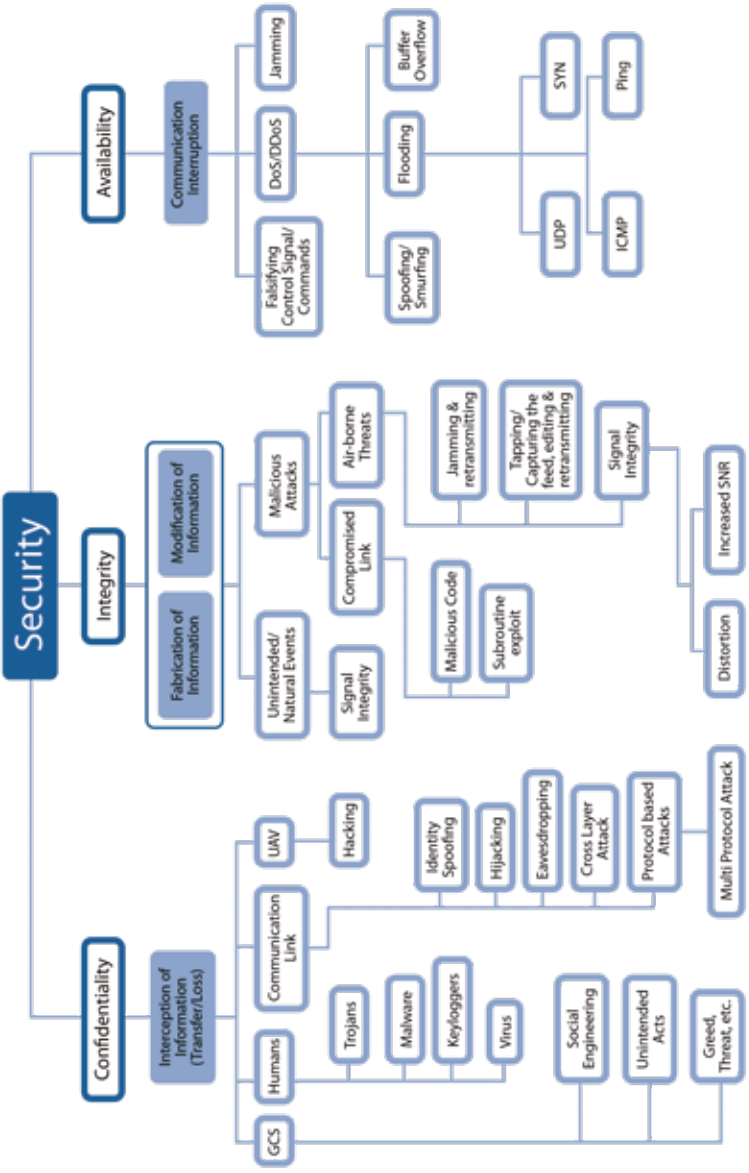


Figure 11.3: UAV System [sic] Cyber-Security Threat Model.[24]

depicted diagrammatically in the 'UAV System [sic] Cyber-Security Threat Model' (cf. Figure 11.3). Remote Code Execution (RCE) is an effective countermeasure which targets not only the flying platform but also the UAS's ground network system, exploiting security flaws and backdoors in firmware, weak passwords, unsecure protocols and software bugs.[22] Moreover, the fact that many of the smaller commercial and consumer drones are using standard, commercially available smartphones as their control platforms, increases the likelihood of known vulnerabilities in the smartphone's operating system to affect the UAS' level of security.[23]

As mentioned, UAS are wide-ranging in type and capability, from small and medium-sized, low-range UAS that can be modified by insurgents and terrorists to suite their purpose, to larger more complex UAS developed by the defence industry including the manufacturers supplying the governments of China, Russia and Iran. It is important to understand as well that it is not exclusively high-end, military-grade UAS that are being employed in conflict. In the Ukraine for example, a large number of civilian or amateur UAS were utilized in the conflict both by the Russian-backed separatists and the Ukrainian Armed Forces, and they are being used extensively in a number of other conflicts including Syria, Iraq, Libya and Yemen.[25] The complexity and cost of the many varieties of UAS vary significantly. The more complex the UAS the more attack surfaces the UAS presents, but they may also have more security provided for them, which consequently requires a greater investment of time and resources to conduct effective C-UAS via Cyberspace.

'Cyber or electronic attack on UAVs [sic] may constitute one of the most direct and immediate ways of implementing cyber power.'

Operators

The operators, whether human or automated, are subject to influence through Cyberspace. The scale of effects can range from trivial such as manipulating the conditions within the deployed climate controlled shelters within which they operate, through to a sophisticated Information Warfare campaign that combines offensive cyber operations with online information operations that aims to influence how they operate and the decisions they make, to more extreme impacts such as contributing to conducting physical attacks on the operators. UAS operators in the Ukraine for example, suffered casualties after being located by Signals Intelligence and targeted by mortar fire.[26] Operators can be targeted even when off-duty, such as via their e-mail or social media accounts, either to influence their behaviour and decision making or as a means to introduce malware into the UAS.

Communication Data Link

UA that are not autonomous are controlled in flight through a communications link referred to as the Common Data Link (CDL). Flight sensor and command data is transmitted via the CDL between the UA and the GCS. The CDL for UAS of short-range (and normally low altitude), such as Man-Portable and Tactical UAS, is via Line of Sight (LoS) that employs either an omnidirectional antenna or a directional antenna aimed at the GCS. Long-range UAS rely on Satellite Communications (SATCOM) networks for the Beyond Line of Sight (BLoS) links. The CDL for Military UAS employing SATCOM is likely encrypted and more difficult to attack.

UAS rely on 'a nearly continuous stream of communications to complete the mission'.[27] However, this CDL can be subjected to cyber-attack, principally with the purpose of gaining control of the

UA. Furthermore, because 'UAVs [sic] are highly dependent on external input and therefore provide multiple input channels' they are difficult to harden.[28] The CDL link can be tampered with, for example through a packet spoofing attack, whereby the attacker mimics the IP (Internet Protocol) address and MAC (Media Access Control) address of the controller since the UA will accept commands when the source IP and MAC addresses are accurate.[29] In many instances if/when this link is lost, the UA will follow a process known as a Lost Link Procedure and first attempt to re-acquire the link, and, if unsuccessful, fly to a pre-programmed geographical position.[30] C-UAS planning that involves interference with the CDL will take this feature of the on-board program into consideration, particularly if the objective is capturing the UA. Loss of the CDL occurs often, as a 2009 report cites that 15 percent of US Army UA accidents were caused by communications failures.[31]

Regarding frequencies, the Tactical CDL (TCDL) is a secure SATCOM link that normally operates in the Ku Band with an uplink in the 15.15 to 15.35 GHz range and a downlink at 14.40 to 14.85 GHz. The data has unique routing, encryption and multiplexing which makes it more difficult to attack. LoS link frequencies are often based on C-Band or Wi-Fi (IEEE 802.11 standard) b-/g- or n- standards with 4.4 to 4.94 GHz uplink and 5.25 to 5.85 GHz downlink. As Wi-Fi employs omnidirectional antennas for controlling UA, it is highly susceptible to eavesdropping.

Internet of Drones

UAS may also be employed to extend an adversary's network connectivity in areas lacking critical IT infrastructure; this arrangement is referred to, in line with the term 'Internet of Things' (IoT), as the 'Internet of Drones' (IoD)[32] In essence, the IoD refers to a configuration where many drones work together, simultaneously

exchanging data, to form a network. They can be operated remotely via the Internet using IP addresses, and this feature opens the possibility for many new applications. At the same time, this means that these UAS are prone to the same security risks as all IP-based functionalities and are vulnerable to be influenced through Cyberspace.

Video Data Link

Apart from the CDL, many UAS employ radio links for additional operational features. Full Motion Video (FMV) is relayed to a Remote Viewing Terminal via a Video Data Link (VDL). This link is also a potential target for exploitation where the link can be intercepted and the images assessed for intelligence by agents other than the operator. In the summer of 2009 US forces discovered days'-worth of US UAS video footage on Iraqi insurgents' laptops which the insurgents were able to capture with software worth $26 (USD)[33] Furthermore, there is evidence of another instance where Israeli UAS video imagery had been intercepted by British forces.[34]

Base System

A UAS is, at its most abstract, an information processing system. Data is sensed, processed, shared, and communicated in order to control flight parameters (speed, altitude, etc.).[35] as well as to collaborate with other UAS within a complex networked environment. UA 'are essentially flying – and sometimes armed – computers'[36] and the base system can be considered the operating system. Therefore, the base system is vulnerable to cyber-attacks comparatively to other information processing and operating systems. Since the Base System is central to the UAS, linking the components, controlling the sensors, navigation, avionics and communications and integrating other optional components such

as special sensors and weapon systems, it is considered a key target for a cyber-attack.[37] With UA being highly technical and prone to faults, many contain Fault Handling Mechanisms (FHM). These FHM could be considered as attack vectors as well, where common functions such as 'self-destruct, automatic-return, land and hover'[38] might be exploited, depending on the desired effect.

Sensors

The UA's sensors include the sensory equipment and integrated pre-processing functions and can be classified according to whether the references are external or internal.[39] Inertial Navigation Systems (INS) are internal sensors, as they detect internal physical parameters such as acceleration or angular rates. Cameras, GPS and Radar are external sensors as they receive information from the environment. Sensors with external references are more susceptible to spoofing and false signals. Internal sensors can drift and deviate from the correct value particularly without synchronization with external sensors so there are inherent errors, but they are less susceptible to attack through the sensors.[40] UA can be outfitted with a variety of different sensors. These include but are not limited to Electro-Optical (EO) and Infra-Red (IR) cameras, low altitude altimeter, Laser Range Finder Designator (LRFD), Synthetic Aperture Radar and Ground Moving Target Indicator sensor (SAR/GMTI). Each sensor provides another attack surface, another vector to engage the UA. The sensor system should be viewed as 'a continuously open input channel and may hence be prone to attacks'.[41] Directions on how to spoof the GPS signal on civilian and military GPS receivers as well as to covertly take over the satellite-lock (a connection synchronised in time and frequency) are posted online for all to see. The possibility of spoofing sensors becomes less likely where data is cross-checked, mutually-enhanced and automatically fused to create a single optical image, as is the case with the MQ-9 'Reaper'

UAS which combines infrared, daylight and light enhancing camera imagery, via the Multi-spectral Targeting System (MTS-B).[42]

Avionics

The avionics system converts the signals either received on the communications channel or pre-programmed (autonomous) to adjust the engine and control surfaces (flaps, rudder, stabilisers, spoilers, digital accelerometers, geofencing software). 'All of these offer a means by which safe operation can be compromised'.[43] UA can be impacted by cyber-attack (such as gain scheduling or fuzzing attack) the effects of which can result in deviations from the values of the altitude, speed, heading, bank angle and/or the pitch angle.[44] Many well-known drone manufacturers, e.g. DJI, for legislation reasons, have embedded geofencing software in their products to prevent them flying over security sensitive areas, such as airports. However, this still voluntary practice cannot be applied effectively for all areas and by every system.

Weapons Systems

Information regarding capabilities to conduct cyber-attacks against Weapon Systems is classified and beyond the scope of this publication. That said, the Weapon Support Systems component of specific UA enable them to carry, launch and operate weapons. It may be enough for C-UAS operations to influence the UA, as controlling the UA may provide sufficient control of the weapons system to meet mission requirements.

UA 'are essential flying – and sometimes armed – computers'.

Data Storage

Many UAS can store up to 30 days of continuous ISR data. However, since the UA sensors can be influenced, whether the stored data is targeted may be less of a factor. Further, the suspected value of the data that is collected and stored will influence the decision what countermeasure to attempt. If the data is desired with no concern whether the adversary is aware, then attempts might be used to capture the UA. If the intent is to acquire the data without the adversary's knowledge, for intelligence or to deceive, then the efforts will be dedicated to exploiting the UAS and copy or alter the data without the operators' knowledge. If, however, the objective is only to keep the data from the adversary then the UA could be destroyed or the data deleted. The storage state will influence the course of action. For example, volatile storage such as RAM (Random Access Memory) is more accessible to compromise of confidentiality. Encryption of the data will protect the confidentiality, but it does not prevent it from being overwritten or being deleted.[45]

C-UAS Cyber Vectors and Tools

Overall, GPS spoofing and Denial of Service (DoS) attacks are the most common C-UAS attacks, and hijacking and destroying UA are the most common results.[46] Passwords are a top priority target in order to gain control of UA and this can be accomplished by tools that execute dictionary attacks, brute force attacks or statistical attacks. Man-in-the-Middle attacks are conducted to exploit UAS and these can be accomplished by eavesdropping and URL (Uniform Resource Locator) manipulation. DoS attacks are used to deny the service to UAS operators and this could be achieved by draining system resources such as processing cycles, power or

memory by continuously flooding the communications with requests.[47] Tools are available to sniff UAS Wi-Fi connections, conduct packet capture and export data as text files, create fake access points, deauthenticate legitimate operators, upload malware (e.g. Maldrone - malware for drones), and execute Buffer Overflow or Cache Poison attacks.[48] These represent but a few of the many possible types of cyber-attacks against UAS.[49] A synopsis of all the cyber-attack vectors and all common tools is beyond the scope of this chapter. Overviews of many common cyber-attack vectors have been published[50] and more tools will continue to be created. In fact, technologies continue to be developed to enable cyber-attacks against UAS (SkyJack, Maldrone, Aircrack-ng and others) and techniques (narratives and videos) on how this can be accomplished are posted online for anyone to access.[51] While applications are available to the public which enable C-UAS in/through Cyberspace for commercial drones, C-UAS capabilities for use against hardened military UAS are classified state secrets and the ability to create and properly Command and Control such effects to reduce unpredictable events remains a 'high art' of which only a few nations are capable.[52]

'The ability to create and properly Command and Control such effects to reduce unpredictable events remains a "high art" of which only a few nations are capable.'

A Special Note on 5G

With the advent of 5G, the next generation of wireless and mobile network, the global commercial and consumer drone industry is likely to change drastically. Although strictly regulatory, frameworks are already in place to restrict commercial drones from

C-UAS Vectors

- Backdoors
- Protocol Vulnerability Attack
- Man-in-the-Middle attacks (also Eavesdropping, URL manipulation)
- Traffic Analysis
- Cache Poison Attack
- ARP Poisoning Attack
- Cinderella (Time Provision) Attack
- Input false data to controller by compromised sensors and/or exploited link between controller and sensors
- Manipulate output data to actuators/reactors from controller
- Compromise network link between controller and actuators
- Distributed Denial of Service (DDoS) Attack
- Buffer Overflow Attack
- Virus/Malware (Maldrone)
- Rootkit Attack
- Password cracking (Brute Force, Dictionary/ Statistical method)
- Port Exploitation
- De-authentication
- Elevation of Privilege
- Masquerade Application
- Secure Socket Layer Interception

C-UAS Attack Hardware/Software

- SkyJackc3
- Aircrack-ngc4
- Node-ar-dronec
- Raspberry Pic
- Parrot AR. Drone – 2c
- Alfac AWUS036H wireless adapter
- Edimaxc EW-781 wireless adapter
- Snoopyc5
- Burp Suite
- LabSat3

Figure 11.4: C-UAS Vectors and C-UAS Attack Hardware/Software.[53]

flying in restricted airspaces. The fact that the 5G infrastructure, especially in urban environments, ensures uninterrupted wireless connection to the Internet, extends the range of small UA beyond the LoS of the controller.

5G's new network architecture allows data rates of up to, theoretically, 10 Gbits/sec, enabling real-time transmission of data and video. Also, this speed reduces the latency to less than 1 ms and ensures the devices will stay connected regardless of their velocity. Finally, 5G exponentially increases the capacity for interconnectivity allowing thousands more IP devices and users to be connected in a small geographical area (network cell).

5G is going to become an absolute game-changer for small- to medium-sized UA as it will provide them not only greater scalability than with 3- and 4G, but also the possibility of BLoS flight, and ubiquitous coverage. For instance, swarming technology is likely to evolve further and military operations will include increasingly more deployable drones with operational squadrons of manned aircraft. Regardless whether small UAS swarms will 'operate as a single body to perform a single function (cooperative swarming) or they perform separate distinct tasks in coordination with each other (coordinated swarming)',[54] it will be possible to control swarms by a single operator and in real time as a result of 5G networks.

To date, C-UAS methods and products have been focused on addressing single UAS threats. As a result, swarming technology enhanced by 5G and Artificial Intelligence (AI) may seem invincible in the immediate future. Exploiting adversaries' UAS swarms can only be achieved by expanding upon the same technology, tools and methods. Sophisticated sensors, tracking software, multifaceted and mixed detection systems, and advanced AI algorithms will be required for an effective C-UAS.

Conclusion

Carter has written that 'The threat of UAS is the strongest multi-domain battlefield weapon of our time'.[55] While such a claim may seem extreme, it remains that effects produced in and through Cyberspace are considered one of the preferred avenues for C-UAS efforts. Being able to bring to bear the capabilities described in this chapter requires a great deal of sophistication and investment of time and resources. Solutions involving Cyberspace are undoubtedly an objective of those nations developing C-UAS programmes and have the ability to project capabilities in and through Cyberspace. Comprehensive knowledge of the targets is critical and here too, the Cyberspace Domain would figure prominently. Cyber espionage activities will be at the forefront of gathering intelligence into Research and Development, Design, Manufacturing, Logistics and Supply Chain processes as part of the Reconnaissance, Weaponization and Delivery stages of the Cyber Kill Chain. However, Cyberspace capabilities are only one element in what should be a broad approach to C-UAS. In short, 'one vector of C-UAS will not solve an issue, other disruptive technologies will have to be combined' to provide a comprehensive solution to counter the UAS threat, as described in the other chapters in this publication.[56]

'One vector of C-UAS will not solve an issue, other disruptive technologies will have to be combined to counter the UAS threat.'

Acknowlegdements

Special thanks to the following people for providing clarification and recommendations during the drafting of this document:

Carolyn Swinney, RAF
Paul Withers, RAF
Hervé Lahille, EAG
Laura Brent, NATO HQ
Nikolaos Fougias, CyOC
Alan Sewell, NCIA

Glossary

- **ARP Poisoning Attack:** Sending malicious Address Resolution Protocol (ARP) packets to a network gateway table and altering the IP (Internet Protocol) and MAC (Media Access Control) address pairs in order to redirect the target's data to a different system.
- **Backdoor:** A method by which users (authorized and unauthorized) are able to by-pass normal security measures and gain access to a system. Backdoors may have a legitimate use and pre-exist to enable System Administrators access. They may be used for nefarious purposes, even created, to allow malicious actors continuous, covert access to a system.
- **Brute Force Password Attack:** A method of cracking a password by systematically attempting different passwords with the intent of eventually guessing the correct password.
- **Buffer Overflow Attack:** An attacker fills a block of memory (buffer) with more data than there is space allocated in order to force the system to execute arbitrary code to take control of the system or cause it to crash.
- **Cache Poison Attack:** Replacing legitimately saved data in a temporary storage area (cache) with corrupted data that contains malicious code such that when the compromised data is sent to, or called up by, the client the malicious code will infect the target with malware.
- **Cinderella (Time Provision) Attack:** Malicious activity aimed at changing the target's clock so that the system's security applications' licenses expire and renders the target system vulnerable to exploitation.
- **De-authentication:** Targets the communication between the user and a Wi-Fi access point by sending disassociated packets and effectively disconnecting the devices.
- **Dictionary Password Attack:** A method of cracking a password by attempting combinations including common words in the dictionary, numbers and symbols or previously used passwords from lists acquired from security breaches.
- **Distributed and Denial of Service (DDoS, DoS) Attack:** A DoS attack is when an attacker seeks to make a system unavailable for its intended purpose typically by flooding the targeted system with more requests than it can process which overloads the system and causes interruption of service. These attacks are relatively simple to conduct, even by unskilled attackers. If the source of the attack originates from multiple, coordinated infected hosts it is referred to as a DDoS attack.
- **Eavesdropping:** A type of man-in-the-middle attack where the attacker makes an independent connection with a victim and relays messages such that the victim believes he/she is communicating with a legitimate party.
- **Elevation of Privilege:** The attacker gains elevated rights to a network, its data and applications due to programming errors or design flaws and is then able to perform unauthorized activity.
- **Firmware Replacement Attack:** Altering the instructions stored in the flash ROM (Read Only Memory) of a device for malicious purposes. The instructions on firmware can be altered in legitimate cases to allow the devices to work more efficiently or function with new operating systems or devices; this occasion can provide the opportunity to covertly modify the instruction set.
- **Fuzzing:** A software testing technique of finding exploitable vulnerabilities by randomly entering different permutations of data (invalid, unexpected or random) into a program to promote abnormal behaviour.
- **Gain Scheduling Attack:** Influencing the attenuation of non-linear dynamics by attacking the systems that use a family of controllers, each of which provides control for different operating points in a system. For example, in aircraft flight control, the altitude and speed might be scheduling variables.
- **Keystroke Logging:** Recording the keystrokes on a keyboard, normally without the user's knowledge, to capture the instructions and data exchanged between the controller/operator and the UAV.
- **Maldrone:** A malware installed and executed in a drone's firmware in order to impact its performance for purposes other than originally designed or perhaps expected by the operator.
- **Man-in-the-Middle (MitM) Attack:** Covertly relaying, and possibly altering, communications between two or more points such that the parties believe they are communicating with each other.
- **Masquerade Application:** When malware is embedded in a legitimate application or when malware is disguised as a legitimate application but executes functions unknown to, and unauthorized by, the user.

- **Packet Spoofing:** Executed by mimicking the IP Address ad MAC address of the legitimate controller, the drone accepts the commands of the rogue agent.
- **Port Exploitation:** Using Internet-connected communications ports required for specific functions for malicious purposes, normally undetected by the operators. This can facilitate service disruption or data theft among other activities.
- **Protocol Vulnerability Attacks:** A general term to describe malicious and/or unauthorized activity against systems by exploiting weaknesses in the rules (protocols) that define how two or more components within a communications system connect and exchange data.
- **Replay Attack:** Delaying the transmission of valid data and re-transmitting altered data in its place without the need of decrypting the message after capturing.
- **Rootkit Attack:** The attacker installs malware on a computer in order to maintain privileged access to areas of its software normally restricted to a limited number of authorized personnel.
- **Secure Socket Layer (SSL) Interception Proxy:** The process of intercepting encrypted internet communication between the client and server without the consent of both entities.
- **Statistical Method Password Attack:** A method of using mathematical statistics to determine passwords with a higher probability of being correctly guessed.
- **Traffic Analysis:** The process of intercepting and examining communications to gain information on transmission patterns. Traffic analysis can be accomplished even if messages are encrypted.
- **URL Manipulation:** Altering the parameters in the Uniform Resource Locator (URL) such that a web server will deliver information to those without authorization.

Endnotes

1. Ley Best, Katherina, Jon Shmid, Shane Tierney, Jalal Awan, Nahom M. Beyen, Maynard A. Holliday, Raza Khan, and Karen Lee, 'How to Analyse the Cyber Threat from Drones', Chapter One, 1, RAND, 2020. [Online]. Available: https://www.rand.org/pubs/research_reports/RR2972.html. [Accessed 20 Apr. 2020].
2. Kim Hartmann, Christoph Steup, 'The Vulnerability of UAVs to Cyber Attacks – An Approach to the Risk Assessment', 5th International Conference on Cyber Conflict, 2013, p. 1.
3. Kim Hartmann, Keir Giles, 'UAV Exploitation: A New Domain for Cyber Power', 8th International Conference on Cyber Conflict, 2016, p. 211.
4. US Department of Defense, Joint Publication 3-12, 'Cyberspace Operations', 8 Jun. 2018, I-2. [Online]. Available: https://fas.org/irp/doddir/dod/jp3_12.pdf. [Accessed 27 Apr. 2020].
5. UK Ministry of Defence, 'Cyber Primer', 2nd Edition, Jul. 2016, p. 7.
6. NATO, Allied Joint Publication 3.20, 'Allied Joint Doctrine for Cyberspace Operations', NATO Standardisation Office, Jan. 2020, p. 3.
7. Lockheed Martin, 'The Cyber Kill Chain'. [Online]. Available: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html. [Accessed 27 Apr. 2020].
8. Kay Wackwitz, 'Anti-Drone Solutions: Possibilities and Challenges', Drone Industry Insights (DRONEII), 17 Jan. 2020. [Online]. Available: https://www.droneii.com/anti-drone-solutions-possibilities-and-challenges. [Accessed 17 Apr. 2020].
9. Ibid.
10. Ibid. 6, 21.
11. Ibid. 8.
12. Ibid. 2, 7.
13. Noah Shachtman, 'Computer Virus Hits US Drone Fleet', Wired, 10 Jul. 2011. [Online]. Available: https://www.wired.com/2011/10/virus-hits-drone-fleet/. [Accessed 1 May 2020].

14. Gaurav Choudhray, Vishal Sharma, Takshi Gupta, Jiyoon Kim and Ilsun You, 'Internet of Drones (IoD): Threats, Vulnerability, and Security Perspectives', Aug. 2018, p. 4.
15. Ibid. 13, 8.
16. Ibid. 13.
17. Major Jason A. Yochim, 'The Vulnerabilities of Unmanned Aircraft System Common Data Links to Electronic Attack', US Army Command and General Staff College, Jun. 2010, p. 67.
18. Ibid. 3, 207.
19. André Haider, 'Remotely Piloted Aircraft Systems in Contested Environments', Joint Air Power Competence Centre (JAPCC), Sep. 2014, 2. [Online]. Available: https://www.japcc.org/portfolio/remotely-piloted-aircraft-systems-in-contested-environments-a-vulnerability-analysis/. [Accessed 1 May 2020].
20. Ibid. 3.
21. Randall K. Nichols, Hans C. Mumm, Wayne D. Lonstein, Julie J.C.H. Ryan, Candice Carter, and John-Paul Hood, 'Understanding Hostile Use and Cyber Vulnerabilities of UAS: Components, Autonomy v Automation, Sensors, SAA, SCADA and Cyber Attack Taxonomy' in Randall K. Nichols (Ed.), 'Unmanned Aircraft Systems in the Cyber Domain', Jul. 2019, p. 74.
22. Ibid. 20, 78.
23. Ibid. 3, 209.
24. Ahmad Yazdan Javaid, Weiqing Sun, Mansoor Alam, and Vijay K. Devabhaktuni, 'Cyber security threat analysis and modeling of an unmanned aerial vehicle system', Nov. 2012. [Online]. Available: https://www.researchgate.net/publication/235676360_Cyber_security_threat_analysis_and_modeling_of_an_unmanned_aerial_vehicle_system/. [Accessed 1 May 2020].
25. Ibid. 3, 205, 211.
26. Ibid. 3, 205, 212.
27. Ibid. 17, 56.
28. Ibid. 2, 5.
29. Elsa Dahlman and Karin Lagreliius, 'A Game of Drones: Cyber Security in UAVs', KTH Royal Institute of Technology, 2 Oct. 2019, p. 19.
30. Ibid. 17, 5.
31. Ibid. 17, 68.
32. Ibid. 13, 1.
33. Ibid. 12.
34. Ibid. 3, 210.
35. Randall K. Nichols, Hans C. Mumm, Wayne D. Lonstein, Julie J.C.H. Ryan, Candice Carter, and John-Paul Hood, 'Counter Unmanned Aircraft Systems Technologies and Operations', New Prairie Press, 2020.
36. John Villasenor, 'Cyber-Physical Attacks and Drones Strikes: The Next Homeland Security Threat', Brookings, 5 Jul. 2011. [Online]. Available: https://www.brookings.edu/research/cyber-physical-attacks-and-drone-strikes-the-next-homeland-security-threat/. [Accessed 13 May 2020].
37. Ibid. 2, 6.
38. Ibid. 2, 17.
39. While this paper delineates UA sensors into 'external and internal,' militaries and other disciplines may separate these components into vehicle (i.e. INS and GPS) and payload (i.e. cameras, radars etc.).
40. Ibid. 2, 12.
41. Ibid. 2, 7.
42. Ibid. 2, 14.
43. Ibid. 3, 213.

44. Alan Kim, Brandon Wampler, James Goppert, and Inseok Hwang, 'Cyber Attack Vulnerabilities Analysis for Unmanned Aerial Vehicles', American Institute of Aeronautics and Astronautics, Jun. 2012. [Online]. Available: https://pdfs.semanticscholar.org/1a95/4775dd9a2596b7543af7693d707415077289.pdf. [Accessed 13 May 2020].
45. Ibid. 2, 15.
46. Ibid. 27, ii.
47. Ibid. 27, 9.
48. Jean-Paul Yaacoub, Hassan Noura, and Ola Salman, 'Security Analysis of Drones Systems: Attacks, Limitations, and Recommendations', in 'Internet of Things', Vol. 11, Sep. 2020, p. 19. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2542660519302112. [Accessed 13 May 2020].
49. Product Description, Aircrack-NG, 25 Jan. 2020. [Online]. Available: https://www.aircrack-ng.org/. [Accessed 3 May 2020].
50. Ibid. 20.
51. Sander Walters, 'How Can Drones Be Hacked? The updated list of vulnerable drones & attack tools', Medium, 29 Oct. 2016. [Online]. Available: https://medium.com/@swalters/how-can-drones-be-hacked-the-updated-list-of-vulnerable-drones-attack-tools-dd2e006d6809. [Accessed 4 May 2020].
52. James A. Lewis, 'The Role of Offensive Cyber Operations in NATO's Collective Defence', Tallinn Paper No. 8, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 2015, 9. [Online]. Available: https://ccdcoe.org/uploads/2018/10/TP_08_2015_0.pdf. [Accessed 13 May 2020].
53. Sources for Figure 11.4: Ibid. 22, 74. Ibid. 49, 19. Ibid. 1, 47. Candice Carter, C-UAS Evolving Methods of Interdiction, in Randall Nichols (Ed.), 'Counter Unmanned Aircraft Systems Technologies and Operations', Feb. 2020, 10. [Online]. Available: https://kstatelibraries.pressbooks.pub/counterunmannedaircraft/chapter/chapter-6-interdiction-technologies-carter/. [Accessed 13 May 2020].
54. G. James Herrera, Jason A. Dechant, and E. K. Green, 'Technology Trends in Small Unmanned Aircraft Systems (sUAS) and Counter-UAS: A Five-Year Outlook', Institute for Defense Analyses (IDA), Nov. 2017, 21. [Online]. Available: https://www.ida.org/research-and-publications/publications/all/t/te/technology-trends-in-small-unmanned-aircraft-systems-suas-and-counter-uas-a-five-year-outlook. [Accessed 13 May 2020].
55. Candice Carter, 'Understanding C-UAS Purpose and Process', in Randall Nichols (Ed.), 'Counter Unmanned Aircraft Systems Technologies and Operations', Feb. 2020, 4. [Online]. Available: https://kstatelibraries.pressbooks.pub/counterunmannedaircraft/chapter/chapter-2-understanding-c-uas-purpose-and-process-who-may-want-or-need-to-counter-uas-operations-legitimate-versus-criminal-selected-c-uas-use-cases-examples-of-how-and-when-c-uas-is-approp/. [Accessed 13 May 2020].
56. Ibid. 52.

12

By Lieutenant Colonel Heiner Grest, GE AF
By Lieutenant Colonel Henry Heren, US SF
By Lieutenant Colonel Tim Vasen, GE AF
Joint Air Power Competence Centre

Space Operations

Main Characteristics of Space Systems and Their Role in Modern Warfare

Today's modern warfare is heavily dependent on the Space Domain;[1] the use of Data, Products and Services (DPS) from Space-based capabilities allows all national armed forces, to include NATO as well as potential adversaries, to achieve their objectives with increased effectiveness and efficiency, with a reduction of time and with lower risks to friendly personnel and material. This is especially true for Unmanned Aircraft Systems (UAS), which strongly rely on all types of DPS.

In the early decades of Space exploration, the two superpowers, the USA and the former Soviet Union, were the driving forces

behind humanity's push to Space beyond earth's atmosphere, and thus reaped the greatest benefits from their endeavours. Today, there are many new members of the exclusive 'Space-Club' who are engaged in scientific, governmental, and economic activities. At the same time, there are also military activities in Space from a resurgent Russia, and both a rising China and India.

When talking about Space, we have to realize the term refers to the operational domain. Often, we are actually discussing Space Systems versus the operational domain, and so we have to add a modifier for specificity and clarity.

Space Systems are seen as consisting of four segments:[2]

- **Space Segment:** the satellite in orbit;
- **Ground Segment:** Command and Control (C2) facilities of the satellite and its payload;
- **User Segment:** DPS received from the payload and used by consumers;
- **Link Segment:** uplink and downlink of electromagnetic signals carrying C2 as well as mission data.

Only the entirety of all segments guarantees the functionality of the overall system. Failure of any one segment, whether intentionally or unintentionally, compromises the use of an entire system, which allows for more than one potential option to counter an adversary's Space-based capabilities, and, in turn, its UAS.

The use of Space-based services brings advantages, (e.g. worldwide coverage with smaller forces, terrestrial information without violating any state's sovereignty, no border crossing restric-

tions, [near] real-time transmission, unfiltered data, enabling expeditionary operations with light forces, reach-back options), as well as disadvantages (e.g. time over target, resolution, some weather conditions) and calls for exact planning (e.g. revisit rate, persistence, responsiveness) with respect to the specifics of each satellite on its respective orbit.

For this document an orbit is defined as a regular and repeating elliptical path around the earth. Typical orbits are:

- **Low Earth Orbit (LEO):** 200–2,000 km, approx. 100 min/orbit, for ISS, ISR (EO, Radar), weather, scientific
- **Medium Earth Orbit (MEO):** 2,000–36,000 km, 5-12 hours/orbit, for GNSS, some communication
- **Geostationary Earth Orbit (GEO):** 36,000 km, 24 hours/orbit, stationary over equator for communications, Early Warning, weather, relay
- **Highly Elliptical Orbit (HEO):** typical 200–40,000 km, main coverage over the Northern Hemisphere with a long dwell time, especially for communications

A full integration of all DPS, provided by Space-based assets and free from any breakage, into modern military systems will assists the effectiveness of almost all modern military operations. The Space Domain is seen as a critical force multiplier or at least as a force enabler; no single modern operation planned or executed by modern armed forces can be done without appropriate Space support.

Given this understanding of the dependencies, UAS operations in particular are highly dependent on Space-based DPS. However, the degree of dependence may vary based on the class, range, mission, and system specifics of individual UAS.

Military Space Capabilities in General

To gain an appreciation for the military use of Space-based activities, a review of the current classifications utilized by NATO is helpful, as is possible adversarial use of the Space Domain. Space activities can generally be structured into six functional areas:[3]

Positioning, Navigation and Timing

Space-based Positioning, Navigation and Timing (PNT) from Global Navigation Satellite Systems (GNSS) provides accurate geo-spatial positioning and timing information anywhere on or near earth. GNSS provide for multiple uses and they allow for precision and lethality in military operations.

The Global Positioning System (GPS) is an established US GNSS, initially intended for military applications, but available for free civilian use since the 1980's. Other GNSS's in use and/or in development are Galileo (EU), Glonass (Russia) an Beidou-III (China).[4] Additionally, India's NAVIC (Navigation Indian Constellation) or IRNSS (Indian Regional Navigation Satellite System) and the Japanese QZSS (Quasi-Zenith Satellite System) are systems with regional coverage and orientation. These are called Regional Navigation satellite systems (RNSS). This variety of systems highlights that GNSS are not limited to only NATO, and that a potential adversary could utilize other PNT information for their unmanned systems as necessary.

Moreover, all of these passive systems, meaning only the satellite is transmitting a signal, enable high-fidelity force navigation and specific military operations, such as precision strike, personnel recovery, friendly force tracking, and network synchronisation. However, there are some potential limitations to these systems

due to the weakness of the signal (e.g., atmospheric influences, urban canyons, or dense vegetation), which makes interfering with the signal (i.e., jamming or spoofing) an excellent option to reduce the effectiveness of an adversary's GNSS.

Intelligence, Surveillance and Reconnaissance

Military planning and operations require access to pertinent information. Intelligence, Surveillance and Reconnaissance (ISR) satellites are one of many means for collecting information for the intelligence community, which can be processed into targeting information for UAS operators. Electro-Optical (EO), Infrared (IR) and Synthetic Aperture Radar (SAR) are typical sensors using specific wavelengths to collect images for various purposes. Most of these satellites provide global coverage, which is valuable for preparations prior to possible conflicts. There are limitations to specific sensors in the form of resolution, coverage area, revisit times, the predictability of their orbits, as well as atmospheric disturbances.

Meteorology and Oceanography

Precise weather forecasts are necessary for planning and execution of all kinds of military operations, especially for UAS, which are generally vulnerable to adverse weather conditions. Satellites monitoring for changes in the earth's atmosphere are one integral part of the Meteorology and Oceanography (METOC) Expert's toolbox. In addition to terrestrial weather conditions, these satellites also monitor solar activities, which may have impacts on military operations. Electronic circuits (both within and outside the atmosphere) may be affected, and this could have a negative impact on communications, navigation accuracy, and ISR sensor capability.

Space Situational Awareness

Space Situational Awareness (SSA) is the creation of an extensive operational picture to monitor all activities in Space, including debris tracking, for operational situational awareness. This encompasses mainly threat warning and assessment, re-entry-warnings as well as the protection of satellites by avoiding collisions through the performance of manoeuvres. Overflight prediction of adversary satellites in order to provide warning to friendly forces is also an element of SSA. In short, SSA is the up-to-date awareness of what Space-faring actors are performing in, through and from Space.

Satellite Communications

Transmission of data (texts, words, videos, etc.) via satellite is possible from any point in the world to another, with some limitations in extreme northern or southern polar areas due to the commonly used GEO orbit. To cover the extreme northern or southern polar areas satellite constellations in LEO or HEO are required. This provides very flexible and secure wireless communications, especially in deployed operations and/or in areas with limited infrastructure. Satellite Communications (SATCOM) utilizes various frequency bands, each with distinct advantages and disadvantages, and some bands which are protected communication lines. SATCOM is primarily used for Command, Control and Communication (C3) purposes, and it is irreplaceable for UAS Beyond Line of Sight (BLOS) operations. SATCOM limitations may vary and are caused by limited capacity, size of antenna, available power, latency, and weather.

Shared Early Warning

Shared Early Warning (SEW) is NATO's and allies use of US provided data related to early warning of imminent missile attacks.

This is a passive part of Force Protection for friendly forces as well as NATO territory and civilian populations and similar capabilities can be expected from any other Space-faring nation.

In addition to these six capabilities, others include Space Launch and Space Operations. However, due to the fact that NATO does not own or operate any space-based resources other than some ground equipment related to satellite communications services, these are not further defined within NATO.

UAS Need for Space Support

Today, there is an enormous variety of UAS, offering different applications and tasks from simple toys to complex military systems. The dependence of these myriad individual UAS on Space-based DPS also varies greatly.

SATCOM is an essential part of all BLOS UAS operations and COTS UAS also utilize PNT signals provided by respective satellite constellations. SATCOM and PNT are the most important Space capabilities required for UAS operations and therefore are the focus of further analysis in this chapter.

Satellite Communication

Different types of UAS use different types of communications for operating the vehicle and for managing the vehicle's payload. UAS operating BLOS are absolutely dependent on SATCOM; primarily GEO satellite networks for near real time control.

Even UAS operating in an automated and pre-programmed mode of flight require the ability to send additional navigation commands to

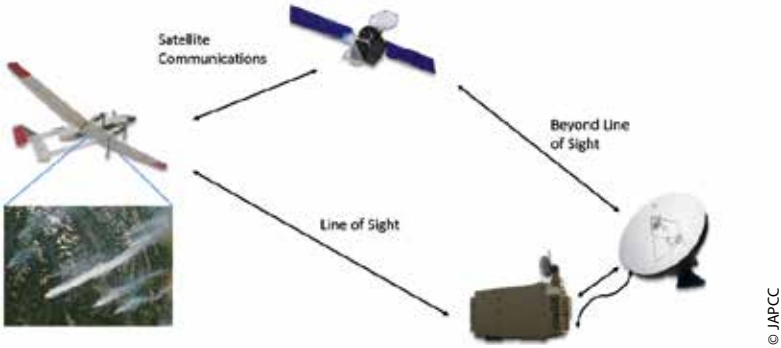


Figure 12.1: UAS using Satellite Communications.

the air vehicle, typically in cases of mission change, and sometimes these changes are necessary on a short notice. Therefore permanent, real-time, low latency and stable Lines of Communication (LoC) are a must. In addition to the primary LoC, alternate, contingency and emergency lines should be planned for and available for critical missions. It should also be understood that these commands generally require less data and lower bandwidth than the payload. At the same time, system status of the UAS must be transmitted to the ground station, and this also calls for stable lines with a low throughput.

In addition to the Unmanned Aircraft (UA) itself, the use of the respective mission relevant payload also requires dedicated LoC. Besides the uplink of mission commands to the payload, it may be possible to downlink data collected by the payload. The capabilities of certain UAS creates opportunities and a few challenges.

Today's more advanced and complex sensor payloads generate an ongoing growth of sensor data with an intense demand for storage capacity for high resolution pictures (EO, IR, and SAR) and in some cases video streaming. The transmission of this data from many

UA via SATCOM to their ground control stations can cause challenges to the system due to limited throughput capabilities of some SATCOM systems.

To compensate for the bandwidth limitations, data and video are often compressed, however this can result in the loss of data, depending on the techniques utilized.

Complex UAS missions, which are dependent on SATCOM, require planning with a mind-set on the communications path of the signals involved. Some of which may result in mission limitations that might affect dynamic asset re-allocation during mission execution, in turn requiring alternative solutions.

Information collected by the ISR payloads of an UAS are often time-sensitive and must be distributed across multiple military organizations, requiring each element of the LoC to be optimized to prevent a delay in data dissemination.

Currently, the main concentration of communication satellites is in the GEO belt. Research on current trends indicates in the near future we will see an increasing number of communication satellites stationed in lower orbits such as LEO or MEO which are known as 'Mega-Constellations' of up to several hundred satellites. They will provide a higher capacity of dataflow, the so called 'virtual fibre', almost anywhere around the world with less limitations than experienced today. This will offer additional primary LoC for UAS operations, as well as alternatives. Besides the developments of NATO member nations, there are also projects declared by potential opponents. China has two militarily usable systems that are currently in their technical test phase prior to their deployment. The 'HONGYAN' constellation[5] has one test satellite in orbit and is to be planned at Full Operational Capability (FOC) in 2023. The

'XINGYUN' constellation[6] has deployed two satellites already and is planned to be FOC in 2025. Both constellations offer frequencies that are usable for the operational control of UAS or for the sensor download-feed. Both of these constellations are operated by state-owned companies. Russia has also planned to enter this arena with the 'SPHERA' constellation[7] a more complex system which also includes payloads other than communications. This constellation will be operated by the Russian Space Agency ROSCOSMOS. The first launch is planned for 2022 and FOC for 2028. It is very likely that the projected operational timeframes for these systems may be delayed due to several reasons. It is also very likely that due to the fact that these systems are state-owned and operated, these systems will not be cancelled due to financial problems.

Positioning, Navigation and Timing

PNT services are a substantial requirement for many types of UAS, based on their individual mission sets; even for most Class I UAS and consumer drones. This is evident for the UA itself, but this applies also for specific payloads.

If an UAS is operating in automated mode, PNT information is vital for flying the pre-planned route, as well as alternate routes or course-corrections. Likewise, if an UAS is being controlled remotely, the transmission of accurate position reports to the control element is essential for the location information and also for the timing signal shared between the ground and air segments of the UAS as they communicate via SATCOM.

For some kinds of payloads, like the employment of Precision-Guided Munitions (PGM), actual PNT-data is indispensable. ISR data collected by a variety of on-board sensors also requires an exact georeference for subsequent analysis and further operational use.

Space Weather and Potential Impact on UAS

In addition to atmospheric influences like clouds, heavy rain, smoke, reflections or industrial pollution, Space weather may have an impact on UAS operations.

Solar activity may result in charged particles, cosmic rays, geomagnetic storms, or solar flares, which may have an impact in various zones above the earth, through increased ionisation, higher radiation levels or signal interferences. These will result in outages in PNT and SATCOM services, which may impact an UAS indirectly, but especially UA operating at (very) high altitudes could be additionally impacted directly with the malfunction of internal power grids, digital chips or avionics.

Cases of extreme solar activities can reach into the earth's atmosphere, which can hamper electronic devices in the ground installations and user segments of Space systems. These impacts are also potentially felt in UAS control elements, and can, to some degree, also include the LOS and BLOS data links.

Possibilities for Countermeasures Against Adversary Space Assets in Support of UAS

As discussed earlier, a complex Space system consists of four segments, which are interconnected. To interrupt the services of the whole system only one segment needs to be affected, which can be done by several types of counter-Space weapons:

Physical attacks destroy or damage Space- or ground-based Space assets through the use of systems like direct-ascent anti-satellite missiles, co-orbital anti-satellite vehicles or by attacking the

ground station through various means, such as offensive counter air operations as outlined in Chapter 8 (cf. p. 136 f.).

Non-physical attacks target the means of transmission by interfering with the various signals comprising the link segment. This can be done by jamming or spoofing and is usually temporary in duration.[8] Chapter 10 (cf. p. 177 ff.) discusses these types of attacks in more detail.

If a single UAS mission is dependent on SATCOM Services and/or PNT Data, any effective attack against one segment of the Space-System leads to a failure of the complete Space service which consequently has an impact on the success and the flexibility of the UAS mission. However, if the UAS C2 link experiences interference, that does not automatically equate to UAS mission failure. The UAS might be able to complete its mission, but without receiving new instructions during the sortie.

Besides physically engaging the UA itself with Air Defence, or the Space-, Ground-, or User-Segment of the Space-System, non-physical attacks against the link segment provide another option to adversaries:

Jamming. Intentional interference of the link by generating a separate but stronger signal in the same radio frequency as the original system. This prevents receivers from distinguishing between the false signal and the real signal, and therefore prevents the system from processing the authentic signal and the relevant mission information it contains.

Spoofing. A more sophisticated form of jamming is imitating an authentic signal to force a receiver to process false data, which the end-user believes is real data.

Positioning, Navigation and Timing

Interfering with PNT signals requires merely some generally low-cost GPS jamming devices.[9] These devices have to be located within a specific range of the GPS receivers they wish to affect. As the antennas of GPS receivers are generally omnidirectional, many avenues of attack are open for jammers on the ground or in the air. Additionally, the signal strength of any GNSS is extremely low power and therefore also vulnerable to unintentional interference.

Furthermore, jamming of GNSS also has an effect on the timing information provided by the signal; which may disrupt the link synchronisation.

Spoofing the GNSS signal may result in the UA flying far from its pre-planned flight path, without giving alarms, or even may cause the UA to crash. Forcing a consumer drone to land due to spoofing the PNT signal has already been successfully tested and it is technically possible that this method could also be used for larger military systems.[10] However, this technique calls for sophisticated technology to create falsified signals to impact the UAS, especially for military-grade signals which are typically encrypted.

Satellite Communications

For communications purposes, specific military satellites provide secure and protected radio frequency signals against jamming threats. If these secure lines are not available for the armed forces, generally non-protected governmental or commercial satellites have to be used; and these signals are normally easier to attack. There are jamming techniques which have been developed to disrupt communications signals in various bands located on mobile, fixed and naval systems.

Uplink jamming prevents the satellite transponder from differentiating the jamming signal and the original signal. To be effective, the jammer must be located within the field of view of the antenna on the satellite.

Downlink jamming disrupts the signals traveling from the satellite to the receiver. To be effective, this jammer must be within the vicinity of the receiving antenna. This type of jammer does not need to produce a very strong signal, because it only needs to be powerful enough to disrupt the reception of the signal at the ground or user node.

Due to the various characteristics of individual UAS, the impact of ground-based SATCOM jammers varies. For downlink jamming to be effective, the jammer most likely has to be in a position between the satellite and the antenna of the UAS. So, for high-altitude UA only Space-based or air-based jammers have a possibility to jam the SATCOM downlink.

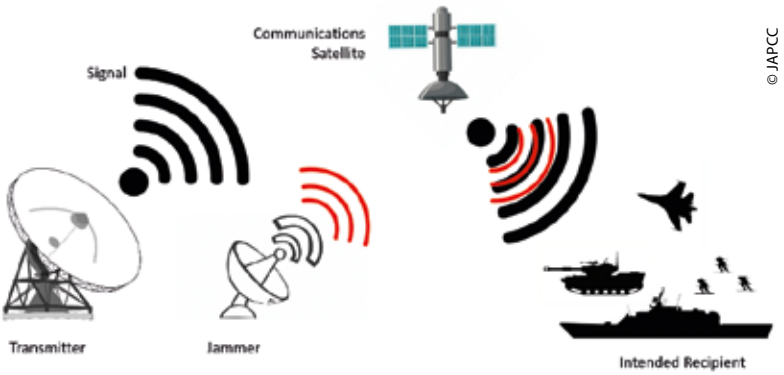


Figure 12.2: Uplink Jamming.

SATCOM jamming is relatively inexpensive and the technology is commercially available and therefore it is not the exclusive purview of state actors. However, jamming an UA is more challenging due to the altitude, speed, range, and on-board protective measures of UA, and therefore requires more advanced technical solutions.

Other Aspects

The intentional interference of a link node is an effective means to disrupt UAS missions with generally temporary effects, which are difficult to attribute to a specific aggressor. Sometimes such an attack is not even detected, other than a mission was not successful.

These kinds of intrusion are elements of Electronic Warfare; basic information and specific aspects of which are described in Chapter 10 (cf. p. 177 ff.).

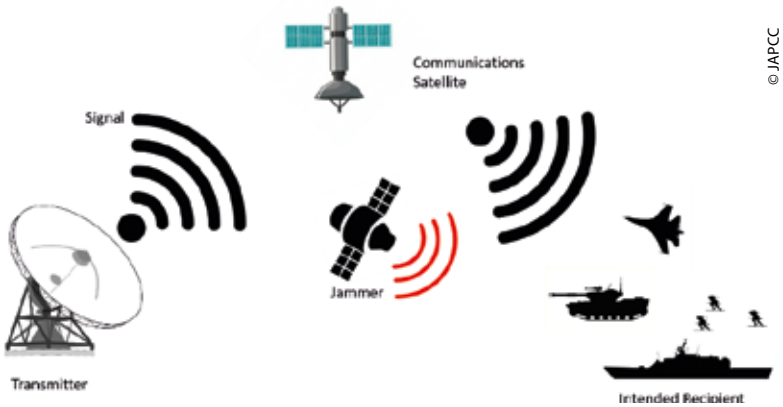


Figure 12.3: Downlink Jamming.

Space-based services also offer potential avenues for cyber-attacks.[11] SATCOM ground terminals and control centres are usually connected via computer networks which can be exploited or disrupted. Chapter 11 (cf. p. 183 ff.) discusses cyber means which are directed against UAS components in more detail.

Conclusion

Various UAS need specific services provided by Space capabilities. The needs are dependent on class, size, level of autonomy, and the specifics of the operation or mission. In close cooperation with actual Space-based DPS, UAS are able to exploit their inherent advantages. The current and future dynamic development in many Space-based areas, such as mega constellations of small satellites in LEO, will provide further possibilities for the operation of UAS.

However, UA are not invulnerable. In the realm of Space-based DPS for UAS operations there is a vulnerability to the impacts of counter-SATCOM and PNT services. The guarantee of PNT and SATCOM services is vital for the success of UAS operations. Denied or degraded Space support will significantly hinder UAS operations.

In order to prevent or influence the success of adversary UAS, appropriate offensive measures must be initiated, which could hamper PNT and SATCOM Services. These measures can target parts of the supporting Space system as well as directly the UAS. Detailed knowledge of the frequencies and procedures used is required in both cases, and in particular to provide the means and awareness to place the countermeasures in the position that makes success most likely.

Endnotes

1. NATO declared Space as an own Operational Domain at the NATO Summit, 3-4 Dec. 2019 in London, UK. NATO, 'London Declaration', Press Release (2019) 115, 4 Dec. 2019. [Online]. Available: https://www.nato.int/cps/en/natohq/official_texts_171584.htm. [Accessed 1 Apr. 2020].
2. NATO Bi-Strategic Commands, NATO Space Handbook, Guide to Space Support in NATO Operations, (NU), Aug. 2017.
3. Due to the declaration of Space as an Operational Domain in NATO this structure is under discussion and object for new formalities.
4. 'BEIDOU Navigation Satellite System', 3 Aug. 2020. [Online]. Available: http://en.beidou.gov.cn/WHATSNEWS/202008/t20200803_21013.html. [Accessed 23 Nov. 2020].
5. HONGYAN will consist of 320+ satellites in LEO and is operated by the state owned CASC (China Aerospace Science and Technology Corporation). The military relevance is highly likely; cf. www.newspace.im.
6. XINGYUN will consist of 156+ satellites in LEO and is operated by the state owned CASIC (China Aerospace Science and Industry Corporation). The military relevance is technically given and likely; cf. www.newspace.im.
7. SPHERA will consist of 640+ satellites in LEO and is operated by the state owned agency ROSCOSMOS. The military relevance is highly likely; cf. www.newspace.im and www.globalsecurity.org.
8. Todd Harrison, Kaitlyn Johnson, and Thomas G. Roberts, 'Space Threat Assessment 2019', Center for Strategic & International Studies (CSIS), 4 Apr. 2019. [Online]. Available: https://www.csis.org/analysis/space-threat-assessment-2019. [Accessed 1 Apr. 2020].
9. In line with the widespread use of PNT systems based on GPS services worldwide, there is also a huge activity in the development of corresponding jammers; leading to large offers at low cost.
10. Melissa Mixon, 'Todd Humphreys' Research Team Demonstrates First Successful GPS Spoofing of UAV', The University of Texas at Austin, 28 Jun. 2012. [Online]. Available: https://www.ae.utexas.edu/news/todd-humphreys-research-team-demonstrates-first-successful-uav-spoofing. [Accessed 1 Apr. 2020].
11. Ibid. 6, 7.

13

By Wing Commander (ret.) Jez Parkinson, UK AF
Joint Air Power Competence Centre

Force Protection Considerations

Introduction

Overview

The subject of Counter-Unmanned Aircraft Systems (C-UAS) has become what can best be described as a 'hot-topic' not just for NATO, but globally. From a Force Protection (FP) perspective, it is offered, the primary question to explore is whether this challenge is new and unique or just one of many threats that NATO faces? As such, can it at least be partially addressed with some intellectual effort, adaptation of existing Counter-Threat methodologies and the use of existing technology, perhaps in a novel[i] way?

[i] Using technology or equipment designed for one task for a different, unintended task.

Abstract

The current perception that UAS are a 'new' threat that requires a bespoke approach should be challenged; who is driving current thinking and why? Are UAS actually something different or, are they just the logical employment by our adversaries of increasingly accessible technology? Current FP Policy, Doctrine and Directives remain fit-for-purpose, as do the FP Estimate and FP Planning processes; all that is required is the inclusion of UAS as another one of many considerations. With the application of intellectual effort to better understand the threat in all its constituent parts, it is offered that it will be realised that existing practices, procedures and technology can be employed to counter most, if not all aspects of the UAS threat. Furthermore, there are 'multiple defeat vectors' and not unlike C-IED thinking, the UAS platform (or 'drone') is but one part of a system-of-systems, all aspects of which have the potential to be neutralised (e.g. the platform, the operator and the broader adversary network can all be targeted either individually or simultaneously). There is undoubtedly a role for the use of new or emerging technologies, but this requires careful consideration mainly because each new technology comes with an inherent training and maintenance burden. The challenge today is not the lack of capability, but the inability to actually employ it. In a crisis situation, with the necessary legal framework in place as a result of robust planning, forces should have the necessary space to manoeuvre and the freedom to act. However, this is not the case for the protection of the Homebase in peacetime. There is a compelling argument that the operation of UAS needs to be better regulated. However, the question of why there is apparent resistance to this approach needs to be further examined, particularly the role of the media. The FP Practitioner when considering perceived new threats, must not lose sight of existing, accepted threats. Finally, to successfully neu-

tralise any UAS threat will require inter-agency co-operation; what might be described in NATO vocabulary as 'a Comprehensive Approach'.

Boundaries

Actors

This issue is not only a challenge for the Air Component; the UAS threat can affect any or all Components. Furthermore, UAS can either be remotely operated or autonomous (i.e. once launched, the vehicle functions without further input from an operator). This said, even autonomous platforms will have a human within the system at some point (e.g. launch and possible recovery). Also, the level of autonomy of any platform will be a function of the level of technology available and the ingenuity of the operator to use even simple technology to best effect.

Focus

The focus of this Section is the conceptual *(Force Protection)* challenge of C-UAS at the Operational Level. It will not provide doctrinal guidance, specific recommendations on Tactics, Techniques and Procedures (TTPs) or, recommend specific equipment that can be employed at the Tactical Level. It is acknowledged that platform capability (payload, speed, detectability, range, level of autonomy, responsiveness, etc.) is variable and in some cases inter-related and these factors will no doubt be considered by our adversaries when 'attack' planning. Technology will continue to develop and the intelligent adversary will always seek to exploit technology to their advantage, therefore, our own thinking needs to remain ahead of that of our adversaries when and wherever possible.

Objective

To provide a baseline for thinking across a broad customer base. This study offers a foundation for the delivery of capability and as a result, attempt to capture and subsequently shape thinking across as many of the NATO Capability Development, Lines of Development (LoD)[ii] as possible. While the reader may perceive that this thinking is air-centric, the principles offered are applicable to all components.

Approach

Recognizing that it is not just UAS that present challenges to the FP practitioner, but Unmanned Systems in all domains, this Section will focus on Air Systems. Countering contemporary threats, to include but not limited to UAS, will require both a Comprehensive and Multi-Domain approach. This Section does not seek to describe the nature of NATO's Comprehensive approach to operations nor the complex issue that is the emerging concept of Multi-Domain operations. However, what is offered, is that countering UAS will require a multi-agency approach *(so not just the military)* and, irrespective of where a threat system is operating, all agencies will be required to cooperate and will likely need to operate in more than one domain simultaneously. The age-old problem of information sharing will no doubt persist, but to create effective C-UAS strategies, inter-agency and inter-state cooperation will be necessary. This factor should lead directly to a significant conclusion - that the Command, Control and Synchronisation (and/or deconfliction) of FP activities, as well as the ability to communicate effectively, often rapidly, across many involved parties, remains an essential

[ii] Doctrine, Organisation, Training, Materiel, Leadership, Personnel, Facilities and Interoperability (DOTMLPFI).

enabling capability for effective and resource efficient provision of FP effects, to include the neutralisation of the UAS threat.

Overarching Considerations

Requirement Drivers

This Section does not seek to explore in detail what drives NATO's capability requirements. What is worthy of consideration though is 'who' can drive the capability requirement? This subtlety is raised because it should be understood that there can be perceived benefit to the individual(s) who brings a challenge to the forefront. This perceived benefit can take the form of kudos, advancement in rank or shaping a future employment opportunity. These individuals are often described as 'Thought Leaders'. The second 'who' is perhaps more obvious – industry. Industry benefits from being able to develop and manufacture solutions that meet identified capability requirements. Having described C-UAS above as a 'hot-topic', careful consideration needs to be given to who is driving the apparent problem set and for what purpose?

New Threats – New Countermeasures

As an extension of the above, the identification *(or perception)* of a new threat should not immediately mean that entirely new countermeasures will be needed, as much as perhaps industry would like this to be the case. It will often be the case that existing equipment, processes and practices can be adapted to counter the 'new' threat. Equally, even if a new capability requirement is identified, it will take time to deliver and therefore, adapting what is currently available will always be necessary in the short to medium term. A key component to countering any threat has to be the intellectual rigour

that is applied to properly understanding that threat in the first place and then how it might subsequently evolve over time and space.

Measures of Effectiveness

A challenge that plagues the FP Practitioner is that of Measures of Effectiveness (MoE). In its simplest form, has a particular FP Measure or indeed an entire FP Posture been effective? Has the adversary been deterred or, simply chosen not to attack? Equally, over the last 20+ years, the inclination has developed that any attack must owe its occurrence, at least in part, to a failure in FP.

Reality Check

Following from the above, the reality of the contemporary operating environment is such that it is inevitable that adversaries will, on occasion, be successful. These apparent successes when considered after the fact, could well be deemed to have been preventable. However, with the level of understanding available prior to the event, FP measures could still be considered appropriate. The current threat paradigm, to include UAS, requires the application of tried and tested FP measures, the subtle adaptation of these measures and where necessary, the development of new approaches. The increasing capability of platforms, their enormous cost and their declining numbers means that the loss of such assets (including their operators, maintainers and supporting structures) would inflict real harm on a nation or indeed the Alliance. In turn, this means that they present an emerging vulnerability which an adversary will undoubtedly seek to exploit. For the FP Practitioner, arguing for a return to 'old' concepts such as dispersal, concealment and hardening will be necessary. Equally, the availability of resources debate cannot be ignored. This should take two distinct forms. Firstly, the requirement for robust FP forces. Second, the

need to have sufficient resources, particularly in terms of enablers to allow the capability to be operated in a warfighting manner rather than in a manner directed by 'just-in-time' logistics or engineering expediency. Clearly, a balance is required, but the current lack of attention to the FP of high-value, low-density and yet incredibly fragile assets is concerning.

Operational Context

Geographic Location

The location of assets to be protected is important from a C-UAS standpoint. C-UAS activity at the tactical level, will necessarily be driven by the location of the asset to be protected. Hence, if the FP Practitioner is included during planning, they can influence the selection of the optimal location, which will help in simplifying the C-UAS task. Furthermore, in addressing the concept that the UAS should be treated as just another threat system, many of the factors that simplify the C-UAS task will also simplify broader counter-threat activity. As an example, complex, densely populated urban terrain in close proximity to the operating location provides a far greater FP challenge than does a sparsely populated, open agricultural landscape.

Homebase versus Deployed Operations

The Freedom of Action (FoA) allowed for the military FP community for the protection of the Homebase in peacetime is likely to be limited. It is often the case that they are not permitted to operate outside of the perimeter and any activity will be confined to responding only once a threat has been detected. In addition, any response is likely to be extremely limited due to legal considerations. In the case of deployed operations, the possibility to

influence the selection of the operating location exists. Furthermore, the challenges of legal inflexibility at the Homebase may be overcome, at least to some extent, through early and robust engagement in the process that develops Status of Forces Agreements, Technical Agreements, Memoranda of Understanding, Rules of Engagement, etc. Perhaps a way to visualise this area is as a sliding-scale where friendly forces FoA to C-UAS increases as adversary action increases and the constraints on FoA are reduced, because the operating environment is becoming less permissive.

C-UAS in Free Space

There are many potential constraints on the ability of the FP Practitioner to counter the threat from UAS. However, if a hypothetical scenario were created where none of the real-world constraints were present, it is likely that it could quickly be identified that the challenge is not the ability of FP to defeat UAS, but rather, the externally imposed constraints on FP that create the difficulty *(not to say that constraints imposed are not in place for entirely valid reasons)*. By first thinking of how best to C-UAS without any externally imposed constraints, a spectrum of capabilities emerges that would undoubtedly mitigate against the majority of the threats. However, a perhaps unpalatable aspect of this discussion is to acknowledge, from the outset, that there are situations where an adversary will be successful. Equally, there can be no reference manual that will provide a written guide to C-UAS in all circumstances; documentation (Doctrine) can only provide a guide or hand-rail. That said, by considering how each of the 'Force Protection Functional Competencies'[iii] or 'Elements of Air Force Protection'[iv] can be employed in C-UAS, a significant number of

[iii] AJP-3.14, Allied Joint Doctrine for Force Protection.

[iv] ATP-3.3.6, NATO Force Protection Doctrine for Air Operations.

options emerge, many of which require neither legal authority to employ nor substantial additional resources. This includes but is not limited to, use of cover, dispersal and concealment. Other more active and/or kinetic options also exist, if permitted. The key take-away here is that effective and resource efficient C-UAS activity has two primary drivers. First, the ability of the FP Practitioner to employ existing capability in an emerging role. Second, understanding the Operating Environment, particularly its constraints, to identify what measures could be employed, if permitted. It is then a case for the Chain of Command to work to either remove those constraints, accept the risk or, to terminate the at-risk activity.

Threat

Understanding Threat

Broad statements that a threat exists are often made. For a threat to exist any adversary has to have both a capability and the intent to use that capability. However, above this sits the fundamental question of what is it that an adversary is actually seeking to achieve (what, why, when, where, how, etc.)? By gaining an understanding of the answers to these questions, the FP Practitioner can start to identify how any threat or, threat system, can be defeated.

Threat Actors

Like the range of possible systems available to an adversary, the range of adversaries is also considerable. Any individual using a UAS can cause a major incident, intentionally or otherwise. The naiveté of the general public in relation to matters of security and safety should never be underestimated. The spectrum of 'Threat Actors' covers the range from lone actor misuse, right

through to deliberate state use. However, irrespective of who might be employing a system deemed to be a threat, many if not all of the available countermeasures can be employed. As already mentioned, the primary limiting factor will usually be the legal framework within which any FP/Security force is required to operate. Note that it is likely that in the case of any deliberate, nefarious use of UAS, the system user will likely be aware of the legal framework in-place, but will simply ignore it. Of significance, is a potential adversary's ability to access and subsequently use technology.

Threat Origin

Understanding the origins of any threat system provides both insight into the possible scale of the threat and how it might be defeated (i.e. if you know where something comes from, then its supply can be interdicted). Also, the more technologically advanced and hence potentially more capable a system is, the greater the likelihood is that it will pose a substantive threat. The more complex a system, the higher the possible cost. Equally, the more complex a system, the higher the intellect of the adversary will need to be in order to use it effectively. These aspects of understanding the adversary and/or their systems could facilitate the targeting of likely individuals and possible operating locations associated with these systems. Understanding and where possible, exploiting the technology that is being used against us, will help guide thinking on both, what priority countering the threat needs to be given (in comparison to other threats) as well as providing an insight into who is operating it. Ultimately, if UAS are viewed as just another threat, understanding important elements of its operations like: where it comes from, who is using it, for what purpose, how it is being operated (adversary TTPs), etc. will all be significant pieces of information to assist friendly forces in neutralising the threat.

Unsurprisingly, the conclusion can be drawn that intelligence will play a vital part in any ability to C-UAS.

Threat Systems

NATO has created a taxonomy for UAS (cf. Annex A, p. 510 f.). It is offered that the primary challenge comes from systems at the lower-end of the spectrum, as these are both harder to detect and (if authorised) engage. When considering the threat, it is perhaps worth noting that the Indirect Fire (IDF) threat from the ubiquitous 107 mm rocket, familiar to many FP Practitioners, was from a projectile that weighed 18.84 kg (41.5 lbs); similar to the weight of an Unmanned System at the lower-end of the 'Small' category (20 kg). Likewise, the 122 mm rocket weighs-in at 66.6 kg (147 lbs). In other words, even in the 'Small' Category UAS have characteristics that existing technology can detect, track and if necessary/authorised engage. Therefore, the challenge exists primarily across the 'Nano' to 'Mini Categories[v] where further useful deductions can be made:

Proximity. The UAS threat of specific concern to the FP Practitioner is likely to originate within the NATO assets Tactical Area of Responsibility (TAOR)[vi] (e.g. the operator and the system will be present in the TAOR).

Operating Height. Operating altitudes will fall within the surface to 3,000 ft range for UAS. At the lower-end of this spectrum, terrain or infrastructure will present an operating challenge whilst the higher a UAS flies, the more readily it will 'unmask' to detection systems (i.e. they will not be able to hide amongst ground clutter).

[v] Notwithstanding that a small charge can have a large effect particularly if it can be delivered 'surgically' and/or with additional kinetic force and/or against a particularly vulnerable/fragile target.

[vi] See AJP-3.14, Allied Joint Doctrine for Force Protection.

Position. Understanding how any threat system functions and its potential use(s) will translate into how it needs to be operated. By understanding how a system must be used, will lead to the identification of locations that it can be employed from[vii]. These locations can then be prioritised for denial.

Endurance/Range. Smaller UAS will have limited endurance, however, increased endurance can be achieved, but often at the expense of reduced payload (and vice-versa).

Payload. Traditionally, smaller UAS have limited payloads. Remaining with the IDF analogy, an 18.84 kg (41.5 lbs) 107 mm rocket only carried a warhead of 1.7 kg (2.9 lbs) (see 'Weapon Effects' below). Similarly, the ability of platforms to carry a sizeable payload will decrease, as the size of the system decreases. The deduction from this is that an intelligent adversary will most likely use smaller UAS primarily as intelligence gathering assets, although in reality, the potential use of any platform is only limited by an adversary's imagination and subsequent access to the necessary technology.

Effects. The matter of 'payload' (above) should remain a separate consideration from 'effect'. Specifically, a small system with limited payload could still have a significant effect, if deployed against the likes of an unprotected 5th generation platform. Equally, the perception that an UAS could be deployed by an adversary as a means of delivering a Chemical, Biological or Radiological (CBR) payload could have a huge non-kinetic (psychological) impact. This effect will be irrespective of the technical feasibility and/or actual effects of any such weapon; *a Weapon of Mass Effect rather than a Weapon of Mass Destruction.*

[vii] It is acknowledged that data from an UAS could be transmitted via some form of link to a remote operator, however, this adds complexity which could in turn be exploited in order to detect and ultimately counter the threat.

- Kinetic. Linked to 'Payload', there needs to be a basic understanding of weapons effects. Most of the use of weaponised UAS by Islamic State of Iraq and the Levant (ISIS) consisted of dropping low-payload projectiles similar in size to a hand grenade. While adversaries have become adept at increasing the effectiveness of their IEDs through the addition of shrapnel (e.g. ball bearings), the ability to add shrapnel (because of weight) on an air-vehicle is significantly reduced.

Vignette

A 2016 video clip aired on many major news outlets showed an Iraqi Army tank being attacked by an ISIS weaponised UAS. It is offered that this was a lucky strike where the weapon fell inside the vehicle but, importantly, the vehicle in question was operating in an urban environment and the crew should have been operating closed-down in order to prevent a hand grenade, Improvised Explosive Device (IED) or even a cruder 'Molotov Cocktail' (fire bomb) being used on the vehicle from above. Therefore, whilst the weapon that destroyed the vehicle was dropped from a UAS, it could have come from multiple other sources. The actual cause of the event was poor crew discipline resulting in a failure to implement basic TTPs for operating armoured vehicles in close terrain. Sensationalist reporting followed by multiple rebroadcasts with increasingly ill-informed comments together with a subsequent failure to properly analyze the cause and effect have led to false conclusions being drawn. Had the weapon (improvised or otherwise) not fallen through an open vehicle hatch, the effects would have been negligible as distance from any blast and shielding be it in the form of armour or infrastructure, reduces blast effects.

- Non-Kinetic. The presence or potential presence in the battlespace of UAS will have an effect, irrespective of whether any system is actually weaponised. It should also not be discounted that kinetic effects can have an associated non-kinetic effect, e.g. on the morale of personnel.

Larger System – Basic Considerations

As a system increases in size, it can be considered to also be increasing in capability. It will have greater range, longer endurance, be more robust and able to carry a greater payload. From the adversary perspective, this might be considered a positive. Although, obtaining a larger, more capable system comes with its own logistical challenges which could, in turn lead to a greater 'footprint' that could be of intelligence value to friendly forces. However, for the FP Practitioner, a larger system in use will also be more likely to be detected and engaged.

Autonomy

UAS can be remotely-operated, fully pre-programmed or have the ability to self-navigate having first been given navigational waypoints. Whilst full autonomy is possible, for the FP Practitioner the fact remains that, if an UAS threat exists, it has at least two tangible and therefore targetable elements; first is the vehicle itself and second, the user.[viii] Much has been made of the potential future use of Artificial Intelligence (AI) and whilst the marrying of AI with UAS adds yet further complexity, the fact remains that there are still identifiable and subsequently targetable elements within the system.

[viii] In the case of an apparently autonomous system, the link between operator and system as a targetable element might be absent, but what would be the ends of that link i.e. the system 'owner' and the vehicle itself, remain tangible, targetable entities.

Swarming

A potential adversary tactic that requires specific consideration with respect to adversary use of UAS is that of the use of so-called 'swarms'. The attacks on Russian Military facilities in Syria, widely reported in December 2017 and January 2018, highlighted this tactic. Whilst this alleged employment of multiple systems could be used as an argument to advance the perspective that 'new' threats evolve quickly both in quantity and possibly quality, an alternative narrative could be advanced. Firstly, and specific to the example above, the ability to confirm the validity of reports in the media is limited in the unclassified domain. Second, and of more importance to the FP Practitioner, what element of a so-called swarm attack should cause consternation? The reality is that any threat can present itself at a scale that will be difficult to defeat (e.g. an attack by a significant number of adversary personnel supported by sustained mortar fire). Timely and accurate analysis of the threat should lead to both the correct FP resources and the quantity of each resource being identified.

Adversary Developments

In developing approaches to mitigate a threat, thought should always be given to how that threat may evolve. If this approach is ignored, it is likely that an intelligent and adaptable adversary will quickly render any counter-measure impotent. As stated elsewhere, consideration also needs to be given to the concept of second order effects and/or unintended consequences. What other effects could a counter-measure have (e.g. interference with other electronic systems). The C-IED fight provides a valuable lesson in this respect, where the deployment of supposedly improved protected mobility only drove the adversary to produce larger and more devastating IEDs. Key aspects for consideration by the FP

Planner are: what will be the impact of effectively neutralising or even defeating a particular threat? What will the adversary conceive next and could it be either more difficult to counter or indeed more effective? An often-overlooked approach is to tolerate or accept one threat, in order to delay or prevent an alternatively more dangerous one from materialising.

User Groups

Uneducated Use of Unmanned Systems

Particularly in the case of the Homebase, not all UAS encountered will be used with nefarious intent. An aspect that has received little attention is the general ignorance of the populace at large to the risks to flight safety posed by unthinking use of UAS in the proximity of air operations, both military and civilian. This is compounded by the growing belief amongst many that it is their right to know everything that in turn, leads a few to believe that they have a right to use UAS to gain insight into what 'the state' and in this case the military, might be doing 'inside the wire'.[ix]

Media

The reason that media use of UAS has been considered as a standalone issue is because this particular area could be problematic for the military. Whilst legal matters are discussed elsewhere, media use of an UAS, even if deemed illegal, is still likely to be described (by the media themselves) as being in the public interest. Furthermore, the information or footage gained during such use is likely to

[ix] Note that some effective measures are already in place to mitigate the risk of uneducated use of unmanned systems (e.g. Geofencing).

be widely broadcast and could, depending on the media outlet, come with a degree of apparent legitimacy.[x] The FP response to any detected use of an UAS in the vicinity of any asset will need to be carefully considered in order to prevent any potential Strategic Communications 'own goal'. Also worthy of consideration is that in discussion with FP Practitioners, there is a perception that some nations are reluctant to use legislation to control UAS. Given the argument offered elsewhere in this Section that such legislation would be of general benefit, the question of who or what is generating this apparent resistance should be explored. Given that the media now routinely uses UAS and limiting their freedom of operation will greatly reduce their utility to the media, the question is, whether the media are responsible for shaping public perceptions and/or influencing political decision making regarding the use of UAS?

Other Legitimate Users

Beyond the media, there are multiple commercial users of a variety of UAS. These users will on the whole be responsible but, better understanding of where UAS are being employed now and where they are likely to be used in the future is required.

Friendly Forces Perspectives

Understanding is Key

The FP Practitioner must understand, in as much detail as possible, both what it is they are protecting and how it functions, as well as what the adversary is seeking to do (what, why, when, where, how, etc.) or more simply, the adversaries desired ends, ways and means.

[xi] Due to the outlets name and/or generally perceived reputation.

A Known Unknown

There is general consensus that unthinking and/or nefarious use of UAS is a problem that requires attention. However, a more worrying question that cascades from this is that if we believe we have a problem, based on what we are seeing, what proportion of the problem is going unseen or indeed unreported? For example, what materiel of intelligence value has been gathered using UAS, without the presence of that system being detected and hence, a lack of awareness of where compromises may already have occurred? Is the current perceived use of UAS, only the *'tip of the iceberg'*; how much UAS activity goes undetected and/or unreported?

Novel Application of Existing Technology

Again, there is an element of understanding required here. What existing technology is available or, which could be made available with little delay and be used to either detect or defeat an UAS? If the FP Practitioner understands how a piece of technology functions or, can consult with the appropriate Subject Matter Expert (SME), deploying technology in a role for which it was never intended should be considered.

No Single Solution

A phrase that was often used when NATO was seeking to respond to the growing use of IEDs by the Taliban was that there was no 'Silver Bullet'; no single approach or piece of equipment that would solve all aspects of the problem. Any solution to the UAS challenge is likely to have multiple facets and require the co-ordinated response of many actors/effectors. Equally, it is unlikely that a solution that works at one location or in one environment can be deployed ubiquitously. If multiple threats exist, each with

their own distinct operating parameters, it is likely that multiple counter-systems will be required. Similar approaches or processes may be applied, but a radar optimised to detect high and fast targets will struggle to detect low and slow targets and sensor performance should not be compromised by trying to cover too large a threat spectrum. If the threat, criticality of the asset and the appetite for risk drivers require it, a considerable range of sensors to include electro-optical, thermal, acoustic and seismic could be required to counter a range of threats. Similarly, if a variety of threat systems are to be effectively engaged, a range of weapons will be required.

Constraints

As with the majority of activities, there are likely to be constraints on what can be done; C-UAS activity is no different. Considerations will include, but will not be limited to electromagnetic spectrum management, jurisdiction, privacy, Rules of Engagement (ROE), geographic boundaries, areas of responsibility, etc. It is offered that the law, in many nations, is by far the biggest constraint, particularly when considering FP of the Homebase in 'peacetime'. It is not that the FP Practitioner is unable to protect against the UAS threat, it is that the means to detect and if necessary, neutralise a threat simply cannot be employed. Note that it remains vital when planning any activity to consider any negative or unintended consequences, such as the potential for collateral damage and negative publicity.

Deconfliction

Friendly Forces and a growing spectrum of other legitimate UAS users exist. From a FP Practitioner's perspective, moving forward will require broad engagement to ensure that other interested

parties are working to develop existing traffic management systems to incorporate new users. This may require the commitment of additional resources, but if this facet of the challenge is ignored, you risk issues of fratricide due to an inability to separate friendly forces and/or legitimate users from ill-advised or foolish and adversary use of UAS. An ability to understand and manage what is in the battlespace will be fundamental to managing risk.

A Proven Approach

General Considerations

While considering the threat of UAS, FP planners must also consider that other, as yet unidentified threats, will undoubtedly emerge in the future. Probably more importantly at this stage, existing threats will endure, re-emerge, evolve or be revitalised/reinvigorated. Consider, if NATO were to deploy a large number of personnel, particularly at short notice, into a high IED threat environment, would that force have institutionalised the lessons learned during combat operations in Afghanistan? The answer is probably not. In other words, we would have to re-learn previously hard-won lessons.

Modification of Existing Practices

Is it realistic to develop new approaches and possibly technology, for every new threat? The problem is that with every new approach comes a training requirement and every new piece of equipment brings a maintenance bill. Put simply, it is unrealistic to think that a bespoke *'golf club'* exists for every eventuality. The key will be the ability to adapt existing methodologies to developing threats through the application of intellectual rigour. Therefore, the FP

Practitioner should focus on maintaining proven, effective and sustainable counter-threat methodologies as captured in NATO FP doctrine, these include:

- Counter-Surface to Air Fire (C-SAFIRE) patrolling;
- Mortar Baseplate Checks;
- Vehicle Check Points (VCPs) within the Tactical Area of Responsibility (TAOR);
- Influence Patrols;
- Overt and Covert Observation Posts (OPs);
- Use of residual air capacity for FP purposes.[xi]

How can activity be modified or re-shaped to take into account the requirement for C-UAS? Examples here include, but are not limited to, conducting sweeps of the likely areas where UAS can be launched and/or operated from, similar to the way that Mortar Baseplate Checks are currently undertaken; if an adversary is building their own, modifying or weaponizing a commercial system, activity designed to identify possible workshops could be considered.[xii] Presence Patrols or Outreach Activity in an urban area can be considered to contribute, as a second order effect, to both any C-IED and/or Counter-Surface to Air Fire (C-SAFIRE) effort - one activity, multiple effects. Knowing what to look for and/or what questions to ask will enhance the ability to interdict any threat before it manifests itself. Other examples of applicable practices include considering an UAS in flight as an IDF threat or, an immobilised system on the surface as either a mine or IED.

[xi] Most NATO installations will have at least a helipad. Any aircraft with surplus fuel can be asked to conduct an overflight of an area(s) of interest in support of the overall FP effort.

[xii] For this to be a realistic option, it will be necessary to have an understanding of what UAS components look like and personnel will in turn, need to be trained in identifying such components. A simple example would be the presence of rotor-blade assemblies or remote-control devices.

Going Forward

When the threat from UAS is broken-down into its component parts as above, it becomes readily apparent that the threat (while clearly a challenge) is not what it may first seem. Proven FP techniques to include (but not limited to) hardening, dispersal, camouflage and concealment, deception and redundancy will all aide in threat mitigation. Equally, the domination of the TAOR around a NATO asset requires the ability to detect, deter, disrupt, neutralise or destroy the threat. The solution to this apparent conundrum lies in the ability of the FP Practitioner to accurately identify the type and scale of threat and subsequently articulate it; the vehicle for achieving this is the FP Estimate. If the analysis within the FP Estimate is robust, it should lead to the generation of the necessary assets to meet and ideally overmatch the threat. In addition, it will certainly provide a solid basis for the understanding of the risk(s) and subsequent Risk Management decisions.

Legal Considerations

Force Protection Perspectives

This is a highly specialized and critical area to consider and where there is no substitute for expert advice. A challenge for the FP Practitioner from the outset is that every location and every activity will have its own distinct legal parameters. In an operational environment where there is a recognised threat, and/or designated adversary, the constraints imposed on the conduct C-UAS activity are likely to be less. However, the real challenge exists in peacetime at the so-called 'Homebase'. In this latter scenario, the inescapable problem is that the FP Practitioner is unlikely to be able to counter the UAS threat in the majority of its manifestations, due to legal

constraints (e.g. the inability to apprehend the operator, the unwillingness of civilian law enforcement to respond or the inability to seize/impound systems). Compounding this dilemma is the current, apparent unwillingness to address these legal issues. It is offered that the ability to protect assets could be greatly simplified if there was a concerted effort to either address legal deficiencies or, apply existing legislation more widely and/or more robustly. Further discussion can be found in Part IV of this book (cf. p. 373 ff.) and also in the JAPCC White Paper entitled: *'The Implications for Force Protection Practitioners of Having to Counter Unmanned Systems – A Think-Piece'*.

Existing Capability

Current Doctrine

A suite of NATO FP documents exists and each contains a list of further reading. Whilst it is acknowledged that as these publications are reviewed, particular mention of UAS as a specific threat will be included, current documents *do* already provide a comprehensive spectrum of counter-threat methodologies than can be applied *now* to the challenge of C-UAS. The pillars of C-IED doctrine (Defeat the Device, Attack the Network and Train the Force) and much of how this is achieved is applicable to C-UAS activity.

The Human Dimension

Perhaps the NATO FP Practitioner's most effective weapon is the ability to analyze and subsequently understand a problem. Equally, it would be an error to consider any adversary as less intelligent than ourselves. Any threat will have a human in the system at some point. Even if an UAS is categorised as autonomous,

a human will still have to set that system in motion and will be expecting that system to produce some output or effect. The FP Practitioner needs to ensure that the correct weight of effort is afforded to the human dimension of the threat as this is ultimately where it is most likely to be comprehensively defeated. Conversely, over-focus on the UAS itself (in C-IED terms 'the device'), will likely lead to a more protracted campaign. At a very basic level, the reinvigoration of 'old' TTPs, such as the deployment of Sentries, will add to the ability to mitigate the threat.

Sensors

It was stated at the outset that this Section would not discuss specific equipment. However, it is probable that any sensor requirement will be bespoke to a specific threat or even to an individual location. In an operating environment with a range of threats, it is likely that a suite of sensors will be required with each sensor system looking at either a specific threat (e.g. Direct Fire), a specific environment (e.g. acoustic or seismic sensors against the sub-surface threat) or, just part of a wider threat spectrum (e.g. an Air Defence Radar specifically 'tuned' for the detection of small, low and slow air threats). For the Alliance, it must be assumed that in a 360-degree threat environment it is inescapable that a range of sensors will be required to detect a range of threats. The ability to fuse sensor data so that a reduced number of sensor operators is required is conceivable. However, the cost, maintainability and supportability of any such solution is questionable at this time.

Effectors

Many current sensors can be deployed with associated effectors as part of a system designed to counter existing, acknowledged

threat-types e.g. Counter-Rocket, Artillery and Mortar (CRAM) systems or Surface-Based Air Defence (SBAD). These systems have a range of effectors optimised for the threat that they are designed to counter. Like the sensors, these effectors may be capable of defeating the UAS threat or if necessary, a tailored system may have to be deployed. However, before considering effectors, the inescapable reality is that the ability to defeat an UAS has to be underpinned by the necessary ROE. There are three major considerations. First, simply, is the engagement of any UAS permitted? Second, in engaging a UAS that could be described as a 'small and fleeting target', if the weapon system in use misses the intended target, where will any effect be realised? Finally, if the UAS is successfully engaged, what will the effect be on both the location being apparently targeted by the system and also any area where the debris (to include a potentially still viable weapon) may fall?[xiii] Now assuming that engagement is permitted, industry is marketing a variety of C-UAS capabilities which utilise various novel technologies. It is offered that whilst these 'weapons' have some ability proven in testing, their long-term viability in the operational environment remains questionable. Also, new technologies will likely have an associated resource burden, even if it is limited only to training and maintenance. At a very basic, but nevertheless important level, the FP Practitioner may have to consider providing FP for any system and its operator(s) as they may not be able to self-protect whilst engaged in C-UAS activity. Introducing new, potentially unproven technologies into the battlespace requires careful consideration with particular attention being paid to second-order effects and unintended consequences.

[xiii] Recognising that this area could well be a civilian area outside the perimeter of an Alliance facility.

System-of-Systems Approach

As of now, the range of threats and hazards faced, drives the range of capability required. If multiple threats can be countered by a single system, this is an advantage. However, an important consideration should be that the system's performance is not compromised by expecting that one system can be equally as effective against all threats. It is offered that it would be better to deploy several systems, each optimised against a specific threat, rather than deploy a single system that is compromised in its ability to deal with any of the threats. With current technologies, it is most likely that a system-of-systems approach will be required.

Further Considerations

Jamming

GPS Jamming may be considered as a tool against the UAS threat. However, with so much Alliance technology relying on GPS or the GPS timing pulse, using GPS Jamming will require careful coordination and deconfliction with multiple agencies. This also assumes that the appropriate (scarce) technology can be obtained for deployment in the FP role? It is more likely that such technology, if deployed, will be deployed against larger systems beyond the immediate concern of the FP Practitioner.

Human Factors

Beyond the resource implications of introducing new capability, is the inescapable fact is that the world of the soldier, sailor, airman or marine is becoming ever more complex and the point is rapidly approaching where the individual is reaching their maxi-

mum capacity. This is in terms of both the physical sense of being able to simply carry all the equipment required and in the cognitive sense, where they are rapidly approaching a 'saturation point' of absorbing how to effectively operate multiple, separately developed, often incompatible systems which is becoming beyond many.

Planning Tools

Following-on from the above, an area where technology could have real positive effect for the FP Practitioner is in the area of FP planning. The author, in the course of researching this Section, was made aware of a software application originally called 'Surface to Air Missile – Precision Rating and Analysis Software (SAM-PRAS).[xiv] This software is in use by a number of nations and over a significant number of years has been developed well beyond a simple Counter-Surface to Air Missile planning tool. The system has now evolved to the degree where it can be used as a Decision Support tool. Different layers can be developed with each corresponding to either a different threat or different manifestations of the same threat. Of equal value is the ability to use the tool to site different friendly forces sensor systems for maximum effect. The key point is that it is highly unlikely for the foreseeable future that significant additional resources are going to be made available for FP. Therefore, more effective planning that enables the better use of existing, scarce resources, has to be pursued and relatively cheap, but nonetheless effective, planning tools require greater investigation; the JAPCC remains actively engaged in this endeavour.

[xiv] Whilst other software applications may exist, none became apparent whilst conducting basic, open-source market research.

NATO Defence Planning Process (NDPP)

The argument advanced within this Section is that the solution to countering the UAS threat lies predominantly in adapting existing counter-threat thinking and TTPs. To do this effectively, particularly if it is identified that additional, specific resources are required, it is perhaps worth considering developing a discreet C-UAS Capability Code and the supporting Capability Statement for introduction into the NDPP.

Takeaways

Specific Observations

During the development of this Section, a number of observations came to the fore that need to be highlighted:

- Organisation should be wary of vocal, overly influential, minorities.
- UAS are just another threat for the FP Practitioner to contend with.
- NATO FP publications remain fit-for-purpose when applied to the C-UAS challenge.
- The intellectual component is key.
- The threat from UAS must be considered together with all other potential threats.
- Even a small UAS with limited range, endurance and payload will present a major threat in certain circumstances (e.g. if used against fragile, high-value but low-density assets).
- C-UAS is not only an FP Practitioner's responsibility.
- A comprehensive, inter-agency, system-of-systems-based approach is necessary.

- In many cases the FP Practitioner is constrained by legal considerations.
- Some existing technology will be effective or, could easily be adapted.
- Any new approach must be considered across all Lines of Development.
- Traditional FP measures such as camouflage, concealment, screening and hardening together with TTPs such as the deployment of Sentries will be effective against UAS.

14

By Lieutenant Colonel Andreas Schmidt, GE AF
By Lieutenant Colonel Jürgen Welsch, NE AF
Joint Air Power Competence Centre

Command and Control

Introduction

Unmanned Aircraft Systems (UAS) are part of daily life, from hobby enthusiasts and delivery companies to actual people/groups with malevolent intentions, and also present a growing capability in armed conflicts. This circumstance gets amplified by the fact that Unmanned Aircraft (UA) are classified in various size/weight categories and may have a substantially different threat behaviour. Due to their omnipresence, Command and Control (C2) of C-UAS must be available from peacetime to conflict, which requires deconfliction between civilian and military responsibilities. The threat of UAS is significant, increasing and cannot be ignored. Due to the very nature of some UA, they will be detected quite late, which drastically reduces the available

time to execute the kill-chain. Therefore, it is not sufficient to only have all the tools, like Air Defence (AD) systems, readily available to counter this threat, but also an intricate system of C2. This includes the appropriate sensors and C2 networks, which are necessary to maximize efficiency and actually bring the overall system to life.

Command and Control for C-UAS in Peacetime

To fully describe the C2 situation for C-UAS, we need to distinguished between peacetime, crisis and conflict conditions, between military and civilian, but also national and NATO responsibilities and the class of UA[i] and the individual components of the UAS.[ii]

In peacetime, two C2 structures/processes, military and civilian are responsible for executing C-UAS operations. On the military side, safeguarding the integrity of Alliance members' sovereign airspace is a continuous peacetime task contributing to NATO's collective defence. The NATO Air Policing mission is carried out using the NATO Integrated Air and Missile Defence System (NATINAMDS), where the Supreme Allied Commander Europe (SACEUR) has the responsibility for the overall mission conduct. Allied Air Command (AIRCOM) oversees the NATO Air Policing mission with 24/7 C2 from two Combined Air Operations Centres (CAOCs), which are responsible for their respective areas of NATO European Territory (NET). When an incident is identified which threatens the integrity of NATO's airspace, the CAOCs will order interceptor aircraft based

[i] Within NATO, UA are classified in three categories. Class I (up to 150kg) for the micro, mini and small drones, to Class II (150-600kg) for medium-sized, tactical systems and Class III (more than 600kg) for Medium-Altitude Long-Endurance (MALE) and High-Altitude Long-Endurance (HALE) aircraft.

[ii] Unmanned Aircraft, Operator, Data Link, C2 Element, Payload and Logistic Support

on the location of the incident. NATO member nations provide the necessary aircraft and assets for the air policing of their own airspace, under SACEUR direction. Subordinate to the CAOCs, national military Control and Reporting Centres (CRCs) not only support the CAOCs with their air picture, but also control military air traffic, including the Quick Reaction Alert (QRA) (I),[iii] within their national airspace.

In contrast, the respective civilian Air Traffic Control (ATC) structure is quite flat. A certain ATC service is responsible for air traffic handling, coordinating with military or adjacent civilian ATC units and ensuring flight safety within their assigned airspace. In case of unauthorized flights within their airspace, they have no authority other than reporting the incident to the appropriate military agencies (CRC) or the police. Civilian ATC units do not have the capability to interrogate uncooperative aircraft or force them to alter their flightpath. If necessary, the corresponding national military needs to support with official assistance.

NATO uses NATINAMDS to ensure the security of NATO nations' airspace. All available sensor data is compiled within the CAOCs into an overall air picture, the so-called Recognized Air Picture (RAP). NATINAMDS includes a network for data transmission (e.g. RAP) and adequate tools to support the AD mission in general. New instruments like the Air Command and Control System (ACCS) or the Air Command and Control Information System (Air-C2IS) aim to improve this capability. In the CRCs, national systems are employed as well (e.g. the German Improved Air Defence System [GIADS]). Since C-UAS is a mission that involves more than the air domain (i.e. targeting all components of the UAS), an

[iii] Quick Reaction Alert (Interceptor)

overall Common Operational Picture (COP) is needed and being made available by NATO sensors, C2 tools and networks.

Air traffic participants have to be identified or have the responsibility to identify themselves by technical or procedural means. Identification Friend or Foe (IFF) transponders are a requirement for a certain subset of aircraft, so are two-way radios and regulated aircraft markings. Also, the airspace is organized by ATC means, which allows for better organization and identification. In addition, typically for smaller drones, national regulations and laws exist in order to deconflict drone flight areas from regular air traffic, civilian infrastructure and special events. If an aircraft's action is constituting a military threat, which is difficult to determine, as defined by NATO and national regulations, agreed upon military measures against the threat can be executed. If the aircraft is in a RENEGADE[iv] situation or in violation of national/international laws without posing a civilian threat, the appropriate national civilian law enforcement agencies and appropriate military Airspace Control Authorities are in charge of solving the issue. This also applies to countering or addressing other components of the UAS, e.g. remote-pilot, data link or control station.

All these situations have one thing in common: the aerial object has to be detected and tracked by one or more sensors and subsequently classified and identified. Class I UA and drones, however, are characterized by a very small Radar Cross Section (RCS). In addition, they normally fly very low in areas with a lot of clutter (cities). That makes it very difficult for any airspace sensor to continuously detect and track them and therefore successfully execute C2. It can be difficult to distinguish between aircraft that do not appear on any higher level (e.g. CAOC or ATC) air picture

[iv] Renegade: Civilian aircraft abused (e.g. hijacked) as a threatening system.

or aircraft that appear only very shortly or sporadically due to low flight levels or size. For aircraft that never appear on the RAP, especially small Class I & II UAS, but are detected either visually or by other means of local authorities, national law enforcement has the task to deal with regulation violations. However, since the respective aircraft are very likely in the category low/slow/small, the measures can only be reactive or very localized. This also applies for countering or addressing other components of the UAS like its remote-pilot, data link or control station. Aircraft that only shortly or sporadically appear in the RAP in the CAOC will be checked by means of an air policing response. If local airspace violations are detected by ATC, local procedures are activated and the incident will be reported via a military CRC. In both cases, countering and addressing the other components of the UAS, such as the remote-pilot, data link or the control station, is the responsibility of national law enforcement authorities. Because of that circumstance, the military, ATC and law enforcement C2 architectures and systems need to have a feasible level of multilateral interoperability and certain automated information exchange mechanisms.

Since these processes, structures, sensors, interceptors and tools are designed to handle known regular and irregular manned air traffic participants and their unmanned equivalents, there need to be regulations about who is responsible for all aircraft which are currently not reflected in or do not abide by the rules. Overall, it is of the utmost importance that the different C2 channels interface seamlessly in real-time.

Deployed NATO forces in peacetime, like maritime task forces, will be part of NATO's peacetime C2 structure. Here C-UAS operations will be limited to self-defence.

Command and Control for C-UAS in Crisis/Conflict

When circumstances dictate the transition from peacetime to crisis/conflict, it will have significant impact on air traffic and its control in the affected region or Joint Operation Area (JOA). The continuous use of civilian UAS will definitely have to be addressed to prevent unintended actions against non-threatening aircraft. In joint operations, NATO will stand up a Joint Force Air Component (JFAC) equipped and manned to conduct and support air operations as part of the joint force in the region. Depending on the intensity of the crisis/conflict, the civilian air traffic will be restricted and reduced to maximize air safety and minimize friendly force attrition. So, regional ATC C2 and NATO military C2 for air traffic control need to be clearly harmonized to maximize safety and minimize friendly attrition. This becomes very critical during the transition from peacetime, when NATO nations start to transfer military forces into NATO's C2 structure and NATO starts executing the mission.

The military approach to counter UAS can be separated into offensive, defensive, active and reactive actions. In the construct of Defensive Counter-Air (DCA) and Integrated Air and Missile Defence (IAMD) operations, military force can be applied according to the Rules of Engagement (ROE) and as necessary for self-defence. In both cases, a clear hostile act or hostile intent needs to be present, or in the most extreme case 'the absence of friendly behaviour', to act with military force. Hostile intent in an environment with a large presence of friendly or neutral UA will be more complex to be unambiguously identified and must be well defined, coordinated and communicated before the mission starts. Otherwise, either collateral damage or the risk level for NATO forces might be disproportionally high. For UA that are within the coverage of IAMD systems, the JFAC can employ various forms of

engagement zones like Fighter Engagement Zones (FEZ), Missile Engagement Zones (MEZ) or Short-Range Air Defence Zones (SHORADEZ). Here, the air battle will be conducted within NATO's Air C2 construct, using current concepts, plans and tools like ROEs or Tactical Battle Management Functions (TBMF). In accordance with international law, NATO forces can always act in self-defence to protect NATO/NATO-led forces and personnel, when an attack is ongoing or imminent. Since a lot of Class II UAS threats (and a majority of Class I as well) are ad hoc, hardly show up consistently on the RAP and have to be dealt with in real-time, which leaves little room for a long C2 chain for engagement decisions. This means that the more time critical the anticipated engagement decisions are, the lower the engagement authorities have to be delegated towards the actual shooter to be effective. Decision points to delegate engagement authorities have to be identified during the planning phase. For the UA that cannot be included in regular air battle decisions, covered by Weapon Control Status, ROE and TBMF, self-defence will have to be applied as the only alternative. This however implies that most C-UAS capable units for Class I and II defence have to be constantly in a higher alert state to cope with the constant threat that cannot be handled by higher C2 levels. This has direct impact on the defence design and emission control planning. In general, even in the regular air battle, the engagement authority for ad hoc threats, like smaller UA, might have to be delegated lower and earlier on compared to more predictable air threats. This could speed up engagement decisions, as dictated by the UA threat.

In smaller NATO missions, where land or maritime components are deployed independently, the C2 for C-UAS will be heavily dependent on self-defence, but otherwise has to be defined in accordance with the task and available capabilities within the mission construct.

For other UAS components, such as the data link, the C2 element or the operator, more C2 segments outside of the JFAC may be necessary. Since it requires special Electronic Warfare (EW) equipment to identify, analyze, interrupt or hijack a UAS data link, especially the more complex satellite or cell phone links, the appropriate C2 of these effects needs to be planned and coordinated via the EW element in the theatre component and effected via the Air Operations Directive (AOD) or the Air Tasking Order (ATO). Engaging or even identifying UAS operators or C2 elements during DCA operations is challenging and therefore needs to be dealt with either by Offensive Counter-Air (OCA) operations or with the support of other theatre components like the land, maritime or cyber component and most likely managed through a Joint Forces Command.

Command and Control Considerations for Deployed Forces

In general, three variations of the operational environment can occur: 1) the JOA encompasses all of NET, 2) the JOA is within a fraction of NET and 3) the JOA is outside of NET. In all three cases it is important to synchronize the C2 of the operational forces and the receiving region within the JOA and with bordering C2 systems/architectures, especially on the fringes of the JOA. Synchronizing with non-NATO C2 architectures might cause interoperability issues. All this needs to be considered during the operational planning process.

If the JOA is outside of NET as part of NATO crisis management, the necessary NATO C2 to engage UAS either within ROE or self-defence have to be coordinated with the host nation's military and civil C2 elements. As a crucial part of operational planning, the activation of ROEs has to be closely negotiated with the host nation. Furthermore, the use of the Electro Magnetic Spectrum (EMS) to control, capture or disrupt the UAS data link needs to be

coordinated with national and potentially other non-hostile military entities as well. For necessary military action on the surface and in the cyber domain, NATO land, maritime and cyber C2 needs to be harmonized, as well. C-UAS operations in NET will continue as before, however, a close linkage to the Air C2 in the JOA needs to be established to foresee or coordinate an increased UAS threat for NET.

If the JOA is within a small fraction of NET, the corresponding crisis/conflict C2 elements also have to coordinate with the host nation's military and civil C2 counterparts. In this case a closer coordination with NATO´s peacetime Air C2 structure needs to be maintained to have a seamless C-UAS coverage (within the IAMD spectrum) over the whole NET. The increased likelihood of 'spill overs' into NET needs to be taken into consideration and potentially the military augmentation of local law enforcement agencies outside, but close to the JOA and within NET should be planned for sure.

In case of a Major Joint Operation (MJO) that encompasses all of NET, NATO C2 will be responsible for the defence of the whole region. However, close coordination with civilian authorities to maintain civil air traffic where possible and to use civilian law enforcement capabilities to augment NATO and NATO nation's military is necessary.

In all three cases, it is possible that components of the UAS (e.g. operator, C2 element, data link hubs) are not within the JOA, enemy territory or a NATO country. Since targeting these components might be necessary, the appropriate authorities need to be identified, potential operations deconflicted and a legal framework needs to be identified. This might encompass military, civilian, regional, national and local C2 structures.

General Issue of C-UAS Command and Control

One major issue with C-UAS C2 is the very small RCS and potentially low flight paths of a large subset of UA, since detection is key to start the C2 process. This leads to significant sensor coverage problems, hampering successful C-UAS C2. Like all other C2 constructs, the C2 for C-UAS operations is constantly evolving to cope with the always evolving threat. However, C-UAS operations are joint and multi-domain by nature, so the corresponding C2 is quite complex. Timely information sharing between decision-makers and operators is key and it needs to be agreed who needs and gets which data for what purpose. However, the use of surveillance data for offensive operations against UAS segments lends itself to legal discussions between NATO nations and might require so called 'red-card holders'. Also, military-civilian information exchange in deployed situations, especially outside of NET, needs to be regulated. In general, the situational awareness of the UAS threat needs to be maximized with available real-time and non-real-time data. For example, equipping highly flexible SHORAD Man Portable Air Defence Systems (MANPADS) with a Link-16 RAP increased their efficiency and effectiveness. Ideas like this could be applicable for C-UAS missions below the IAMD spectrum.

The more data from various sensors in the joint environment that is available and the more dynamic the opposing use of UAS will be (especially with small RCS and low flight profiles), the faster C-UAS C2 needs to be to produce decisions that will be relevant and effective. The implementation of Artificial Intelligence (AI) or deep learning processes might be beneficial to support C-UAS C2 for air picture interpretation and potential decision support. Again, it needs to be regulated and defined how machine supported C2 decisions can be used/implemented in C-UAS missions or if such tools only augment the current C2 process.

Conclusion

NATO has existing and functional C2 structures, processes, networks and tools that are capable of countering the traditional air and surface threats. Over the last decade, NATO developed and improved its C2 to counter evolving and emerging threats like ballistic missiles or threats from the cyber domain. The same needs to be done with C2 for C-UAS. For missions that fall into the realm of IAMD, available C2 seems sufficient, but UAS that are clearly not within the scope of IAMD or on the fringe areas, need to be reflected in a well-integrated C2 environment. Especially because the very nature of C-UAS makes it a joint and multi-domain issue, the associated C2 needs to take that into consideration to allow for the appropriate effects to be delivered in time. It needs to be evaluated, whether the structure, process, tools and network are fast enough to address the threat and minimize the risk.

The widespread use of UAS of all classes for civilian and military purposes complicates proper situational awareness and therefore accurate and timely reactions to a potential threat or to mitigate the risk. Regulations about the use of civilian UAS and military/law enforcement authorities need to be robust in peacetime, crisis and conflict.

C-UAS as a military problem involves all levels of C2, from strategic decision-makers down to the individual warfighter. C-UAS C2 needs to ensure that all necessary information is available at all levels to allow vital decisions, especially final engagement decisions, to be made in time to be relevant. Lastly, the C-UAS C2 needs to be flexible enough to reflect the evolving multi-domain environment and all available and upcoming C-UAS systems.

15

By Lieutenant Colonel André Haider, GE A
By Lieutenant Colonel Roy Milke, GE AF
Joint Air Power Competence Centre

Education and Training

Introduction

Education and Training (E&T) is an integral part of any armed forces' ability to generate, maintain and strengthen their military capabilities, provide security and practise collective defence in the broader context of the NATO Alliance. With today's swift innovations in technology and their incorporation into military forces, non-state armed groups, and terrorist organizations, E&T requires constant review and adaptation. This holds especially true for unmanned systems, due to their increased civilian and recreational use and the subsequent complications for military activities, even before actual conflict.

NATO has defined four core dimensions to this adjustment process: education programmes, individual training, collective training, and exercises.[1] With an emphasis on the tactical level, this chapter focuses on the first two dimensions as prerequisites to any further collective training and exercises on the operational level and higher. It discusses how Unmanned Aircraft Systems (UAS) and drones present new challenges to NATO forces and thus require enhancing individual knowledge and skills to defend against them.

How Unmanned Aircraft Systems and Drones Change(d) Warfare

Proliferation of Unmanned Aircraft Systems and Drones

The last two decades have seen the evolution of military unmanned capabilities, predominantly in the air domain. The success of UAS operations in the global war against terrorism, as well as the use of drones by the terrorists themselves, created an unprecedented demand for those systems on both sides. At least 95 countries currently possess UAS or run their own development programmes.[2] At the same time, the commercial market has been flooded with drones for a variety of recreational and commercial applications. Chapter 3 (cf. p. 34 ff.) outlines the proliferation of UAS and drones in more detail.

Due to this widespread proliferation of UAS and commercially available drones, and based on numerous examples of recent conflicts, it should be expected that the probability of these systems being used against NATO forces is exceptionally high. This likelihood, in turn, requires a thorough analysis of these systems' capabilities, the potential new threats they present, and how forces need to be educated and trained to cope with this challenge.

New Capabilities, Potential Threats, and Challenges

For decades, if not centuries, the military has been the driving factor for the development of new technologies and state of the art equipment, which has almost exclusively been reserved for military purposes. This situation changed drastically after drones became a product for wide recreational and commercial use.

Sensors. Chapter 3 (cf. p. 41 f.) provides an overview of the typical sensor suites currently available for military and commercial systems, such as Electro-Optical/Infrared (EO/IR), Synthetic Aperture Radar (SAR), Light Detection and Ranging (LiDAR), or Multi-/Hyper-Spectral Sensors. Most of these sensors are not new, but due to the commercialization of drone applications, these sensors are no longer exclusively reserved for military use and are no longer a niche capability. Sensor resolution has been significantly increased over the last 5-10 years, while Size, Weight and Power (SWaP) requirements have been drastically reduced. These improvements enables even small drones to carry sophisticated sensor equipment, something that was not considered feasible just a few years ago. Hence, NATO has to expect that every UAS and drone is likely capable of capturing high-definition imagery and video, to include recognizing thermal signatures. More dedicated sensors such as LiDAR can even map terrain and objects through clouds and beneath forest canopies or detect disturbed soil from, for example, tracked vehicle movements.

Weapons. Depending on their size, many UAS are capable of carrying the same air-to-ground and in some cases air-to-air munitions as their manned counterparts. It is noteworthy that Russian, Chinese and to some extent Iranian systems are almost always armed, independent of their actual primary mission. Chapter 3 (cf. p. 36 ff.) and Annex B (cf. p. 513 ff.) provide an overview of these systems. Commercially available drones, although generally

unarmed, can be converted into an airborne Improvised Explosive Devices (IEDs). Even a payload of explosives as little as a couple of hundred grams can have devastating destructive potential if aimed properly. Moreover, UAS and drones report their sensor data back to their attached network or operator which can then be used to generate coordinates for targeting or indirect fires. Hence, even small drones require serious attention if spotted in the vicinity of friendly forces or infrastructure.

Employment. UAS and drones offer the unique advantage to employ a surveillance and strike capability at relatively low cost and with reduced risk of friendly casualties. Consumer drones, due to their almost negligible cost, may be intended for one-time use only and not recovered. Additionally, Low, Slow, and Small (LSS) drones operate at altitudes insufficiently covered by traditional air surveillance radars. LSS drones also offer little to no relevant signatures for current air defence systems to be employed successfully, notwithstanding the significant cost-benefit imbalance of high-tech anti-air munitions against the drone. These factors strongly support the employment of UAS and drones even in heavily defended air space or other situations where manned combat aircraft are at risk. Therefore, NATO has to anticipate UAS and drones to be directed against friendly forces at all stages of a conflict and independent of own air superiority.

Current Education and Training versus New Threats

The possibility that our forces may be subject to airborne ISR, air-to-ground strikes, and indirect fires is not new. However, NATO forces have neither experienced nor were required to anticipate any substantial air threat since the end of the Cold War-era. Air dominance was either a given or always achieved easily and there-

fore not a priority task for the majority of NATO forces. A lot of NATO nations significantly reduced their Surface-Based Air and Missile Defence (SBAMD) forces and some nations even totally dismantled their Short-Range Air Defence Systems (SHORAD), losing with them an entire generation of educated and trained personnel. However, the possibility to employ UAS and drones anytime, anywhere, and with affordable, robust capabilities implies a significant change to the potential threats NATO has to anticipate from the air.

Airborne Intelligence, Surveillance, and Reconnaissance

Protection against reconnaissance from the air has taken on a whole new dimension. UAS and especially drones are affordable in much larger numbers, and often operate at significantly lower altitudes than legacy ISR aircraft, thus bringing their modern sensors way closer to their target than was thinkable in the past. During the Cold War-era, it was assumed to be sufficient to spread camouflage nets over large areas and blur vehicle tracks in the terrain to escape enemy reconnaissance from the air, or at least to make it more difficult. However, today's sensors can easily penetrate the forest canopy and wide meshes of traditional camouflage nets, detect IR radiation and recent changes in ground conditions.

Air-to-Ground Strikes

The leap in unmanned technology in conjunction with the refinement of Precision-Guided Munitions (PGM) merged into a strike capability that was not envisioned during the Cold War nor has it been witnessed from any adversary in NATO's recent warfighting history. Moreover, UAS and drones can be used with kamikaze tactics by turning the vehicle itself into a weapon, homing in via their sensor inputs, such as thermal signatures, pre-programmed picture patterns, or radar and radio emissions. These threats were

traditionally countered, for example, by the dispersal of forces in order to minimize the potential damage of an attack. In contrast, NATO's recent decades of warfighting against an asymmetric enemy led to a situation in which protective measures focused mostly on a two-dimensional threat. For example, vehicles in military convoys or patrols followed each other very closely, and field camps were set up centrally and in the open to host large amounts of forces.

Direction of Indirect Fires

In the same way as NATO's recent warfighting history was not confronted by any substantial air threat, massive artillery fires were also not of concern apart from irregular and uncoordinated mortar fire incidents. Future conflicts against a near-peer or peer adversary, however, may see a re-emergence of an indirect fires threat. Modern artillery systems can deliver massive firepower within minutes of request and UAS and drones are likely to provide the respective target information. This has already been demonstrated in Eastern Ukraine where Russian forces directed and adjusted artillery fires with even Commercial-Off-The-Shelf (COTS) drones. The new threat dimension arises from the potential increase in speed between target acquisition and delivery of fires. In addition, improved accuracy of target data and therefore fires as a whole must be expected, since both UAS as well as artillery systems now utilize space-based navigation and timing support.

How Education and Training Needs to Adapt to Countering the Unmanned Threat

First and foremost, it is imperative to recognize the C-UAS challenge and approach the problem holistically. Chapter 5 (cf. p. 75 ff.) outlines a possible comprehensive approach to C-UAS, whereas

E&T plays a fundamental role for the recommended preventive and reactive countermeasures. However, it may not always be required to develop new Tactics, Techniques, and Procedures (TTP) to deal with a changing threat environment. Many long-established training concepts probably just need to be revitalised or moderately adapted to cover parts of the new unmanned threat. The following sections briefly describe the respective educational disciplines and training areas.

General Knowledge of Drone Capabilities

The first step in defending against a threat is to understand it. Education about UAS and drone capabilities should start as early as possible, preferably as part of the general basic training of new recruits or cadets. 'Drone Defence' should have a priority equal to other general topics, e.g. Nuclear, Biological, and Chemical (NBC) defence or All Arms Air Defence. The curriculum should at least cover the different classes and types of military UAS and commercially available drones, their sensor capabilities, as well as their potential weapons effects. For very little money, basic training units may be equipped with consumer drone models to demonstrate basic sensor capabilities first-hand.

Adapted General Rules of Conduct for the Individual Soldier

Defensive tactics against UAS and drones needs to be trained down to the lowest tactical level. There are already many traditional countermeasures against air threats in place that merely need to be adapted. The following subsections contain brief examples of possible adaptations of established tactical level TTPs. This list is far from exhaustive, and the general rules of conduct should be thoroughly reviewed concerning UAS and drone threats.

Camouflage. Command posts, combat vehicles in resting areas or hidden positions, as well as larger equipment, have always been concealed from air threats. In contrast, traditional measures of individual soldiers were usually aimed against observation from the ground only. Soldiers need to amend their camouflage tactics to also include measures against UAS and drone observations.

Thermal Screening. The standard pairing with an EO camera is an IR sensor. Thus, heat sources require additional attention when attempting to conceal them from enemy view. Older camouflage nets have a mesh size of several centimetres which cannot sufficiently shield thermal radiation. If newer generations of heat shielding nets are not yet available, makeshift measures such as covering bonnets with a thick layer of earth, may be considered.

Emission Control Measures. UAS can be equipped with Signals Intelligence (SIGINT) payloads which can be used to detect, track and locate the source of Radio Frequency (RF) transmissions, since modern Command and Control (C2) relies heavily on this type of communications. Therefore, enemy SIGINT requires thorough attention and probably reintroduction of traditional measures such as radio silence, cable communication or even forwarding messages by courier if possible. Other often overlooked sources of radio transmissions are the soldiers' mobile phones, wireless headphones and smartwatches which can undermine all other radio silence measures.

Dispersion. A long-established and successful measure to mitigate enemy weapons effects is the dispersion of combat vehicles and soldiers. With regard to the anticipated future presence of armed UAS and drones converted into airborne IEDs, it is even more essential to stick to this principle. Current TTPs developed and refined over the last decades of asymmetric warfare probably require an update in this regard with added focus on the third dimension.

Reporting. With their sensors, UAS and drones can cover an area much larger than can be observed by an individual soldier, a team, squad or even platoon. The presence of an enemy UAS or drone can be very likely linked to an upcoming attack or other effect. Reporting procedures about these detections help alert adjacent units and support the situational awareness of higher echelons. With regards to UAS and drones, it is important to accurately identify the class and type of system, altitude, direction and observable weaponry to help prepare appropriate countermeasures.

Adapted Readiness Levels for Air Defence

Dedicated air defence systems as well as All Arms Air Defence adhere to a set of NATO wide defined readiness states which regulate the weapons control status and areas of anti-air weapons. These levels may be reviewed and amended to also incorporate rules and measures to defend against the different classes and types of UAS and drones, if not already covered. Permission to fire at unmanned systems may be granted more easily than against manned aircraft since only material damage will be inflicted.

Adapted Responsibilities and Fire Areas for Anti-Air Weapons

UAS and drones come in various sizes and operate at different altitudes and airspeeds. To avoid responsibility gaps, all anti-air weapons in NATO are typically integrated and fire areas coordinated. However, NATO's Integrated Air and Missile Defence System (NATINAMDS) needs to adapt to the new UAS and drone threats and consider (re)integrating the Army's organic air defence units as well as the upcoming generation of dedicated C-UAS systems. This, in turn, requires review and revision of current air defence capabilities related doctrine and TTPs.

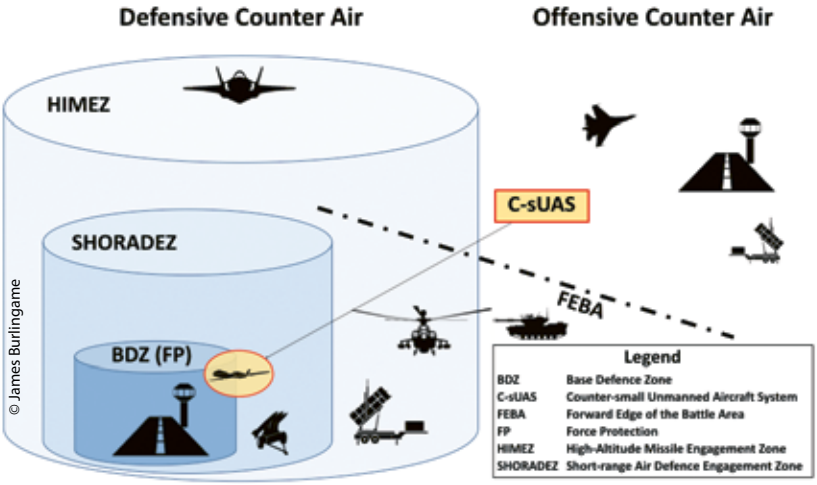


Figure 15.1: Layered Approach to C-UAS.

NATO Integrated Air and Missile Defence will have to counter the UAS air threat that already is within its identified threat spectrum (e.g. HALE/MALE). Also, the total subset and amount of UAS and drones that can be handled by NATINAMDS needs to be identified and integrated into current doctrine and policies. The interface to other capabilities outside of NATINAMDS needs to be specified and incorporated into these same doctrine and policies.

Short-Range Air Defence (SHORAD). Tactical UAS fly typically lower and are usually smaller than HALE or MALE systems. This lower region of defended airspace may be covered by SHORAD systems that are not part of NATINAMDS. As tactical UAS are relatively low cost, Anti-Aircraft Artillery (AAA) and Counter-Rocket, Artillery, & Mortar (C-RAM) systems could provide a cost-efficient anti-air capability against these systems.

All Arms Air Defence and Dedicated C-UAS Systems. Consumer and commercial drones fly at even lower altitudes than tactical systems, typically below 1,000 ft. They can usually only be detected by dedicated C-UAS systems and the reaction time for countermeasures is so low, that defending against these drones is mostly a self-defence duty.

Supplementary Curriculums for Aircraft Identification

LSS Drones, and also to a certain extent tactical UAS, can be expected to fly below the threshold of traditional air defence radars. This capability gap could be filled by air observers, which are supported by dedicated C-UAS equipment against LSS air threats. E&T for air observers should be reviewed and adapted to include the aforementioned threats. Specialized C-UAS equipment will likely expand the respective curriculums significantly and may necessitate the training of dedicated specialists on the unit or platoon level.

Recommendations

UAS and drones have been successfully incorporated into our countries' military inventories, and these systems have significantly changed the way NATO conducts warfare. Due to this success, potential adversaries are keen to follow the same approach and replicate NATO's unmanned capabilities. As a result, the Nations have to review and adapt their E&T curriculums to address the threat from UAS and drones being directed against friendly forces.

NATO Training Doctrine, Tactics, Techniques, and Procedures

Countering UAS and drones is a comprehensive challenge, and this chapter primarily discussed how education and training are

affected down to the lowest tactical level. Still, the true scope of the C-UAS challenge unfolds only in conjunction with the other chapters of this book, which address the various other military disciplines involved. To address this challenge, the different NATO training doctrines and TTPs need to be identified, reviewed, and, if necessary, revised. It may be worth considering having a dedicated C-UAS doctrine as a single point of reference and to avoid spreading interrelated content over too many publications.

NATO Countering Unmanned Aircraft Systems Working Group

The NATO Countering Unmanned Aircraft System Working Group (NATO C-UAS WG) was formally established in February 2019. This working group may also opt to take responsibility for further developing C-UAS related E&T in NATO, as the review of existing policies and the development of new policies, doctrine, and TTPs is already one of its priority focus areas.

Dedicated Countering Unmanned Aircraft Systems Discipline

'Discipline' is a NATO-approved sphere of knowledge and skills which supports existing and evolving capabilities. The list of disciplines is developed by the NATO HQ Supreme Allied Command Transformation (SACT) to focus E&T efforts on achieving NATO operational requirements in the respective fields. NATO should make 'Countering UAS and drones' a dedicated discipline in order to coordinate and align the respective E&T curriculums. The department head could help liaise between all the different disciplines involved in the C-UAS challenge.

Endnotes

1. NATO, 'Education and training', 24 Jul. 2019. [Online]. Available: https://www.nato.int/cps/en/natolive/topics_49206.htm. [Accessed 19 Oct. 2020].
2. Dan Gettinger, ,The Drone Databook',The Center for the Study of the Drone at Bard College, 2019. [Online]. Available: https://dronecenter.bard.edu/files/2019/10/CSD-Drone-Databook-Web.pdf. [Accessed 19 Oct. 2020].

16

By James S. Corum PhD, Lieutenant Colonel (ret.), US A
University of Salford

Strategic Communications

Introduction

This article will focus on the current and future use of UAS by states and groups hostile to NATO and Western allied nations and the Strategic Communications (STRATCOM). There are two salient facts that NATO forces have to take into account:

Firstly, UAS technology, primarily provided by Russia and Iran, is supplied to proxy nationalist and militant groups, thus, the employment of UAS against NATO and allied nations will become a standard feature in future operations.

Secondly, the Russians, Iranians and other states, as well as the assorted nationalist and militant groups allied with those powers,

will employ disinformation about their UAS (and all other) operations in order to gain political support and confuse and dishearten their enemies.

Countering disinformation and providing a full range of information support for the operations of NATO and Western allies is an essential mission for NATO STRATCOM leaders and planners. This article will propose some means by which an increasingly capable NATO STRATCOM programme can deal with the current threat. It will also look forward to understanding how the disinformation threat will likely evolve. Understanding the nature of the threat is an essential step in shaping an effective STRATCOM response.

Strategic Communications and Disinformation – An Overview

Disinformation, that is using various media to deliberately spread false accounts of events in order to defame and discredit one's enemies and gain and support and influence for one's own cause, is an ancient and very effective tactic within a broader strategy of conflict. Propaganda and disinformation are as old as warfare. However, thanks to mass media, modern means of communications and social media, spreading disinformation is an easy task. When carefully crafted for a target audience and used as part of a broader strategy of STRATCOM, disinformation can be highly effective as a political weapon. A careful study of disinformation shows different approaches used by nations and militant groups. The Russians, for example, have long employed a broad spectrum of STRATCOM methods from traditional media to social media and use of influencers and the use of 'troll factories' to flood social media and crowd out commentary. The Russian states use disinformation routinely more to seed confusion in the minds of the public

and their adversaries rather than to convince anyone. A common approach is to employ the media and influencers to encourage sometimes outlandish conspiracy theories and to provide alternative interpretations of Russian actions. A blitz of false information was an integral part of Russia's first push into the Ukraine.[1]

Not only hostile states, but even large terrorist movements have the talent and media resources to mount a STRATCOM effort that uses various media- newspapers and magazines, videos, pamphlets, films, and social media and internet sites to spread a message. The Islamic State (IS) has shown a genuine sophistication in using a wide variety of media to disseminate an array of messages to targeted audiences. At one level there is a campaign to encourage its followers and to assure them of eventual victory. At another level different media campaigns were developed to recruit targeted audiences. Finally, media was developed to discredit the Western and hostile regional powers that opposed the IS. Disinformation was part of all these campaigns and standard themes developed. Over time the IS honed and evolved its message.[2] Hamas and Hezbollah in the Middle East have demonstrated a real talent for putting together crafted messages geared to specific audiences. Both groups represent a large, popular party and they have used every form of media in a sophisticated manner to spread their message. Both have proven to be experts in working sympathisers in the international media and Non-governmental Organisations (NGOs) to support their narrative.[3] These groups develop their own video and photo media and are skilled in using the internet and social media to reach their own members and to put their case to a large, international audience. Their anti-Israel stance wins them broad support in the Middle East as well the support of many factions and groups in the West, usually the hard left of the European and American political spectrum. Both factions have shown they can use sympathetic

NGOs in the west to spread their version of the news and to accept their press releases and claims with little critique.

In short, some states and militant groups hostile to the West have demonstrated a sophisticated and multifaceted approach towards influencing the local and international public and media. Such states and groups have made strategic communications a major component of their conflict strategy. Adversary groups and nations do not hesitate to use disinformation as one of their major tactics. In many cases disinformation has proven to be an effective means to confuse their opponents, camouflage their true intent, and win support locally and among Western sympathisers. Information operations provide a militarily weak opponent the means to gain significant political advantages. However, disinformation themes also fall into common patterns and can be predictable to Western STRATCOM specialists who have studied the adversary's information operations. Armed with an in-depth knowledge of how adversaries promote their narratives, NATO and Western STRATCOM staffs can employ strategies that effectively counter adversary campaigns and expose their credibility and legitimacy as a sham.

NATO established the principles of STRATCOM during the ideological struggles of the Cold War and those principles are still valid in today's conflicts. Democratic societies can only conduct military operations with the support of their people and a healthy civil/military relationship can only function if the military is open and transparent about its operations – keeping classified only operational plans and capabilities whose release might put the military in danger. NATO will not allow disinformation as such actions would erode the legitimacy of its operations. NATO STRATCOM asserts that information about operations, even information about mistakes made and collateral damage inflicted be released to the public fully and as quickly as possible.

UAS Technology of Groups Hostile to the Western and Aligned Nations

We can look at some recent military operations in both Europe and the Middle East to examine the kind of groups that have acquired sophisticated UAS and how they employ them and factor them into their information campaigns. Russia, for decades one of the leading nations in aviation technology, has been able to field a considerable number of sophisticated UAS to support their sponsored Russian separatist forces fighting the Ukrainian government in the Donbas region since 2014. In 2018, Russia deployed 741 UAV across the 409 km front line between Ukraine and the Russian occupied east of the country. Ukrainian forces today face two to three sorties a day from Russian or Russian allied militants in the Donbas, but as many as ten sorties a day have been noted. In order to hide the Russian nature of the UAS and make them look as if they were the product of homemade Russian nationalists the UAS have been equipped with Swedish and Japanese-made video recorders and Chinese-made engine parts and even Israeli components. The Russians have shown considerable sophistication in providing these very capable hybrid UAS equipped with a wide variety of foreign made avionics and parts, but such efforts enable the Russian denial that they are actively arming and supporting Russian nationalists in a civil war in the Ukraine.[4]

The Iranian aviation industry, which has long supplied rockets and missiles of increasing range, firepower and sophistication to client factions in the Middle East that include Hamas, Hezbollah, and the Houthi rebels in Yemen, has designed some large UAS capable of long-range strike missions.[5] The Qatef, or 'Striker' drone used by the Houthis was examined by Western experts in 2018 and found to be 'virtually identical in design, dimensions and capability to that of the Ababil-T, manufactured by the Iran

Aircraft Manufacturing Industries'. The Ababil-T can deliver up to a 45-kilogram warhead up to 150 km away. Apparently the Iranian UAS was brought into Yemen and assembled there. In this manner, much like the Russian UAS supplied to the Ukrainians, the Iranians could deny that its drones had fired on targets in Saudi Arabia. In 2017 and in 2019, models of this UAS were fired at Saudi oil infrastructure targets from Houthi territory, while the Iranians denied any responsibility for the attacks. However, parts from the one largely intact drone that had failed to explode in Saudi Arabia proved to be Iranian -made parts identical to Iranian UAS recovered in Afghanistan and Iraq.[6] As the Iranian Quds Force, Iran's combination of intelligence agency and special forces, is heavily involved in Yemen and given the very limited Yemeni technical capabilities, it is likely that the Iranians are fully behind the use of UAS against their Saudi enemies.

For decades Iran has been the sponsor, financier, military supporter, and supplier of arms to the Hezbollah Party in Lebanon. Since its founding in 1982, Hezbollah has been closely linked with Iran as both countries are Shia and Hezbollah sees the Iranian Revolution as a model for its own ideology. Hezbollah has always had a large supply of rockets and missiles because the friendly Syrian regime has allied with Hezbollah and Syria offers an easy transit route for Iranian weapons and supplies. Although rockets have always been the primary weapon for Hezbollah, since 2004 Hezbollah has employed UAS against Israeli targets. During the 2006 conflict between Israel and Hezbollah, a small Hezbollah UAS packed with explosives struck an Israeli gunboat off the Lebanese coast and caused extensive damage. Given this success, the Hezbollah/Iranian UAS programmes proceeded and soon Hamas, also an Iranian client, was equipped with UAS. In late 2010, Head of the Counter-Terrorism Bureau in Israel, Brigadier-General Nitzan Nuriel said that both Hezbollah and Hamas were in posses-

sion of a number of drones with a range of over 300 km.[7] In 2013 the Israeli Air Force intercepted a Hamas UAS inside Israeli airspace. Since then the Israelis have shot down a number of Hamas drones but the Hamas UAS programme, working with Iranian components, has progressed to field more capable models. By 2014 Hamas was beginning to employ the Ababil UAS which is essentially the Iranian Sarir H-110 UAS.[8]

It should be noted that the forces employing UAS in increasing numbers – from the Ukraine to Yemen, Lebanon and the Gaza Strip – all try to hide the direct involvement of their suppliers Russia and Iran by claiming the UAS fielded are their own manufacture. Indeed, the Houthis and Hezbollah and Hamas have claimed great successes for their UAS, and they have certainly had some successes, and they use their possession of UAS as a major propaganda weapon- claiming that they have the capability to strike deep into Israeli or Saudi territory.[9] Thus, possession of UAS, especially those capable of carrying a warhead has become an important propaganda method for Middle Eastern factions. However, the groups also assert that these UAS are indigenously produced and attempt to maintain that they are independent forces and not serving as mere proxies for another power. Russia and Iran, for their part, work hard to hide their role as supplying and effectively controlling the factions aligned with them.

What this means for NATO STRATCOM is significant. One can look at a likely scenario. Should Iran supply any of its UAS to a militant group fighting the government of Afghanistan, a country that NATO supports with military aid and a training mission, then it should be a STRATCOM priority to expose and publicise the Iranian connection to the militants. Exposure of the Iranian connection would not only be a blow to the militants, undermining

their message that they are independent actors, but also win international support from the Arab states and encourage political action to further sanction the militant groups. One can also see a similar STRATCOM strategy playing out in the Ukraine, where exposure of Russian high-tech military support would help build political support for sanctions.

Human Shields Protecting Adversary UAS Assets and NATO's Response

In conflicts since the 1980s, the use of human shields to protect military targets and to create a propaganda message has become a common tactic in fighting Western powers. Indeed, the use of human shields has become one of the most effective weapons in limiting Western Air Power. Although highly illegal, the use of human shields is more effective – and much cheaper – than a sophisticated anti-aircraft system. The use of human shields is a tactic used by both state military forces and by non-state militant groups. The practice is widespread enough that planning to deal with it and to deal with the STRATCOM effects of this tactic should be part of NATO air doctrine and planning. The use of human shields is a key part of an adversary STRATCOM strategy that seeks to maximize civilian casualties whenever a vital military asset is targeted during an air campaign. If a valid military target is attacked and civilian casualties occur, the story will be presented to the international media that Western nations are deliberately targeting civilians. If air forces are deterred from attacking valid military targets for fear of the media effect, then the adversary state or group has effectively protected its important weapons. Adversary groups see this brutal use of civilians as a 'win-win' strategy.

In Middle Eastern conflicts first the PLO, then Hezbollah and Hamas employed human shields to protect their military forces and assets and to serve as an important disinformation tactic as well. They know their opponents take great care to avoid civilian casualties and collateral damage in air operations. Placing command centres, arms depots, drone workshops and UAS ground stations next to clearly civilian institutions, such as schools or hospitals, are likely to deter Western air forces from attacking the targets for fear of killing civilians. If Western air forces strike such targets – even taking exceptional precautions and using only precision munitions to minimize collateral damage – the militants will show sympathetic journalists the civilian damage and casualties as 'proof' that their Western enemies are war criminals attacking civilians as they ensure that no mention of the actual military target is made. Even if military forces and equipment are lost by means of an air strike, the political/media effect can be of equal or greater worth than the military loss.

UAS have become valuable prestige weapons for militant non-state groups. The possession of large rockets and weaponised UAS demonstrate to their followers and their enemies that they have a genuine conventional military capability to strike targets deep in their enemies' homeland. The possession of UAS gives non-state groups considerably more political leverage and credibility. Proliferation and rapid technical development of UAS means they will be acquired and used in ever increasing numbers. Absent highly sophisticated and expensive anti-aircraft systems, military items beyond the financial and technical expertise of non-state groups, NATO and Western nations can expect that non-state movements in possession of UAS will routinely employ human shields to defend their prestigious weapons that are important for both military and information operations. In operations against non-state groups NATO and Western nations can expect that the UAS and

larger rocket will be assembled and stored, and likely controlled, from prominent civilian targets (schools, mosques, hospitals). It is probable that they will be launched in the close proximity to prominent civilian facilities. This will place any Western forces trying to destroy hostile UAS before they are fully assembled or launched in the difficult position of either allowing the enemy full use to employ long-range weapons with no retaliation, or face negative media coverage for striking such weapons. Indeed, such 'human shield' actions by authoritarian states and militant groups are common enough that NATO headquarters and staffs need to train to deal with this tactic and also plan to conduct an information campaign to educate the media and the public.

Another key part of the information/disinformation campaigns carried out by militant groups is their ability to control the media coverage and present a united front to support their message. Adversary non-state groups could also enforce their will and their message upon the population they control with brute force.[10] Many militant groups admit Western journalists to their territory, but only under strict conditions and controls and their coverage is carefully edited and censored by media minders.[11]

This theme of civilians killed by Western Air Power plays well with the local population and has played well with much of the European public in the past, so this theme and variations on it can be expected as a pillar of any future adversary information campaign. Another key theme played in the information campaigns of militant groups is their ability to carry out strikes into enemy territory. This theme is directed to both internal audiences as well as international audiences. A poor military situation can be played as a military/political victory as long as the adversary maintains the ability to fire rockets and fly UAS into their enemy's territory.[12] One can easily imagine a conflict in the near future where

a NATO air strike on a drone storage facility surrounded by civilian human shields would be presented to the international media and cause a severe political backlash for NATO. On the other hand, if NATO refrained from targeting the UAS storage facility, the ability to continue long-range attacks by UAS would give the adversary state or group an enhanced level of military/political credibility.

Evolution of NATO STRATCOM Policy and Doctrine in the Last Decade

STRATCOM has taken an increasingly prominent role in NATO planning and operations in the last decade. By 2010, NATO began publishing more detailed guidance on STRATCOM that included improved coordination among friendly actors, more use of social media, market research to better understand the audience, and developing civilian channels of communication.[13] The Russian invasion of the Ukraine in 2014 added further emphasis to NATO's effort to improve its STRATCOM capabilities. The STRATCOM doctrine has evolved considerably and, thanks to the Afghanistan experience, today NATO moves more quickly and efficiently in declassifying imagery information and in responding to adversary propaganda and charges. Indeed, rapid declassification and information response was a primary lesson from Afghanistan where NATO had to contend with a constant onslaught of Taliban disinformation. All of these changes and the new emphasis on STRATCOM remains firmly within the democratic principles of NATO: truthfulness is paramount. STRATCOM must maintain the credibility of the organization as democratic institutions require credibility, communication remains a collective effort, the information environment must be understood, and words and actions must be aligned.[14]

To effectively understand the information environment and to counter disinformation and adversary narratives NATO took a big step forward in establishing the NATO Centre of Excellence (CoE) for STRATCOM in Riga, Latvia in 2014. The STRATCOM CoE directs and publishes detailed research on adversary information operations. The Riga CoE is a key resource for understanding adversary states and groups and their disinformation methods, media use, influencing operations and narratives. The NATO STRATCOM CoE studies provide the essential background for the STRATCOM and operational planner to organise and conduct information operations prepared with information about adversary information methods, most common themes, and methods of disseminating disinformation.[15]

Ensuring that the message and actions are aligned, requires training and doctrine. The Strategic Communications Principles on NATO Joint Air Power of November 2017 provides guidance on building STRATCOM capability and better training and coordination. The accompanying document, The NATO Joint Air Power Capability and Capacity Needs (9 November 2017), specifically mentioned the importance of countering disinformation and lays out a concept of improved STRATCOM training to meet the threat.

Helping the Public Understand Air Power and UAS

While training and doctrine are essential parts of the military response to disinformation, one must also look to the long-term need to counter disinformation and improve STRATCOM before the broader public. A main reason for disinformation being able to flourish is the lack of understanding of Air Power and UAS among the general public of the NATO countries. The mainstream media tends to have little understanding of the military and Air

Power, so even when the media is given accurate information, they tend to lack the basic context needed to communicate clearly to the public. There are several long-term actions that NATO STRATCOM can employ to improve the understanding of the media and the public about Air Power and its use by NATO. The 2017 study on Air Power and Disinformation by the Joint Air Power Competence Centre (JAPCC) recommended that NATO provides week-long orientation courses for media members to educate them about air power and UAS. Such a course would let journalists visit airbases and receive an orientation on air operations and the UAS themselves. The adversary UAS threat could be outlined and, in the case of targeting adversary UAS the essential elements of UAS operations, to include the requirement for ground control stations, UAS storage and workshops, and satellite communications (SATCOM) installations as well as the UAS itself. Dealing with the UAS threat requires not only anti-air actions, but also targeting the key elements of the UAS system before the UAS is launched. Should NATO need to target adversary UAS at least some in the media will understand the basic concepts of UAS operations.[16]

Another recommendation of the JAPCC study on disinformation is to embed some selected journalists with air units during operations. Embedding journalists with ground units in Afghanistan proved successful as a means to educate the public about the nature of the NATO forces employed in the country and the problems they faced. Moreover, this has been done without exposing classified information. Embedding journalists into air units is possible under similar controls that would assure that current operational plans or exact technical capabilities would not be revealed. Such actions, in the long-term, can help the media report more accurately and give the public a better view of the operational challenges faced by NATO.[17]

Responding to Disinformation about Adversary UAS

In countering the expected disinformation that has, and will, arise from adversary use of UAS the first step is to maintain NATO STRATCOM's current policy and doctrine of quick declassification and release of information concerning the employment of UAS. Accurate information to the public about the operating principles, effects and capabilities of UAS and the defensive response will help settle the expected hype that will originate with the states and factions that employ UAS. A first principle of STRATCOM is to be truthful and transparent. Without credibility NATO could lose the public support required in a democratic alliance.

In responding to an adversary UAS use there are two specific actions that should be emphasized by NATO and Western STRATCOM. First of all, as adversary UAS use today comes not from nation-states fighting conventional wars, but primarily from proxy groups that are not capable of designing and manufacturing capable UAS on their own and are reliant on outside powers – specifically Russia in the case of Russian factions fighting in the Ukraine and Iran in the case of non-state groups fighting in the Middle East. In both regions of conflict, large state powers go to considerable lengths to hide the origins of the UAS being supplied to the non-state groups. The non-state factions, for their part, attempt to minimize or deny their close dependence on outside powers as their own information campaigns push the popular narrative that they are fighting a valiant 'David versus Goliath' battle against overwhelming odds. Thus, rapid exposure and analysis of imagery of adversary UAS, as well as analysis of captured or shot down UAS and determining their origin and manufacture, will go a long way to discredit the false narrative of the proxy groups that employ UAS. While local people and foreign media find the image of the resolute and independent freedom fighters attractive, the image of

a proxy army doing the will of a major power is certainly not conducive to building a popular local and international image.

The second action that should be emphasized is to record, document and publish the use of human shields protecting UAS ground installations and drone workshops by adversary states and militant factions. The use of human shields is one of the most common disinformation tactics of militant groups. Given their record to date, and the positive media they have achieved from the civilian losses and collateral damage that occurs when legitimate military targets are struck, we can expect that militant factions will protect their UAS assembly, storage and launching sites by placing them in, or adjacent to, civilian homes and institutions. Such actions are a clear violation of international humanitarian law and the use of human shields to counter any NATO operation needs to be thoroughly exposed. NATO could deploy a specialized media and legal team to collect, record and document the use of human shields by adversary states and groups. Such records should be used to bring war crimes charges against the perpetrators.[18] Adversary violations of international humanitarian law should always be a major theme of NATO STRATCOM.

Information operations are more important than ever. Disinformation can be expected, but it can also be effectively countered with a good understanding of likely enemies and their information operations. The last decade has seen a much more developed STRATCOM doctrine, a well-resourced STRATCOM directorate, enhanced training in information operations. This is also supported by the research and analysis of the NATO CoEs for STRATCOM and Joint Air Power. While disinformation remains a major threat against Air Power in general, training and better understanding puts NATO in a much stronger position to counter the threat of enemy information operations than a decade ago.

Endnotes

1. On Russian disinformation see James Corum (Ed.), 'Mitigating Disinformation Campaigns Against Air Power', Joint Air Power Competence Centre (JAPCC), Kalkar, 2017, pp. 49–50.
2. On the ISIS Information strategy and Operations see Rafel Zgryziewicz (Ed.), 'Daesh Information Campaign and its Influence', NATO STRATCOM COE, Riga, 2015. This study provides an in-depth analysis of the ISIS information campaign techniques, narratives, target audiences, and regional and local distribution.
3. 'How the media helped Hamas in the third Gaza War'. Missing Peace Website, 6 Aug. 2014.
4. Joseph Hammond, 'Ukraine drones show sanctions don't clip Russia's wings', Defence Post, 4 Oct. 2019. See also John Wendle, 'The Fighting Drones of Ukraine', Air and Space Magazine, Feb. 2018.
5. Dr Can Kasapoglu and Miriam Fekry, 'Iran's Proxy War in Yemen: The Information Warfare Landscape', NATO STRATCOM COE, Riga, Jan. 2020.
6. John Gambrell, 'How Yemen's rebels increasingly deploy drones', Associated Press, 21 May 2019. On Iranian UAS used in Yemen see 'Iran's Game of Drones: The Growing Threat from the Sky', The National Interest, 10 Aug. 2019; Ali Bakeer, 'Iran reportedly unveils military unmanned aerial vehicle (UAV) for reconnaissance and surveillance', Military and Aerospace Electronics, 9 Sep. 2019; John Gambrell, 'Devices found in missiles, Yemen drones link Iran to attacks', Associated Press, 19 Feb. 2020.
7. Arthur Holland Michel and Dan Gettinger, 'A Brief History of Hamas and Hezbollah's Drones', The Center for the Study of the Drone at Bard College, 14 Jul. 2014.
8. Ibid.
9. Ibid.
10. During the 2014 conflict with Israel several reports noted that Hamas had summarily executed as many as 50 members of the Palestinian Fatah Party as 'Israeli spies'. Hamas has also publicly executed Palestinian dissenters in 2012 and dragged their bodies through the streets of Gaza. See Shira Kipnees, 'Hamas Executions Against Palestinians Protesting War in Gaza', JSpace-News, 29 Jul. 2014; 'Hamas Suppressing Wartime Dissent: Shooting to Kill Palestinian Protesters', World Tribune, 31 Jul. 2014.
11. An example of this is Hamas' manipulation of the media, allowing journalists to photograph only dead civilians and not to show any military casualties or equipment. See 'How the media helped Hamas in the third Gaza War'. Missing Peace Website, 6 Aug. 2014.
12. A poll taken just after the 2014 conflict showed that Hamas' media policies and its ability to fire rockets into Israel won it increased support from the local population. See 'Poll: After Gaza War, Hamas Gathers Support Of 61 Percent of Palestinians' CBS DC, 2 Sep. 2014.
13. Allied Command Transformation (ACT), 'NATO Military Concept for Strategic Communications', 27 Jul. 2010.
14. Mark Laity, 'NATO and Strategic Communications – The Story So Far', The Three Swords Magazine 32/2018, Joint Warfare Centre, pp. 65–73.
15. Studies about disinformation and adversary information operations from the NATO STRATCOM Centre for Excellence can be accessed and downloaded from their website. Some recent studies include: Russian Information Campaign against the Ukrainian State and Defence Forces (Feb. 2017), The Russian Perspective on Information Warfare (Mar. 2017), Russia's Footprint in the Nordic-Baltic Information Environment (2018). The STRATCOM Centre of Excellence also publishes numerous detailed studies on non-state militant groups and their information operations. Some recent publications include: Daesh Information Campaign and its Influence (Jan. 2016), Daesh Recruitment: How the Group Attracts Supporters (Nov. 2016), Iran's Proxy War in Yemen: The Information Warfare Landscape (Feb. 2020).
16. Ibid. 1.
17. Ibid. 1, 180–183.
18. Ibid. 1, 179–180.

Part III

Civil Perspectives

17

By Alex Morrow, US
By Phil Pitsky, US N (vet.)
By Amit Samani, UK
Dedrone

By Lieutenant Colonel André Haider, GE A
Joint Air Power Competence Centre

Protection of Critical Infrastructure

Introduction

The challenges in countering drones are faced in both war and peacetime. As discussed in the previous chapters of this book, the risks presented by drones have increasingly come into the civilian focus over recent years. In particular, the incidents at Gatwick Airport (cf. Chapter 3, p. 48) and their consequences for flight safety, flight operations and, above all, economic losses have clearly illustrated this.[1] However, drones do not only threaten large facilities such as airports or military installations. The range of critical civil infrastructure is immense and in contrast to burglary and fire protection, awareness of the potential threat posed by drones is far from being widespread. Therefore, this chapter is intended to show which areas of critical civil infrastructure are exposed to a possible threat from

drones, what these threats may consist of, and how they can be dealt with pre-emptively because civilian businesses usually do not possess the legal authority to employ most of the active countermeasures discussed in this book.

Critical Civilian Infrastructure

Depending on the country, the definition of what constitutes critical infrastructure varies slightly. The German Federal Office for Information Security defines critical infrastructure as 'organizational and physical structures and facilities of such vital importance to a nation's society and economy that their failure or degradation would result in sustained supply shortages, significant disruption of public safety and security, or other dramatic consequences'.[2]

The United States' Cybersecurity & Infrastructure Security Agency defines 16 critical infrastructure sectors (cf. Figure 17.1) 'whose assets, systems, and networks, whether physical or virtual, are considered so vital [...] that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof'.[3]

Critical infrastructure components are, to a large extent, dependant on one another. Agriculture requires the supply of clean water, water purification and pumps require electricity, and electricity may be generated from the stored water behind a dam. Interference with transportation systems may cut off supplies for critical manufacturing and medical services. Communications, information technology and financial, commercial as well as public services are closely interlinked. These are just a few examples of how the disruption of a single critical infrastructure can trigger a series of effects that, together, can have far worse consequences.

Figure 17.1: Critical Infrastructure Sectors.

Therefore, any critical infrastructure has usually an emergency response plan in place to cope with any threats that may interfere with its operation. With the increasing proliferation of drones, a new threat has emerged that now requires consideration and incorporation into these response plans.

The Drone Threat – New Wine in Old Skins?

Critical infrastructure – civilian as well as military – has always been protected against the threats of its time. For centuries, even the principal threats have not changed, including burglary, theft, espionage and catastrophic damage to property and lives. Since the Great Wall of China, the construction of walls and fences around a site has been and still is the standard measure to protect

it against the aforementioned threats. The computer age was the first real game changer by offering a new attack surface for an adversary, namely the internet and its connected networks. But even in this new cyber domain, the traditional threats remain unchanged and the standard measure is – again – building a digital variant of a wall, commonly known today as a 'firewall'. The 'drone age' is not different. It just offers a new attack surface, the air domain, for the same set of threats, whereas the air domain is not even new, but it's now accessible for the broader public.

The 2019 Global Cyber Risk Perception Survey conducted by Marsh and Microsoft revealed that cyber-attacks are the predominant concern of international businesses, outranking other threats like criminal activities, industrial accidents, espionage or terrorism by a wide margin.[4] Because drones were not even part of the questionnaire it could be concluded that the current perception of their threat is rather low. However, it could also be argued that drones themselves do not represent a new type of threat, but could rather be seen as a new means of delivery only. Therefore, the following sections briefly outline how the initially mentioned centuries-old threats can be delivered by a drone and where traditional countermeasures continue to be sufficient or are being challenged.

Burglary

Burglary is typically defined as the unlawful entry into a structure with the intent to commit any crime inside. Traditional protective measures include, but are not limited to, building walls and fences around the structure, closing and locking gates, doors and windows, or employing a guard force. These measures either try to physically prevent access to the building or deter illegal activities by threatening the offender with detection, identification and prosecution.

Drones offer an offender the possibility to bypass any physical barrier by simply flying over them. Current consumer models reach altitudes of several hundred metres with ease. If no dedicated drone detection system is in place, chances are high, that this intrusion will even go undetected if properly planned. For example, guard shift changes or visual conditions at dawn, dusk and night may open a window of opportunity for an intrusion attempt. Drones also offer the advantage of minimizing the offender's risk of being identified and prosecuted, even if the drone is captured.

In peacetime, it is extremely challenging to prevent the intrusion of a drone as legal restrictions prohibit the use of active defence systems in many cases. It is therefore important to realize that burglary usually has a purpose, which is to commit one of the crimes described below. So even if it cannot deny access to the property, a reliable drone detection system will help to take the appropriate security response and measures to prevent the drone from fulfilling its mission.

Theft and Industrial Espionage

The term theft is used widely to refer to crimes involving the taking of a person's property without their permission. In our information age with businesses operating globally, not only physical, but also to a greater extent intellectual property has large monetary value. Physical property is typically secured by the measures of the structure hosting it. Sometimes it is additionally protected to either prevent unauthorized access to the property or to prevent removal of the property itself. In the cyber domain, this concept is represented by firewalls preventing access or by encryption of the property to prevent theft and espionage.[i]

[i] Encryption does not prevent downloading a file from a compromised network, but it will prevent the use of the obtained information unless it is decrypted.

Apart from specialized bomb disposal robots, drones are not (yet) designed to remove physical property from a structure. However, this is different with intellectual property. Current consumer drone models are typically equipped with electro-optical high-resolution cameras which are often also capable of sensing in the infrared spectrum. Drones may also be reconfigured with highly sensitive microphones to capture voice communications or even with a high-power wireless network repeater to force wirelessly networked devices and mobile phones to connect to the drone and, in turn, capture their communications.

Long established security measures for the protection of intellectual property and sensitive information can significantly hinder a drone from accomplishing its theft or espionage mission. It just has to be recognized that height no longer provides protection and every window, no matter on which floor, is prone to a drone's high-resolution camera and microphones. Closing the window and its curtains easily prevent a drone from taking any imagery. Arranging the office so that no sensitive information faces a window is also an option. Classified meetings can be held in windowless rooms so that no sound can be sensed through any windows or outside walls. Strict enforcement of cybersecurity measures not only for the company's computer systems, but also for the personnel and the private hardware they bring with them, would help reduce the risk of a drone-based cyber-attack.

Damage to Property and Life

Threats which may cause fatal damage to property and human life can range from unintentional, unwitting, or careless actions by one's own staff, resulting in an accident, up to intentional, wilful, or malicious acts of crime or terrorism.

Accident prevention is an integral part of even a small business' operations and is usually required by law. New structures are usually planned with fire protection and extinguishing systems right from the start. Fire drills are often mandatory to be performed at least once a year. Evacuation plans or information on hazardous substances are typically displayed prominently for everyone to see. All these measures contribute to raising the awareness of existing threats and to educate the staff on the appropriate mitigation strategies. Expanding on this principle by displaying information about drones and educating personnel on a corresponding mitigation strategy would help them to better respond to a potential drone incident.

'Run a drill. You don't have to have a flying object to run drill any more than you have to have a fire to have a fire drill.'[5]

Richard Lusk
Director, UAS Research Center, Oak Ridge National Laboratory

Defending against criminal or terrorist acts in the civilian domain is usually limited to passive protection measures, as businesses do not possess any (or very restricted) legal authority to employ potentially lethal force against an intruder. Apart from the external protection of the premises, additional access controls, baggage screenings or metal detectors are often used to prevent the introduction of weapons and other dangerous materials into the structure. Drones can be used to bypass these security measures and to deliver hazardous materials into the site, near the outer walls or on rooftops of a structure, where these materials may range the entire Chemical, Biological, Radiological and Nuclear (CBRN) spectrum. Similar to the aforementioned accident prevention measures, establishing shelters or evacuation points and

maintaining the respective drills can help to mitigate the effects from criminal and terrorist acts.

Indications and Warnings

Not every drone sighting is an attempt to compromise the site and spy on the business' intellectual property. Not every drone sighting is an attack. Indeed, it can be assumed that most incidents are caused by drone operators who either act carelessly or simply unknowingly violate the boundaries of a property. Drone detection systems can help to establish patterns of routine drone presence in the area and detect unusual flight activity that may indicate a potential threat.[6] Moreover, law enforcement, intelligence, and other related agencies need to provide appropriate indications and warnings to help businesses build and maintain a sufficient level of situational awareness so they can adjust their mitigation strategies against potential criminal or terrorist threats accordingly.

Threat Analysis and Risk Assessment

Threat Analysis and Risk Assessment are two sides of the same coin. To recognize potential drone threats, they first need to be distinguished from the regular and lawful airspace users. Once recognized, the drone model and its capabilities need to be identified to further proceed with a risk assessment, i.e. the evaluation of the drone's potential actions that could negatively impact the critical infrastructure's ability to operate. Without proper data put into the risk assessment, an organization is likely to remain vulnerable to their top priority threats without even knowing of their existence.

Therefore, airspace activity data must first be collected and thoroughly analyzed. Airspace activity data is gathered through de-

tection hardware, such as radio-frequency sensors, cameras, microphones, or radar. These sensor inputs are then fed into a software program, which can process the raw data and provide a situational picture over time and statistics of the respective airspace for further analysis. Emphasis is placed especially on the following statistical information:

- On average, how many drones are regularly operating in the respective airspace?
- On which days, at what time, and how long are specific numbers of drones operated in the respective airspace?
- What kinds of drones are being used?

This data helps to build a statistical drone usage profile for a critical infrastructure's airspace and its surroundings, which, in turn, helps to identify deviations from the statistical norm. These deviations are the first indicator of a potential threat. Hence, the information-gathering process is the most important, but at the same time, the most challenging step for critical infrastructure security leaders to begin. Building a statistical drone usage profile can take several months until sufficiently meaningful data is collected.

Once a solid statistical picture is available, security teams can start analysing questions, such as:

- Can drone activity be correlated with standard operational activities within the organization such as shift changes or shipping and receiving?
- Does the level of attention from outside organizations such as competitors or media change the level of drone activity?
- Are drones appearing during special events outside of normal operations, whether they be quarterly forecast meetings, prior or

during major acquisitions or announcements, or arrive when special guests are on-site?
- What are the flight patterns of the drones? Do they reveal common flightpaths or areas on the property which may require additional security?

With these insights, backed by statistical data and a solid drone usage profile, security personnel can adequately detect deviations from regular air traffic and identify potentially malicious intent of non-compliant drones.

Planning and Integrating the Countermeasures

Not every drone incident requires security teams to actively interfere with the drone or even to take it down. Simple passive measures to counter a potential threat have already been described in the previous sections. But it is important to have a drone mitigation plan prepared and exercised. It should be the norm that a drone mitigation plan is mandatory for any critical infrastructure, very much like it is required to install fire extinguishers, first aid kits, and emergency exit signs, as well as having personnel trained in emergency response or the company's data security policy.

The following passive techniques and measures may be considered when developing a drone mitigation plan.

- **Sirens, loudspeaker announcements, flashing lights:** The most actionable of all countermeasures. This strategy not only ensures that the drone pilot knows he/she has been spotted, but it also can trigger other ground support to implement further emergency or protective procedures.

- **Leading people and sensitive materials to safety:** The first action should be to minimize the risk of injury to people and/or the destruction of property, whether it be to move an outdoor gathering away from a hovering drone, or cover and hide sensitive property or prototypes from view.

- **Dispatching security teams to locate and apprehend the drone pilot:** Modern drone detection systems can not only detect a drone in mid-air, but also triangulate the location of the remote control. Security teams can use this information to get hold of the operator and hand him/her over to law enforcement authorities. The statistical drone usage profile also helps discover patterns in drone activity which highlights airspace vulnerabilities, and allows security to strategically target areas with the most drone activity.

- **Integration of IoT[ii] capabilities for automated responses:** Especially when protecting intellectual property or large groups of people, drone detection systems can be integrated into additional security technologies, such as automatically or manually deploying retractable roofs, lowering window blinds, closing doors or enabling additional physical security measures.

There are many ways that location information can be used to either locate or deter operators who are flying their drones where they shouldn't. It is well worth considering the variety of passive responses that are now possible via the integration of real-time detection data. Although it is only natural to think of defeating unwanted drones, that option is not available to most organizations.

[ii] Internet of Things (IoT). The IoT is a system of interrelated computing devices with many applications in the consumer, industrial and military domain.

However, when passive mitigation measures are not enough, and the last option is taking down unwanted drones it is essential to layout what technologies and assets are available, as many defeat systems are restricted or reserved for governmental use only. All organizations can implement defensive responses to drone incursions, but explicit legal authorities must be granted for those using offensive techniques.

As is the case with deploying a suitable detection solution, there are several factors to consider when using offensive techniques, including:

- **Physical environment:** The physical environment where mitigation is desired is the first major driver and challenge to determine mitigation options. A vast physical space, such as an airport or military installation poses entirely different challenges from a building or campus in a dense, urban environment.

- **Legal authorization for use:** Laws vary across countries for different organizations on how they can defeat drones. The US federal government specifically prohibits the interference with a drone's operation with very few exceptions. To implement offensive mitigation techniques, users need to research and understand what the legal prohibitions are and what organizations and situations are exempt from compliance.

- **Current policies and security procedures:** Some organizations already have existing policies and procedures that define how security teams will respond to reports of drone sightings. In many cases, visual identification of an incursion is first required for further reporting and action, which is often too late with

[iii] The DJI Phantom 4 Pro drone, a very common consumer model, has a top speed of 72 km/h or 20 m/s.

regard to a drone flying on average between 10 and 15 metres per second at full speed.[iii]

Offensive mitigation techniques include kinetic and non-kinetic solutions that will either 'hard-kill' (destroy the drone hardware) or 'soft-kill' (interfere with the drone software or operating system). Kinetic solutions involve some form of physical motion that interacts with the drone hardware, for example.

- Hard-Kill: Shotguns, bullets or other projectiles will destroy or damage the drone
- Soft-Kill: Net guns or net drones can be deployed to capture the drone, and keep it intact for forensics

Non-Kinetic solutions do not involve a physical motion, but rather an electronic or technological interference, for example.

- Hard-Kill: Directed-energy such as lasers and dazzlers use technology to destroy the drone's hardware
- Soft-Kill: Jamming and protocol manipulation may force the drone to land, return to home or enable another pilot to commandeer the drone and control the flight path

It is still reasonable to deploy defensive strategies first, and then escalate as needed and authorized with offensive tactics to protect assets. It should be noted that many if not all of the offensive measures are usually reserved for the law enforcement authorities. Therefore, close cooperation with the police and incorporating them into the drone incident response is often required to successfully implement an adequate drone mitigation plan.

Summary

Drones are a new tool to deliver century-old threats. Hence, it is not always necessary to develop new mitigation strategies. There are a variety of established measures which are more than adequate to counter a drone threat and which can easily be adapted and implemented into existing emergency response plans.

However, drone threats are not yet commonly recognized, and many critical infrastructures lack a drone mitigation plan. Gathering drone traffic data is a prerequisite for developing a statistical drone traffic profile which enables businesses to understand the actual scope of the threat. It should be a matter of course to have a drone mitigation plan in place, just as there is a plan for fire protection. Obviously, this also needs to be exercised in regular 'Drone Drills'.

Finally, active measures are almost always reserved for law enforcement agencies. Hence, close cooperation with the police is required to establish an adequate drone mitigation plan which can hold against even a worst-case scenario.

Endnotes

1. 'Here's how much mayhem one drone can cause flying near an airport', CNBC, 20 Nov. 2017. [Online]. Available: https://www.cnbc.com/2017/11/20/london-gatwick-airport-grounds-flights-due-to-drone-intrusion.html. [Accessed 9 Jun. 2020].
2. 'Recommendations for critical information infrastructure protection', German Federal Office for Information Security, [Online]. Available: https://www.bsi.bund.de/EN/Topics/Industry_CI/CI/criticalinfrastructures_node.html. [Accessed 9 Jun. 2020].
3. 'Critical Infrastructure Sectors', US Cybersecurity & Infrastructure Security Agency, 24 Mar. 2020. [Online]. Available: https://www.cisa.gov/critical-infrastructure-sectors. [Accessed 9 Jun. 2020].
4. 'Global Cyber Risk Perception Survey Report 2019', Marsh and Microsoft, Sep. 2019. [Online]. Available: https://www.microsoft.com/security/blog/wp-content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf. [Accessed 8 Jun. 2020].
5. 'UAS and Critical Infrastructure – Understanding the Risk (Video)', US Cybersecurity & Infrastructure Security Agency, 27 Nov. 2019. [Online]. Available: https://www.cisa.gov/uas-critical-infrastructure. [Accessed 9 Mar. 2020].
6. 'Airport Airspace Activity Study 2018', Dedrone, Jan. 2019. [Online]. Available: https://www.dedrone.com/library/airport-airspace-report. [Accessed 9 Jun. 2020].

18

By Senior Chief Inspector Jürgen Künstner, GE
By Chief Inspector Sascha Berndsen, GE
German State Police of North-Rhine Westphalia
Radio Surveillance and Counter-Drone Operations Department

By Lieutenant Colonel André Haider, GE A
Joint Air Power Competence Centre

Law Enforcement

Introduction

Today, drones have become omnipresent and are widely used throughout society. Not only are they popular products for recreation, but they are also more and more used in the commercial sector. At present, the number of drones used in Germany is estimated at more than half a million units. In addition, the portion of drones used for commercial purposes continues to increase steadily.[1] The fact that drones are spread throughout society is what makes them a challenge that reaches far beyond the military sector, and, hence, falls under the sphere of competence of national regulatory authorities – at least in peacetime.

This chapter serves to show the limitations of the individual capabilities and powers of both police and military, where civilian

and military agencies can and where they must complement one another. This chapter has been written with a view to general applicability to the extent possible. However, various national legal provisions, powers, and competences for the domestic employment of military resources, in particular, may deviate from the perspective represented within this document.

Law Enforcement Authorities and Military Powers in the Homeland and in Peacetime

Whereas International Humanitarian Law (IHL), the Law of Armed Conflict (LoAC) and, where necessary, an associated UN mandate form the legal foundation for the employment of military force between nations, the use of military assets and resources in the home country during peacetime is subject to distinctly different regulations in most NATO nations. Often, the lowest common denominator when using force of arms is the right to self-defence only.

Military Aid to the Civil Authorities

In general, the constitutions of the Western democracies allow the domestic employment of regular armed forces within a strictly limited legal framework only. However, many NATO nations have either amendments to their constitutions in effect or particular legislation that enables so-called 'Military Aid to the Civil Authorities (MACA)', 'Military Aid to the Civil Power (MACP)' or 'Defense Support of Civil Authorities (DSCA)'. As a rule, all terms denote the employment of armed forces in support of the civil authorities of a state.[2,3] The armed forces do not, in general, operate autonomously under military command but are assigned for mission performance under operational command

of the police forces to be supported or at least ordered to cooperate with them. Based on such arrangements, many countries have employed military forces in response to national crises after the SARS-CoV-2 coronavirus breakout.[4]

Military-organized Police Forces (Gendarmeries)

Many NATO nations also have military-organized police forces, so-called Gendarmeries, which belong to the military. However, in peacetime, these forces are assigned to the Home Office and assume various police responsibilities in their home countries. Gendarmeries can be found, for example, in France (Gendarmerie Nationale), Italy (Carabinieri), the Netherlands (Koninklijke Marechaussee) or Spain (Guardia Civil). In 2004, the European Gendarmerie Force (EGF) was established on the initiative of France as an autonomous supranational gendarmerie unit. Besides France, present EGF member states are Italy, the Netherlands, Poland, Portugal, Romania, and Spain.[5]

Domestic Military Operations

To counter an already increased threat situation in peacetime, several nations have established their own domestic 'operations' for their armed forces.

Operation Sentinel is a French military operation with 10,000 soldiers and 4,700 police and gendarmes deployed[6] since the aftermath of the January 2015 Île-de-France attacks, with the objective of protecting sensitive 'points' of the territory from terrorism. It was reinforced during the November 2015 Paris attacks, and is part of an ongoing state of emergency in France due to continued terror threats and attacks.[7,8]

Operation Temperer is a British government plan to deploy troops to support police officers in key locations following a major terrorist attack. It was put into effect for the first time on 22 May 2017 following the bombing of an Ariana Grande concert at Manchester Arena[9] and for a second time following the Parsons Green bombing.

Operation Vigilant Guardian was a Belgian army operation following the January 2015 Île-de-France attacks and the dismantling of a terrorist cell in Verviers[10] having foiled attacks imminent, to deal with the terrorist threat and protect the 'points' of sensitive territory. The operation was put in place 16 January 2015 and significantly strengthened during the same year, after the attacks of 13 November, notably through the implementation of an absolute emergency in the Brussels area from 21 to 26 November 2015 and after the attacks of 22 March 2016 in Brussels.[11, 12]

Military Assistance – The 'New Normal'?

As a conclusion, one can say that the employment of armed forces at home and in peacetime can be an option for protection against threats to public safety when resources and assets of the civil regulatory authorities do not suffice. For such a purpose, the established and proven approaches described above already exist and may serve as an example for potential implementation in other nations.

On the other hand, based on the lessons learned in recent history, in particular the two world wars, the separation of police and military, as well as the separation of powers in Western democracies in general, has proven to be purposeful and sensible over many decades. With a view to past crisis situations, such as natural disasters or terrorist attacks, it can also be seen that the domestic deployment of armed forces is an increasingly recurring necessity.

It should be assured, however, that these operations will not become the new standard, so that the separation of police and the military mentioned above remains clearly defined.

With regard to drone defence, it must be clarified in a timely manner at which threat level, with which military resources and under which hierarchy, military force should or may be used.

The Applicability of Military Countermeasures against Drones in the Homeland and in Peacetime

As mentioned above, the use of military force is subject to fundamentally different legal provisions in peacetime and in case of war. However, despite national differences, it can be generally concluded that domestic military operations in peacetime are subject to considerable restrictions. For this reason, the military options for drone defence and their limitations in peacetime and at home will be discussed in the following paragraphs.

Employment of Weapons

The most obvious military resource in drone defence is the use of force of arms. These assets may be, for example, air defence systems to engage the drone itself or firearms employed against the drone's operator.

The principles of the distinction between civilians and combatants and the proportionality of the resources used, as laid down in international humanitarian law (IHL), do not constitute the legal foundation in peacetime, but can by their very nature also be found in various national legislations on the use of sovereign force. For this reason, it must generally be assumed that within the

NATO community of shared values, the protection of its population has priority over all other considerations. This is in direct contrast to IHL, which allows balancing the military advantage against the collateral damage anticipated. In peacetime and at home, such balancing is not admissible and the protection of the health and life of uninvolved persons must always be given priority.

This issue places the use of potentially lethal force of arms under considerable reservations, unless other legal foundations, such as the right to self-defence, explicitly allow this use of force. For this reason, the employment of weapons in or near urban areas can be regarded as largely unwarranted, as it is not possible to exclude with certainty that uninvolved persons will not be jeopardized. In individual cases, this issue may be assessed differently with regard to the protection of remote military installations or critical civilian infrastructure that is not located in immediate proximity to the population.

Electronic Jamming

Defence action that has become a de-facto standard in both the military and police sectors in recent years is the jamming or spoofing of radio communications between drone and operator as well as drone and satellite. This 'jamming' has already proven itself in military operations against the threat of 'improvised explosive devices' (IEDs) by preventing the attacker from detonating IEDs by interrupting radio contact. Within drone defence, depending on the model, the interruption of radio contact usually results in the drone remaining in its current position, returning to its starting point, or even in the crash of the drone itself.

Wireless networks. Commercial drones use various frequency bands for their data links, including the range between 2.4 and 5.8 gigahertz (GHz). The two frequency bands are used, among

other things, for wireless network connections, which are also used by many civil authorities, industrial plants, or hospitals. For this reason, jamming measures in the vicinity of such facilities have the potential to cause considerable problems and possibly economic costs, unless very directional or localized omnidirectional radiation is being employed.

Mobile radio networks. Recent drone models are capable of using mobile radio networks to establish data connections. Electronic countermeasures in this area will presumably cause at least local communication failures in the mobile radio network affected. Since many private homes and smaller companies no longer have landline connections, emergency calls may no longer be made in the event of a mobile radio connection failure, which could indirectly jeopardize human lives.

Navigational systems. Usually, many drones use the 'Global Positioning System' (GPS) to determine their altitude and position. Due to the relatively weak GPS signal strength, the system can easily be jammed or spoofed. However, GPS does not only transmit position details but also extremely accurate time information. A variety of military and civilian applications take advantage of this. For this reason, jamming the GPS signal presumably has the most far-reaching consequences of all electronic countermeasures. Depending on the range of the GPS jammer, interference with air traffic may also be expected. Hence, cooperation with the national aviation authorities is essential in this area, since the authorities must alert manned aviation to GPS failures in cases of the compelling need to jam GPS frequencies. This procedure has already been successfully tested by the police in operational situations.

Typically, domestic frequency jamming in peacetime is subject to strict conditions and licensing requirements imposed by national

telecommunications or regulatory authorities to avoid the aforementioned implications with other users of the networks. For this reason, large-scale and continuous jamming measures in the vicinity of other network users must always be assessed with regard to the proportionality of the measure and possible failures must be communicated to the bodies concerned. If used in a target-oriented manner, limited in time and space, and above all coordinated with the civil authorities, these electronic countermeasures are an adequate means, for drone defence. It should be noted, however, that the effects of jamming are often only indirect and it is, therefore, often difficult to assess the benefit of their use.

Cyber Attacks

Electronic jamming – as described above – always requires an intervention in the civilian network structure, and negative impacts on other network users must always be anticipated. Countermeasures in cyberspace, on the other hand, can be employed in a much more target-oriented manner and possibly allow taking over and controlling the drone in question. One civilian manufacturer of drones already offers a system exclusively to regulatory authorities that is capable of tracking its own drones.[13] In most cases, such systems also allow locating the remote control so that measures against the operator can be taken as well. Military developments in this sector are based on either the voluntary disclosure of data protocols or reverse engineering of such protocols without consent provided by the drone manufacturers. Some of the latest systems are capable of filtering radio signals of known drones in a radius of more than 10 km, identify the model, read out stored details (such as the serial number), and – depending on the model – take over these drones fully automatically to, for instance, keep them outside of a perimeter, fly to a particular position or turn off the rotors and, thus, cause them to crash.

Cyber-attacks against and the takeover of drones always involves infringing on the property rights of the operator. Moreover, reading out the data memory may violate national data protection regulations. Reverse engineering of decrypted radio communication protocols will most likely violate patent rights. However, the higher precedent right to protect the health and life of the population should presumably justify such interventions. This weighing of the proportionality must, however, always be carried out with regard to the individual situation of the operations, and may require a court order or authorization.

If legally assessed and admissible, the above measures in cyberspace offer the advantage of causing the least possible impairment to uninvolved persons and the public space in general.

Potential Police Actions and Powers for Drone Defence

Police Responsibilities

The basic pillars of police responsibilities include the protection against threats to public safety, monitoring compliance with applicable laws, and law enforcement. These responsibilities are also part of drone defence.

Protection against threats to public safety. An essential element of police work is the protection of life and limb of the population. With regard to the threat posed by drones, this responsibility has most often priority in the protection of events. These may be public events, such as concerts, sports events, or demonstrations, but also closed events, such as summit meetings, expert meetings or conferences. Also, critical infrastructure and facilities that are currently in the public focus always represent

potential targets for an attack and must be protected from the threat of drones as well. Since the scope of responsibilities of the protection against threats to public safety can be compared very well with military installation defence (force protection), synergies between police and military concepts of operation and technical equipment should be identified to learn from one another and provide mutual support, where required.

Monitoring compliance with applicable law. In drone defence, this responsibility includes monitoring compliance with the relevant regulations, such as the European drone regulation, or compliance with the conditions for drone flights under national aviation law. However, in contrast to the long-established monitoring of civil air traffic, comprehensive monitoring of drone flights can only be performed in smaller areas at the moment since there is neither pertinent legislation nor general technical implementation by the drone manufacturers. At present, only one larger manufacturer offers appropriate antenna systems capable of identifying their own drones within a radius of up to 50 km.[14]

Law enforcement. Following the measures taken to protect public safety against threats and in the event of violations of, among others, the laws mentioned above as an example, the police are responsible for criminal prosecution. As a precondition for all further criminal prosecution activities, it is first of all essential to identify the owner or user of the drone. For this purpose, registration of the owner would be helpful, similar to the licensing of a vehicle by its owner. However, at present, it is usually necessary to locate the position of the drone's remote control, since the drone itself rarely bears identification marks of its owner or does not even come into the possession of the police.

Potential Drone Defence Systems in Police Operations

Not every available drone defence system is suitable or admissible for police operations. Some systems that may be used or that are already in service use are briefly described in the following paragraphs.

Radio bearing. The direction of a radio signal can be determined by means of radio bearing. Using several direction-finding facilities results in cross bearings, which can be used to determine the position of the radio transmitter. Since the drone and its remote control both act as transmitter and receiver, this technology can be used to locate the signals transmitted. From the perspective of the police, special focus is on the drone's launch preparation activities. The signals resulting from the remote control's coupling with the drone when the devices are switched on can inform the emergency services of the possible location of the drone operator, even before the drone takes off.

Radio frequency detection. In addition to the aforementioned radio bearing, the monitoring of radio frequencies received can also be used to filter out and decode typical communication signals transmitted by drones. This allows the readout of position details and other data of the drone and its remote control. The system by DJI mentioned above is partly based on this principle but uses an additional ID signal transmitted by DJI drones. Future developments might also decrypt signals transmitted by uncooperative drones and read out this information. This might be endorsed by appropriate legislation on the disclosure of encryption and communication protocols for governmental purposes.

Primary radar. In contrast to the secondary radar (see below), the primary radar actively transmits signals and is capable of locating objects in the airspace based on the reflections received. Modern

radar systems with several radar panels arranged in a circle can thus achieve coverage of 360 degrees all around and 180 degrees upwards with a range of up to 5 km. These so-called 3D radar systems have the advantage that not only the direction but also the altitude of approaching flying objects is determined. By software analysis of the radar energy reflected and the object's flight path, these radar systems are capable of distinguishing quite reliably between drones and other naturally occurring objects, such as birds or leaves.

Secondary radar. As a rule, manned aircraft are equipped with a transponder that, if available, must be used. In some areas of the airspace, such as airports and their surroundings, aircraft may only fly using an active transponder.[15] At present, there is no obligation for drones to use a transponder, and there is a general ban on flying in areas where a transponder is required. If future regulations stipulate the installation and use of a transponder or make it a precondition for the licensing of drones, secondary radars might be capable of providing a pertinent air picture to aviation and regulatory authorities. In conjunction with primary radars, uncooperative air traffic participants might be filtered out to enable further target-oriented countermeasures.

Laser-based video reconnaissance. The normal ambient lighting may not be sufficient for visual verification of objects in the airspace, in particular, for the identification of smaller drones, depending on the local conditions, e.g. in case of heavy clouds, rain, twilight, or at night. In such cases, laser-illuminating the flying object to be verified can still enable identification using a high-resolution electro-optical camera at a distance of more than 2,000 m. A precondition for this so-called laser-gated viewing is, however, target location and tracking by more traditional means of, for example, radar.

Laser defence. High-energy lasers can be used to blind the sensitive electro-optical sensor of a drone camera and if necessary, destroy it. For this purpose, the laser is scattered to generate a correspondingly wide laser field in the direction of the drone or sensor. On the other hand, a laser can also be focused on the drone in order to heat its electronics in fractions of a second to such an extent that the electronics eventually fail and the drone is destroyed. However, it should be noted that the use of a high-energy laser always involves a risk to the affected areas of the airspace, and its scattered light can be dangerous to the human eye. For this reason, the use of lasers always requires local conditions to be taken into account and cannot be realized by the police under the current circumstances.

Hunter drones. Destroying drones always entails the risk of jeopardizing uninvolved parties, e.g. through falling components or the release of hazardous substances. Hunter drones solve this problem by tracking, capturing, and transporting the drone to be repelled, usually by using a net, which can be ejected by the hunter drone. The captured drone is then transported to a predetermined position, which is typically defined in such a way as to eliminate the hazard to personnel and material. Here, further measures can then be taken, e.g. defusing of explosives, evaluation of the data memory, or determination of identification features.[16]

Problematic Issues

Due to the legal restrictions to military and police operational resources within drone defence, but also with regard to technical and operational differences, the problematic issues briefly discussed in the following paragraphs can be derived.

Protection of Domestic Military Facilities

The guarding and securing of military facilities against unauthorized entry and espionage is usually the responsibility of the military. However, traditional measures of installation defence usually aim at only securing the immediate area of the military site. In legal terms, too, the use of military force is usually limited to this area. Outside military installations, only the police are responsible for the protection against threats to public safety. However, this strict separation is not helpful in the defence against drones, as drones can easily operate both inside and outside military installations. So when it comes to the defence against drones, the question arises as to the extent to which police forces are allowed to act inside military installations, or military forces may act and possibly engage drones outside the installation. In addition, there is also the question of coordinating the measures in order not only to avoid jeopardizing uninvolved parties but, above all, to avoid jeopardizing their own personnel.

Resources Required for the Protection of Critical Infrastructure and Major Events

Even when combining all currently procured police and military defence systems, the present capacities would not nearly be sufficient for comprehensive protection against the threats posed by drones. Drone defence measures are therefore only performed selectively and based on careful threat analysis. In the event of a general increase of the threat situation and the resulting increased need for protection of civilian and military facilities, the capacity limits of all available state resources for drone defence will be exhausted quickly. For this reason, it is imperative to effectively coordinate and deploy the defence systems, which are available to only a limited extent. This raises the question of the command

relationships and directive powers among the authorities involved. There is also the question as to what extent defence systems and measures can be placed under the responsibility of state or commercial operators of critical infrastructure, and how these can be integrated into a holistic approach to drone defence.

Interoperability of the Police and Military

In order to enable joint operations, if necessary, technical interoperability of the systems used on the one hand and mutually agreed-upon procedures on the other hand are essential.

Technical interoperability. Police and military reconnaissance and defence systems are generally optimized for use under their own command and within their own network infrastructures. For security reasons, the police and military usually operate these system structures as separate and self-contained systems. For example, frequency ranges are reserved for the individual police or military use and, if necessary, secured by their own discreet encryption protocols. Some radio sets are not even designed to transmit or receive in the frequency range of the other authority. Since drone defence is still at a relatively early stage of development in both the police and the military, these interoperability issues should be taken into account in the planning phase of procurement projects. It will also be helpful to use widespread file formats for audio, image, and video files to ensure the possibility of mutual data exchange.

Mutually agreed procedures. In accordance with the military principle of 'train as you fight, fight as you train', joint measures for drone defence can only be successful if police and military operational procedures are coordinated and successfully tested together in exercises. This includes even the simplest but most

essential training contents, such as the common understanding of appropriate operational terminology.

Mutual Legal Foundations

As briefly outlined at the beginning of this chapter, the police and military operate under different legal prevailing conditions. As a rule, this also applies if the military is deployed at home on special occasions. Whereas different legal provisions do not stand in the way of joint operations, they can complicate planning and implementation. If this conflict cannot be resolved by special legislation, a jointly agreed upon regulation of competences, subordination and responsibility is imperative in order to create security of action and clarity of the available options for all parties involved.

Summary and Recommendations

Due to the widespread proliferation of drones, they must be expected to fly into military installations and critical civilian areas at anytime and anywhere – whether it be intentionally or accidentally. The number of areas in potential need of protection exceeds the resources available to the police by a considerable amount. The military can provide temporary and local support in the event of an increased hazard situation. However, the rules of engagement of soldiers and their military defence systems must be modified to reflect the legal prevailing conditions for operations in peacetime and in their home country. To improve joint drone defence between the police and the military, or in some cases to achieve it in the first place, it is necessary to procure equipment that is interoperable on a technical basis, and practice coordinated operational principles.

Endnotes

1. German Aviation Association, 'Analysis of the German Drone Market', [Online]. Available: https://www.bdl.aero/en/publication/analysis-of-the-german-drone-market/. [Accessed 7 Apr. 2020].
2. Military aid to the civil power (MACP) is the use of the armed forces in support of the civil authorities of a state. Different countries have varying policies regarding the relationship between their military and civil authorities. [Online]. Available: https://en.wikipedia.org/wiki/Military_aid_to_the_civil_power. [Accessed 7 Apr. 2020].
3. Defense Support of Civil Authorities (DSCA) is the process by which United States military assets and personnel can be used to assist in missions normally carried out by civil authorities. [Online]. Available: https://en.wikipedia.org/wiki/Defense_Support_of_Civil_authorities. [Accessed 7 Apr. 2020].
4. Louisa Brooke-Holland, 'Coronavirus: Deploying the armed forces in the UK', House of Commons Library, 20 Mar. 2020. [Online]. Available: https://commonslibrary.parliament.uk/research-briefings/cbp-8074/. [Accessed 7 Apr. 2020].
5. Teresa Eder, 'Welche Befugnisse hat die Europäische Gendarmerietruppe?', Der Standard, 5 Feb. 2014. [Online]. Available: https://www.derstandard.at/story/1389857860322/welche-befugnisse-hat-die-europaeische-gendarmerietruppe-egf. [Accessed 7 Apr. 2020].
6. Kim Willsher, 'French police search home of man suspected of driving into soldiers', The Guardian, 9 Aug. 2017. [Online]. Available: https://www.theguardian.com/world/2017/aug/09/paris-police-hunt-driver-hit-soldiers-on-patrol-levallois-perret. [Accessed 7 Apr. 2020].
7. 'Suspect in hit-and-run on French soldiers unknown to spy agencies: source', Reuters, 10 Aug. 2017. [Online]. Available: https://www.reuters.com/article/us-europe-attacks-france-idUSKBN1AQ1DE.
8. Sunita Patel-Carstairs, 'Man held after terror attack on French soldiers'. Sky News, 9 Aug. 2017. [Online]. Available: https://news.sky.com/story/french-soldiers-hit-by-vehicle-in-paris-10980625. [Accessed 7 Apr. 2020].
9. Gordon Rayner, 'What is Operation Temperer: Theresa May becomes first PM to deploy up to 5,000 soldiers on streets', The Telegraph, 24 May 2017. [Online]. Available: https://www.telegraph.co.uk/news/2017/05/23/operation-temperer-theresa-may-becomes-first-pm-deploy-5000/. [Accessed 7 Apr. 2020].
10. 'Deux ans après: l'image de la Défense améliorée par la présence des militaires en rue', RTBF, 17 Jan. 2017. [Online]. Available: https://www.rtbf.be/info/dossier/explosions-a-brussels-airport/detail_deux-ans-apres-l-image-de-la-defense-amelioree-par-la-presence-des-militaires-en-rue?id=9505164. [Accessed 7 Apr. 2020].
11. 'Notre mission en Vigilant Guardian'. [Online]. Available: https://www.mil.be/fr/nos-missions/belgique-operation-vigilant-guardian/. [Accessed 7 Apr. 2020].
12. Kenneth L. Lasoen, 'War of Nerves. The Domestic Terror Threat and the Belgian Army', in 'Studies in Conflict & Terrorism', Vol. 42, Jan. 2018.
13. 'Aeroscope', DJI. [Online]. Available: https://www.dji.com/de/aeroscope. [Accessed 7 Apr. 2020].
14. Ibid.
15. Deutsche Flugsicherung (DFS), Nachrichten für Luftfahrer Nr. 1-1011-17, 20 Apr. 2017. [Online]. Available: https://air-law.de/wp-content/uploads/2019/02/NfL-1-1011-17-Transponder-1.pdf. [Accessed 7 Apr. 2020].
16. 'Drone Hunter: The World's Premier AI-enabled Interceptor Drone', Fortem Technologies, 13 Aug. 2020.[Online]. Available: https://fortemtech.com/products/dronehunter/. [Accessed 19 Oct. 2020].

19

Courtesy of Digital Forensics Magazine
This article has been originally published in the Digital Forensics Magazine, Issue 34, February 2018.

By David Kovar, US
Unmanned & Robotics Systems Analysis (URSA)

By Joel Bollö, SWE
Micro Systemation AB (MSAB)

Drone Forensics

David Kovar and Joel Bollö explain how the growing use of Unmanned Aerial Vehicles (UAVs) creates new forensic challenges and opportunities for investigators.

Introduction

The popularity of small UAVs (a.k.a. Drones) has been surging for several years now among both hobbyists and professionals in a range of industries, producing stunning videography, superb survey maps, and an increasing tempo of interference with manned aircraft operations.

But this growth has brought risks and threats as well. Malicious actors ranging from ISIS to drug cartels to local criminal organizations

have also adopted these highly flexible and capable aircraft for their purposes. ISIS used off-the-shelf UAVs as early as 2014. A BBC article[1] suggests that Her Majesty's Prisons first saw drones overhead in 2013. A blog article[2] states that Mexican drug cartels were researching home built drones for drug deliveries in 2013 as well.

Her Majesty's Prisons reportedly investigated more than 160 drone-related incidents in the last eighteen months and a heavy lift consumer drone delivered 13 kg of methamphetamines in California late last year. A weaponized DJI Mavic was captured from a Mexican drug cartel months later.

Drones are a component in a larger system, an Unmanned Aerial System (UAS). Information relating to UAS sourcing, construction, tactics, and operations are created, stored, and transmitted throughout the UAS environment. Information resides in sensors, 'black box' log files, cell phones used as Ground Control Stations (GCS), and in NVRAM[i] on flight controllers, GPS chips and other difficult to access hardware. This data, when correctly extracted and accurately analyzed, provides valuable tactical and strategic intelligence about launch locations, flight profiles, and logistical and operational linkages.

It is important to remember that drones are not some strange new technology for which we require completely new tools and ways of thinking. Innovation is certainly required but it rests on existing forensic principles and techniques. Any drone can be broken down into component parts. Considered in this light, they are

[i] Non-Volatile Random-Access Memory (NVRAM) is random-access memory that retains data without applied power. This is in contrast to Dynamic Random-Access Memory (DRAM) and Static Random-Access Memory (SRAM), which both maintain data only for as long as power is applied, or such forms of memory as magnetic tape, which cannot be randomly accessed but which retains data indefinitely without electric power.

simply an instance of the Internet of Things (IoT) or a Cyber Physical Engineered System (CPES), a network of sensors, storage, CPUs, and actuators with network connections that enable them to share data and control information. All of these components are involved in a complex, often real time, flow of telemetry, sensor, and environmental data in clear text, binary, and encrypted formats.

The art and science of UAV forensics is at the point where mobile device forensics was 10 years ago.

So, a single drone is an IoT/CPES instance unto itself, several CPUs, a network and sensors all on board talking to external systems via network links. In most cases those external systems are a remote controller and the GCS, often a standard mobile device. Extending outward, a swarm of drones is a collection of interoperating IoT/CPES instances. To understand the entire environment we need to break all of these instances down into component parts, CPUs, networks, sensors etc., establishing a foundation, and building a complete picture from the component parts. Many of those component parts are familiar to us, particularly the mobile devices used to control the drones.

Challenges

There are a number of major challenges facing us:

- Learning what questions we can ask;
- Learning where the data to answer those questions resides;
- Learning how to extract and analyze that data;

- Learning how to present the analysis in the most efficient form for the analyst;
- Preparing for tomorrow, while answering today's needs.

For investigators and analysts working to mitigate threats from drones and utilize drone forensics in their operations, two challenges stand out:

1. We must prepare for tomorrow's threats or we will be reacting to the threats rather than proactively addressing them.

- There are many vendors other than DJI. ISIS are already using PixHawk flight controllers in their home built drones.
- Drones are part of unmanned systems. We must be able to analyze all of the components, not just the drone, or the mobile device, or the remote controller.
- Machine learning, artificial intelligence, and the use of swarms, are coming or are already in use, the classic dual use technology problem.
- 3D printing, a global supply bin, 'maker spaces', and hackers will all help enable one off, custom, or heavily modified drones that challenge our ability to extract and analyze data and other forensic evidence.
- Non-state, state, academic, and commercial organizations are all creating new capabilities and demonstrating possibilities for others to operationalize.

2. We must know what is possible to ask of the data and we must challenge vendors to enable us to answer those difficult questions.

Different cases will lead investigators in different directions obviously, but some common questions that investigators should be prepared to answer are:

- What happened during this flight? Where did it start, how high did it fly, what route did it take?
- What other flights did this aircraft perform? What other sites might have seen this aircraft?
- What are the history, flight, maintenance, software, and firmware, of this aircraft?
- Did an expert maintain it capable of modifying the firmware or hardware?
- What components of the aircraft are uniquely identifiable and traceable?
- What identifiable components, such as batteries, are shared with other aircraft? Can we link this aircraft to a larger operation?
- What other devices, services, individuals and accounts are related to this aircraft and how can we identify them? How do we reach out into social media, third party data services, and the physical world using the data on the drone?
- What questions should we be prepared to ask operators, service providers, and vendors to enhance our investigations? What can we expect them to know, and to share? How do we frame the questions to encourage an efficient and accurate response?

Where is the Data?

There are three ways of thinking about UAVs that help an investigator identify all of the potential sources of forensic artefacts. Evidence from one source will lead you to evidence from other sources. Combined, they produce a compelling picture of the immediate flight, but also of operations, logistics, and supply chain.

The three approaches are: Physical, Process, and Flow.

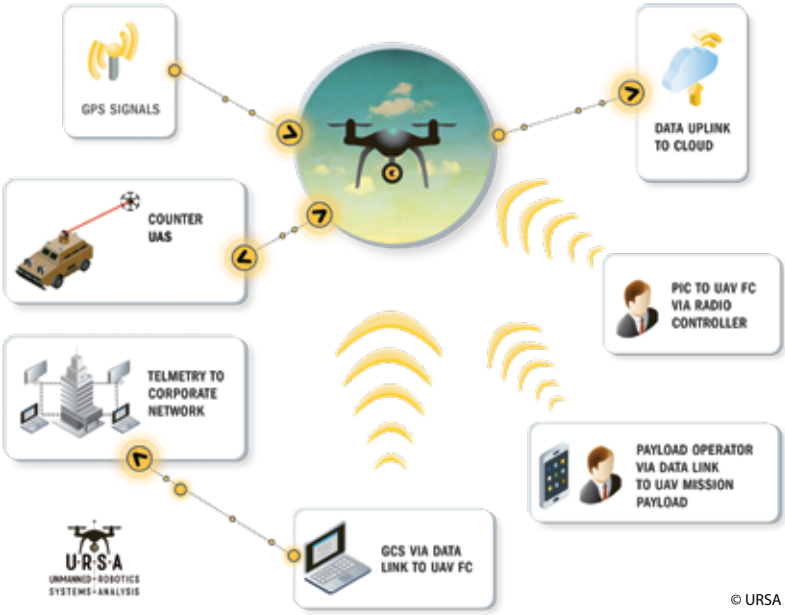


Figure 19.1: Typical UAV Deployment Scenario.

Attribution

Accessibility, availability, and lack of registration enforcement pose one of the greatest challenges to investigators. Anyone with a credit card and shipping address can order highly capable and flexible drones online with few restrictions. This is true for the common consumer drones but also for drones such as the DJI Agras MG-1 that can be purchased from Walmart or Amazon. The MG-1 has a '… powerful propulsion system that enables the MG-1 to carry up to 10 kg of liquid payloads,

Evidence is on the physical devices, the drone, the batteries, the sensor, the remote controller, the ground control station, and on any computers used to maintain the drone or process its data.

Process evidence derives from how an operator prepares for a flight, conducts it, and manages the data after the flight. The phases are:

- Mission Planning;
- Approval;
- Execution;
- Analysis;
- Delivery.

Each phase involves documentation, communication, or activity that can be collected and analyzed. Some artefacts reside on drone specific hardware or in drone specific databases but a lot of useful information is available to normal tools once the investigator knows where to look.

including pesticide and fertilizer. The combination of speed and power means that an area of 4,000–6,000m^2 can be covered in just 10 minutes'. A significant threat in the wrong hands.

Cyber Physical Engineered Systems

Cyber-physical systems (CPS) are 'engineered systems that are built from, and depend upon, the seamless integration of computational algorithms and physical components'.

Flow evidence derives from the communication between the drone, the environment, its supporting systems, and systems on the Internet. Wi-Fi traffic can be collected and analyzed, cell tower logs will support evidence of the operator's location extracted from the drone, DNS tables will show that the operator was using a specific third party drone data analysis service.

What Data is Available?

Most investigators will work with one of two primary log sources, the drone and the mobile device used as a ground control station. The drone's logs are generally very detailed, containing frequent entries from every system on the drone. The mobile device usually has a less robust version of the data on the drone but adds more information about the user's actions, such as setting waypoints and changing views in the application.

Both sources generally contain the following fundamental information:

- Serial number of the aircraft and some components;
- Version numbers for critical firmware;
- State change information such as launch/land, manual/waypoint operation, GPS available or unavailable;
- Geo-location information for critical locations – launch, land, and home point;
- Flight track information.

The onboard logs for most DJI products contain information from the following systems:

- Vision Positioning;
- Telemetry;

- Barometric;
- GPS;
- Flight Controls;
- Gimbal;
- Motors;
- Batteries;
- Message Console.

Different models and different versions of firmware will add or remove systems. For example, the agricultural model adds a sprayer system to the drone. References to it exist in some versions of the firmware even if it is not equipped.

Drones are not some strange new technology for which we require completely new tools and ways of thinking.

Collecting Evidence

Many vendors provide ready access to the onboard logs and often to the application logs as well. Access to the onboard logs is generally through a USB port on the flight controller and the logs appear in a mountable filesystem.

Older DJI models stored the onboard logs on a SD card epoxied onto the main board of the drone. For forensically sound extraction the card could be physically removed and imaged. Alternatively, the drone could be put in 'flight data mode' and the files would be available via a mountable filesystem.

In October of 2017, the log files on DJI Mavic's running the latest firmware vanished, users could no longer instruct the drone to

expose the SD card via the USB port. Investigations revealed that in newer Mavic models the SD card slots were present but empty. It seemed unlikely that DJI completely disabled such a valuable source of maintenance and failure data. Further investigation determined that the log files had been moved to storage on the flight controller and that they were no longer accessible via flight data mode.

DJI's Assistant 2 application provides some ability to export the flight logs however:

- the resulting files are sometimes corrupted;
- the process is unreliable; and
- the application reports some user activity to DJI's servers.

Missing Valuable Data

Many law enforcement agencies are currently failing to find and recover valuable evidence from drones.

Kovar & Associates purchased a DJI Mavic drone from a police auction site in the US. It arrived intact but with signs that someone had started to disassemble it but stopped. Continuing the process, we extracted an intact micro SD card and found over 30 flight logs on the card, valuable evidence of where and how it had been operated.

Many law enforcement agencies are not aware of the volume and value of data present on drones and on the supporting devices, so

DJI certainly has access to these files using in-house tools. Researchers located an exploit that provides limited access to the files.

It is expected that this change in the user's ability to access flight logs on their own aircraft will extend to some or all future models. If this trend continues, exploits may be the best option for extracting flight logs. For drones with failed electronics JTAG or chip off data extraction maybe the only option.

Log Structure

Some vendors provide flight log data on the drone in the form of CSV files. This is certainly the simplest source to work with but doesn't necessarily reflect the way that the systems actually record the data.

greater awareness is needed. Widely used mobile forensic tools like XRY and Cellebrite now support drone forensics for many of the most popular models.

Internet of Things (IoT)

The Internet of Things (IoT) is the network of physical devices, vehicles, home appliances and other items embedded with electronics, software, sensors, actuators, and network connectivity which enables these objects to connect and exchange data. Each thing is uniquely identifiable through its embedded computing system but is able to inter-operate within the existing Internet infrastructure. (Source: Wikipedia)

Two common flight controllers, PixHawk and DJI's family, write log messages from each subsystem as individual records as they come in so the structure is more similar to a network packet capture than an event log. Viewing this data as a table rather than as a series of distinct but related messages obscures valuable nuances in the data.

Her Majesty's Prisons first saw drones overhead in 2013.

DJI complicates flight log analysis by encoding each record and by not publishing the file format. Vendors developing analytical tools are further challenged by the fact that the file, record, and field formats and names change depending on the model, firmware version, and other factors. A tool that supports a DJI Phantom 3 will not automatically support a Phantom 4. Support for a Mavic Pro running today's firmware will not necessarily fully support the next release of the firmware.

Onboard versus Mobile Devices

As noted earlier, flight log data resides both on the drone and on the mobile device. The log files from vendor and third party applications are generally less of a moving target and are subject only to the access controls provided by the operating system.

Conclusion

The art and science of UAV forensics is at the point where mobile device forensics was ten years ago and will likely follow a similar trajectory with surges in understanding and capabilities offset by

development of security controls that inhibit our ability to access and comprehend the data. Drones will never be as ubiquitous as mobile devices but they will certainly play crucial roles in our society. As drones continue to advance in capabilities and come into wider and wider use by both legitimate users and by malicious actors, it is essential that law enforcement, corrections, security and military professionals increase their levels of knowledge and preparedness regarding drone threats, including the art and science of drone forensics.

Endnotes

1. 'Big rise in drone jail smuggling incidents', BBC News, 23 Feb. 2016. [Online]. Available: http://www.bbc.com/news/uk-35641453.
2. http://missouridronelaw.blogspot.com/2013/05/if-drones-are-illegal-then-only.html. [Source no longer available].

20

By Georg Schweizer, CH
Senior Consultant Mobile Security Systems
Securiton GmbH, Germany

Translated by Lieutenant Colonel André Haider, GE A
Joint Air Power Competence Centre

Cloud-based Command and Control for Security and Drone Defence Applications

Introduction

Small drone systems for private and commercial use consist of many high-tech components, offering many useful new applications for the public. However, drones are also ideal instruments for criminals and terrorists to considerably expand their capabilities. An effective defence against drones which are operated with malicious intent is therefore likely to require a similar approach utilizing sophisticated counter technology.

Today, drones are readily available to anyone and are becoming increasingly powerful. The potential, and with it the frequency, to harass, endanger and commit criminal or terrorist acts with the help of drones is constantly increasing.

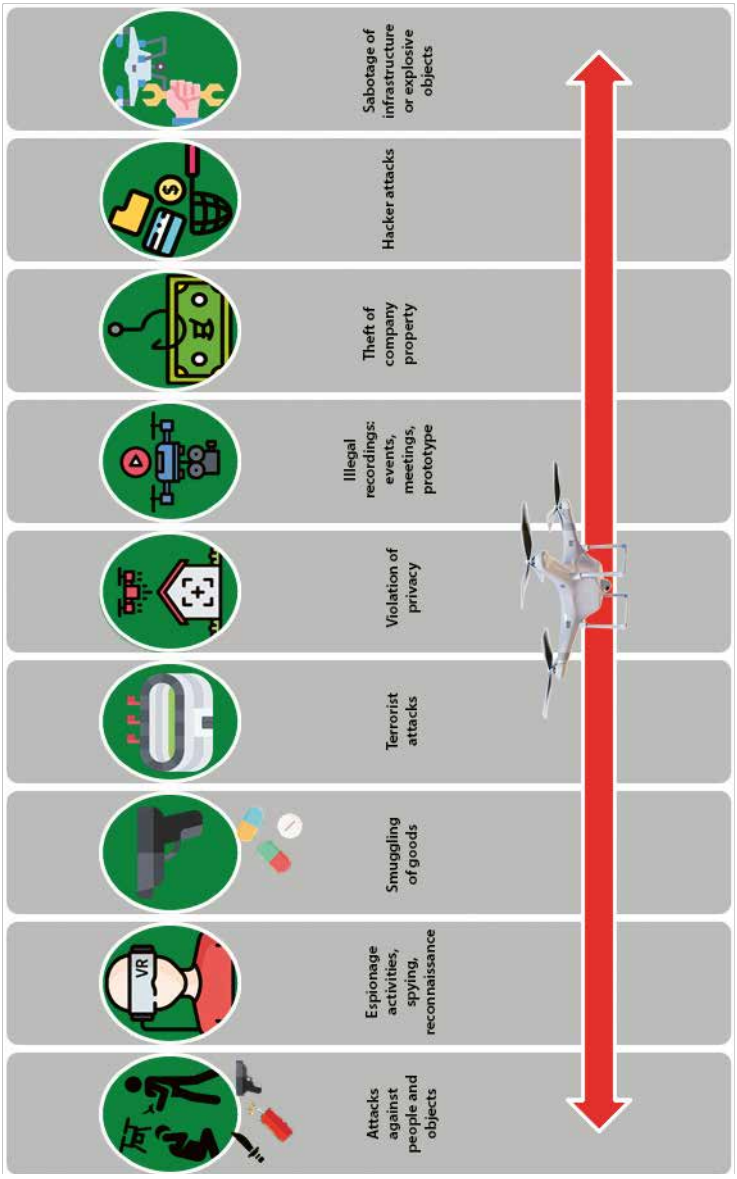


Figure 20.1: The Common Offences Using Drones

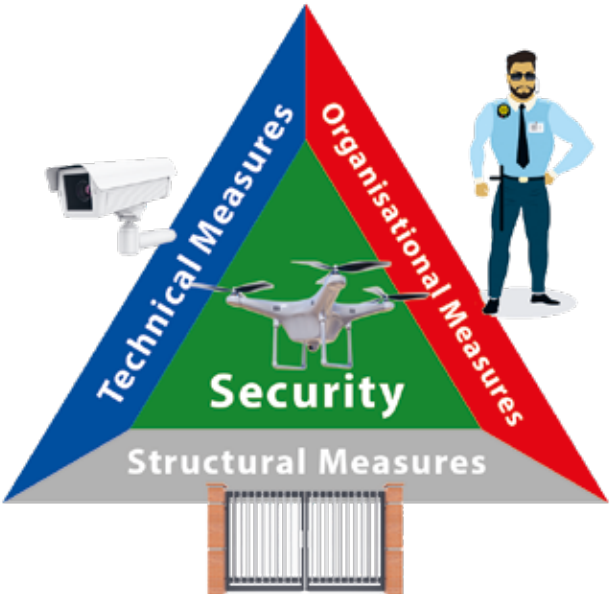


Figure 20.2: The Security Triangle

Drones allow offenders to act quickly and undetected, thereby minimizing their risk. At the same time, it is not easy for a victim to recognize a drone and immediately assess its intentions. The sudden and unexpected appearance of a drone, in the vicinity of critical infrastructures or protected persons, should generally always be considered a malicious use of a drone.

How can one protect themselves from such surprises? Are there countermeasures that are about as expensive to purchase as drone systems and that can be used swiftly and readily in any given area of application?

Traditional Protection Measures

Historically, castles or strongholds were erected (structural measures) and guards were stationed (organizational measures) to protect property with valuables and to safeguard key persons. If an important person had to leave the castle or precious materials had to be transported, they were usually accompanied by a reinforced guard force.

Today, in addition to fences, walls and protective armour, technical equipment such as fire alarms, intrusion detection systems, video security systems (technical measures) are used as aids for access control, security guards and response teams to protect critical infrastructures. The organizational measures comprise risk analysis as well as contingency plans to avert and limit damage in the event of any threat.

The highest level of security against potential threats can be achieved if all three of the above-mentioned groups of measures (cf. Figure 20.2, p. 353) are properly coordinated.

A feasible, yet cumbersome method, to protect against a drone attack, is placing people and property inside a building (shelter) and to close all entrances and windows. However, hardly any structural measures are feasible against airborne drones in the open. Organizational measures, like security guards performing airspace surveillance, are also largely ineffective against small drones, since their size, speed and mobility overstrain human eyesight, especially in the closer vicinity.

Therefore, countering drones can only be achieved using specialized technology in conjunction with the appropriate organizational provisions. It should be noted that drones may also be used while key persons are travelling, valuables are being transported,

many people are gathering at one place or while valuables or critical materials are temporarily stored in the open.

Drone Protection Technologies

A technology for protection against drones should be as fast and as user-friendly as possible and be applicable everywhere, just as one or more drones can be used quickly, easily and at any place.

Drone Detection Methods (Sensors)

To protect against drones, it is first necessary to detect them. This requires sensors like:

Radio Frequency (RF) Sensor: The RF sensor is a Beyond Line-of-Sight (BLOS) sensor that can detect drones and drone remote controls at great distances and distinguish their transmissions from the overall radio spectrum. It is the only sensor that is capable of detecting drone operations in the preparation phase, as soon as a remote control unit is activated. Smart RF sensors capture the content of radio transmissions to drones which allows for – depending on the model – identification and display of the drone model, battery charge status and maximum payload of an approaching drone. For accurate 3D target acquisition of drones, an RF sensor must have at least 2 (preferably 3) distributed 3D RF antennas in order to determine the targets' details (drones and drone controller) by means of triangulation. A single RF sensor can detect a drone at a distance of several kilometres.

Acoustic Sensor: An acoustic sensor is also operating BLOS and can detect the typical noise of a drone's propellers. However, depending on ambient noise, the detection range may be quite limited.

Radar Sensor: A radar sensor actively transmits RF energy and captures the reflected signals. This mode of operation requires LOS to the target, but it can detect drones at higher altitudes and distinguish them from other flying objects such as birds. A radar with 3D characteristics can also determine the direction to the drone target, its flight altitude and speed. Dedicated radars for drone detection are capable of sensing drones at distances of up to several kilometres. Radar sensors often require approval from the civil authorities to operate, depending on the model and location.

Image Sensor: An Electro-Optical (EO) video camera, often also combined with an infrared (IR) sensor, requires LOS to the drone and recognizes it using image processing, provided that the drone passes the camera's field of view. Special camera systems with smart video sensor technology achieve viewing angles up to 360°. A camera mounted on a Pan-Tilt-Zoom (PTZ) head is usually dependent on initial target recognition by an RF or radar sensor. However, once a PTZ video camera has locked on the drone, it can follow it autonomously and provide live images of the drone, its

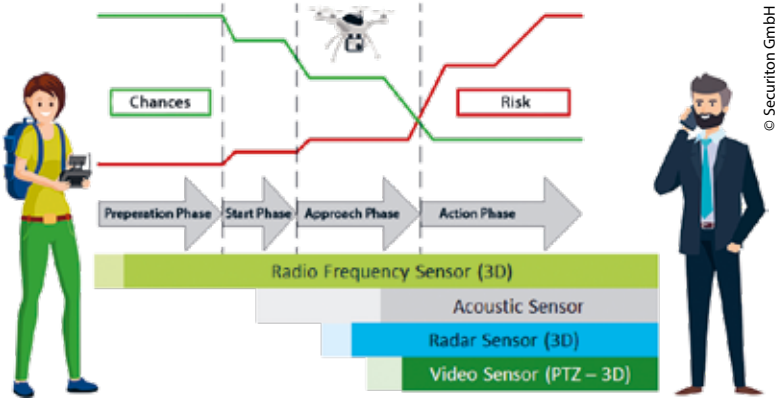


Figure 20.3: Drone Detection – Chances and Risks.

cargo and its behaviour. A PTZ high-performance camera with an AI-supported video sensor can track a drone at a distance of several kilometres and still display a recognizable image of the target.

Remote Identification Sensor: This type of sensor detects the Remote Identification (RID) signal transmitted by a drone. In addition to the unique RID, it is foreseen that drones will also be required to constantly transmit their current position, altitude, speed and flight direction. Drones with CE Class C1 - C3 are to be equipped with RID from 01.01.2021 onwards. From 31.12.2022 onwards, RID will become a mandatory standard for every drone, and older systems are to be equipped with it as well. Chapter 21 (cf. p. 375 ff.) covers these upcoming regulations in detail. If drones then have to be registered with the authorities, the registered owner of the drone can be identified through its RID. It is foreseeable that receiving drone RID signals will be supported by cell phones as well. This will enable any private person with the appropriate app to track the drone traffic in the vicinity.

This is a significant advantage not only for airspace surveillance but also for drone defence. Now, all drones have to transmit radio signals during flight and thus are identifiable by RF sensors at all times, even if they operate autonomously or on a pre-programmed flight path. Additional information about the drone can be obtained immediately once the RID transponder is in place. Drones without RID can then be distinguished from RID-compliant ones, and special attention can be paid to them.

However, even today's drones without RID, which operate autonomously or pre-programmed typically still send radio signals back to the remote control and thus are detectable by RF sensors today. This is especially true when on-board cameras transmit their video signals to the operator’s screen. Hence, since almost all drones and

their remote controls emit radio signals, RF sensor technology for the detection of these systems should always be considered as the primary sensor option. Simple yet powerful RF drone sensors are already available on the market for a reasonable investment.

In the unlikely case of a drone operating completely autonomously and without any emission of radio signals or RID, this drone needs to be treated like a flying object without a predictable flight path. For this purpose, other sensors such as radar, acoustics or video must be used in addition. However, as a general rule, more than one sensor should always be used for reliable drone detection.

Drone Defence (Effectors)

Having to counter airborne drones is literally the civilian variant of the military Air Defence mission. Although the civilian options are limited, there are several possibilities available, which are listed below:

Jamming: Since almost all drones and their controllers emit RF signals, radio interference is the most straightforward and effective countermeasure against small drones. Jamming affects the approaching drone in its communications with the drone controller or its navigation via GPS and will force the drone to initiate contingency measures, which usually leads to aborting its mission. However, interference on public frequencies is generally prohibited and reserved for the civil authorities.

Depending on the jammer, certain frequency bands or only specific frequencies can be interfered with. If the direction of approach and the communication frequencies of a drone are known, it is possible to jam the drone without overly disturbing other radio

users. However, it should be noted that some drones can automatically tune the frequency within their used frequency band in case of radio disturbance. Hence, in most cases, the entire frequency band used by approaching drones needs to be jammed.

Locating the Remote Control: Locating the remote control and thus pinpointing the operator of the drone is a highly desirable means of taking legal action against the originator of unauthorized drone activities. However, the time following detection must be sufficient for authorized security personnel to reach the location of the offender while he is still present.

Take over control: The complete takeover of a drone by security forces is feasible from a technical point of view but due to the complexity and potential legal challenges of this countermeasure, it can only be carried out with specialized equipment and only by authorized law enforcement agencies.

Hard Kill: Firing at drones using special weapons with pellets or net projectiles, laser, sound, heat or electromagnetic pulses are technical possibilities for the defence against drones. However, due to the potential hazards to uninvolved parties these countermeasures are restricted, if not prohibited, for private and commercial use and reserved solely for authorized law enforcement agencies, which are then also responsible for any collateral damage caused by their operations.

Intercept: It has already been tested to intercept drones with trained birds of prey, with varying success and always with the risk of injury to the animal used. The more effective way is probably to use sophisticated intercept drones equipped with special sensors and a net to capture small drones and transport them to a safe location. Intercept drones are already available on the market, and

due to the lower risk of collateral damage, specially licensed versions may even be authorized for use by the private and commercial sector in the future.

Many variables such as drone size, numbers, speed, distance, flight behaviour, topography, or environmental conditions can have a significant impact on the effectiveness of sensors and effectors used in drone defence. Provided that radio communication is used for almost all drone operations, the influence of the aforementioned factors on the radio frequencies used is minimal. Hence, radio communication is still the primary vulnerability of drone operations, which allows for its detection and countermeasures to be taken.

In contrast to the mere detection of drones, the possibilities for actively defending against them are very restricted for the private

© Securiton GmbH

Figure 20.4: Example of a portable, small and lightweight RF sensor and display of the model specifications of a detected drone and its remote control on a cell phone or smart watch.

and commercial sector. Unfortunately, harassment, threat or even the committing of a crime using drones can currently only be reported to the police, who will then follow traditional prosecution measures to cope with a non-traditional offence. Whether the police will be able to effectively counter drone incidents in the future is currently subject to new legislation, the provision of new equipment for police forces, the intended implementation of RID and registration of drones also supports this objective.

Command and Control

For cost reasons, small drone defence systems do not have dedicated personnel available for 24/7 operations. The reporting of detected threats as well as the activation of countermeasures must be handled via mobile devices such as cell phones or tablets, so as not to have personnel permanently tied to one location, like an operations centre. When a drone is detected, the alarm is immediately sent to one or more designated mobile devices and the person(s) concerned can then decide on any further measures that need to be taken. A minimum configuration of such a small system with a detection range of up to 2 km is depicted in Figure 20.4.

In addition to the small configuration example above, drone defence sensors and effectors can be integrated into any existing security infrastructure as well. Many larger companies have stationary alarm centres established where fire, intrusion and other alarms are centralized. Hence, it seems reasonable to integrate the alarms for unwanted or unauthorized drone incidents as well. The staff on duty can alert people affected by a drone incident, mobilize security forces, report to the law enforcement agencies, or initiate technical countermeasures.

Security Applications and the Internet of Things

The 'Internet of Things' (IoT) is a collective term for a global infrastructure of information technologies, which enables physical and virtual objects to be networked with each other and to collaborate through information and communication technologies.

Applications that are implemented with IoT technologies allow interaction between humans and any electronic systems that are connected to them as well as between the systems themselves. Embedded computers, which are continually being made smaller and smaller, are designed to support people without being distractive or even noticeable.

Mobile Monitoring, at its highest level, is the IoT of security technology. Mobile Monitoring is a collective term for temporary surveillance using mobile technical equipment. In this context, the term 'mobile' stands for being mobile and relocatable as well as for mobile (cellular) communications. Mobile Monitoring supports security companies and their staff with the surveillance of persons and objects.

Digital video and audio technology, sensors, effectors, GPS, radio systems, mobile communications, the Internet, Virtual Private Networks (VPN), mobile and cloud computing, as well as small accumulators form the basis for mobile monitoring. Many of these technologies are also in use with drone systems.

Of course, (mobile) monitoring systems can also be used for an unlimited period of time in a fixed location to protect infrastructure and personnel. Actually, most of the security systems in use today are located at only one site, and are permanently installed, with fixed cable connections for power supply and data exchange.

Examples of such isolated applications are fire alarms, intrusion detection systems, or surveillance cameras, together with their sensors and effectors. These are connected to a siren and/or a control centre, manned by personnel on 24/7 duty, who initiate the appropriate countermeasures and damage mitigation in case of an alarm.

Drone systems, on the other hand, can be considered an application of IoT technologies as well. Therefore, mobile monitoring must keep pace with, if not stay ahead of, the development of drone technology to provide a comprehensive solution for countering them.

The Advantages of IoT Security Technology

The advantages of networked IoT security technology, especially for drone defence, are:

- Sensors, effectors and devices for Command and Control (C2) that can be deployed swiftly everywhere.
- Temporary or permanent use with mobile or stationary sensors, effectors and devices for C2.
- Plug and play - easy to use with little training effort.
- Suitable for applications in personnel and infrastructure protection as well as for site security.
- Can be networked as required, also with ground-based devices, to form an all-encompassing perimeter protection system against today's known threats on the ground as well as against the new threats from the air.
- Tailored for client or mission requirements
- Inexpensive in procurement as well as in operation.
- High computing power and plenty of data storage capacity provided by cloud systems in secured data centres. Scalable in any number of sensors, effectors and devices for C2.

- Comprehensive monitoring and logging of all processes and events in data, text, audio, image or video.
- Features such as current 3D position displays and Artificial Intelligence (AI) can be made available across the board.
- Remote operations and support for reporting are possible at any time.
- The most current technology together with the latest system data and configurations of drone and drone defence technology is always available.

A drone control system has to be built only for its specific drone model. In contrast, a drone defence system needs to cope with all drone types and their control systems available on the market. This is a challenge that can only be met with networked IoT security technology, from both a technical but also a financial point of view.

Cloud-based Security

Cloud Computing is the on-demand availability of computer system resources, especially data storage (cloud storage) and computing power, without direct active management by the user. The term is generally used to describe data centres available to many users over the Internet. Large clouds often have functions distributed over multiple locations from central servers.

Cloud-based Security describes the use of cloud computing for the purpose of providing security for people and property. Here, the

[i] The Tier IV certification is currently the highest classification among data centre facilities. Tier IV data centres are considered 'fault tolerant'. Unplanned maintenance does not stop the flow of data to a data centre Tier IV. Day-to-day operations continue regardless of any support taking place.

cloud is the central element of the security system in conjunction with modern data network technology.

These security systems use corporate or private cloud systems, as opposed to a public cloud, which is accessible to essentially everyone. The technology of these two types of clouds is basically identical, the difference being only the level of the security measures implemented to protect these clouds. These security measures give only selected users and devices controlled access to the cloud, thus restricting flexibility.

Cloud computing is usually distributed over several redundant and secured data centres at different locations. A data centre in which a security cloud is hosted should be certified to comply with the following international security and Information Technology (IT) standards:

- Built and certified to Tier IV[i] standards;
- ISO 27001:2013 for highest information security;
- ISO 50001:2011 for comprehensive energy management;
- ISAE 3402 Type 2 Test Report;
- Payment Card Industry Data Security Standard (PCI DSS).
- Security Cloud applications are also characterized by:
- High-security encrypted data transmission;
- High-performance firewalls;
- Minimal latency through special routing concepts;
- Multicast capability;
- Designed to interface with various system technologies across sensors, effectors, as well as C2 centres;
- Support for all common data transfer protocols for data, text, audio, image and video;
- Fully scalable for data storage capacity and number of applications;

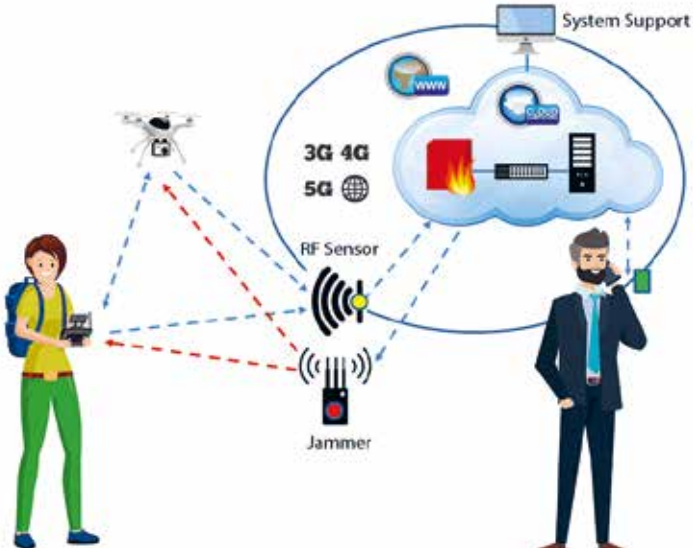


Figure 20.5: Security Cloud application using the example of a drone detection system for private or government use by a service agreement with a security provider.

- Capability to separate, manage and monitor clients and missions.

All complex technical systems in the cloud are set up in such a way that their application in the field - including the required hardware – is as simple as possible and as secure as necessary: 'plug and play' and 'easy to use' also means minimal training effort on site. In addition, being networked with the cloud's system support allows remote assistance for users on the job, if required, and keeps the entire system up to date.

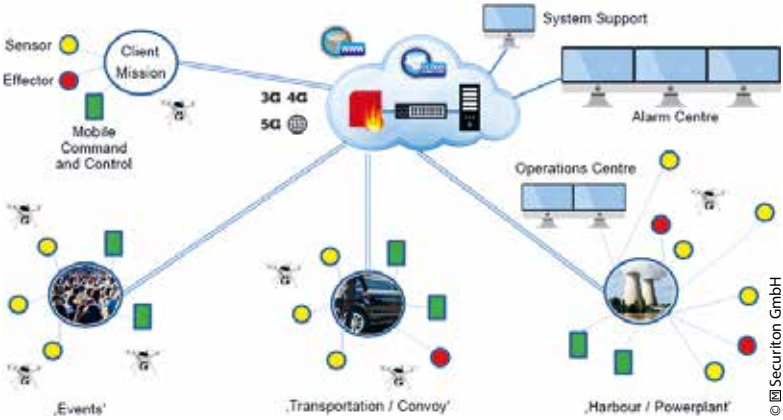


Figure 20.6: Implementation of security cloud applications on the example of drone detection and defence of a private-sector security organization or a government agency with corresponding functions from the perspective of the security cloud.

Examples of Cloud-based Security Applications

Cloud-based Security for Consumers

For private use, a consumer subscribes to a service agreement with a private security company. The security company then provides the consumer with portable RF sensors. The consumer can now use these sensors at home, in his vehicle or anywhere else he desires. Via a small portable router, the RF sensor is then connected to the security company's cloud over the cellular network. There, a user account is set up for the consumer and the secure connection with one or more RF sensors is established. Now the consumer installs an app on one or more mobile devices ('cell phones') and registers with this app on the security cloud. The application is now set up, and the consumer receives a warning whenever drones are near one of his active RF sensors.

Cloud-based Security for Government Agencies

An application for governmental use is basically identical with the private use. A government agency such as the police or the military purchase the sensors and effectors for their officials to use and the security cloud is then set up and operated by the security agency. In contrast to the private user, officials may also have the authorization to use portable effectors to counter drone threats. Examples of such an operation would be large-scale incidents, such as accidents, natural disasters, or demonstrations, where unwanted private drones would interfere with the deployment of first responders and security forces.

Cloud-based Security for Mobile Applications

For large events such as music festivals, outdoor sporting events, street protests, military exercises or police operations, mobile counter-drone systems can be installed in trailers or mounted on vehicles

Figure 20.7: Deployable drone defence system with high-performance sensors, effectors and built-in command and control centre.

and deployed to the area that needs to be protected. These systems may include a mobile C2 unit or the sensors and effectors can be connected to a remote alarm centre, both options utilizing the security cloud for event monitoring and response activation. When connected to the security cloud, security teams (with or without portable sensors and effectors) can be integrated into the system as well, so that they can swiftly respond to events wherever necessary.

Cloud-based Security for Stationary Applications

Critical infrastructure such as harbours, airports, industries, tourist attractions, stadiums, power plants, communication hubs as well as important structures of governments, militaries, or law enforcement agencies may have large and powerful sensors and effectors permanently installed and wired to the site's power and data networks. If the infrastructure has its own operations or security centre, the sensors and effectors may be directly linked to it, so that the drone situational picture would be readily available to the

Figure 20.8: 3D Drone Position Picture.

security staff. Connected to a security cloud, the drone situational picture could be transmitted to other alarm centres such as dislocated security forces or the police who may then support with emergency response or other countermeasures.

Flexibility and Scalability of Cloud-based Security Applications

Cloud-based security is highly flexible and scalable. It can easily grow with the expanding requirements of the customer, be it an individual, commercial industry or a government agency. Sensors and effectors, mobile as well as static, can be integrated as needed, even if it is only temporary. Cloud-based security allows for swiftly adapting to a developing and dynamic drone threat by providing and distributing situational awareness where it is needed while supporting centralized as well as decentralized C2 of drone defence missions as required.

Cloud-based security also offers the possibility to share sensor data, countermeasures and security personnel amongst multiple co-located infrastructure. Large commercial or industrial areas with multiple businesses may collectively set up a drone defence system with a central guard force which protects all property in the respective area. The same approach may be feasible for governmental districts in capital cities or large logistic hubs where air, water, rail, or road transport lines merge.

Summary

Today, consumer and commercial drones are readily available to anyone and are becoming increasingly powerful, making them ideal instruments for criminals and terrorists to considerably expand their capabilities.

With cloud computing and IoT technologies, security systems for drone defence can be deployed quickly, easily, anywhere at reasonable cost. This permits drone defence applications to be maintained over a long period of time, with the necessary services, and at a level of performance that can keep pace with the rapid developments in drone technology.

Part IV

Legal Perspectives

21

By Dr iur. Ulrich Dieckert, GE
Dieckert Recht und Steuern GbR

Translated by Benjamin Sauer, GE
German Federal Office of Languages

Regulatory Frameworks in Support of Counter-UAS

Introduction

Effective Defence against threats by Unmanned Aircraft Systems (UAS) requires timely detection and ranging. The determination of intended threats and unintended violations of rules and regulations is of significant importance. The technology available is prevalently more developed than the legal framework. Hence, detection and defence systems need adequate legal consideration: it has to be checked, whether the system is admissible from a legal point of view and/or whether new regulations need to be created or existing ones need to be amended.

This article will therefore mainly focus on discussing the above-mentioned questions. This chapter will first consider the current

legal framework and then move on to discuss possible future legal solutions to the questions at hand.

To avoid a detailed discussion of the respective regulations in national laws, we will focus mainly on European law, and only touch upon national law where necessary.

Subsequently a special focus beside the European legal framework will be put on those legal principles which are implemented in all democratic systems, e.g. self-defence and the legal doctrine of self-help, protection of personality rights and personal data as well as guaranteeing physical integrity and the protection of property.

Existing Legal Framework

Defence of common security and order against threats is subject to the state monopoly on the use of force and predominantly attended by (national) police organizations with support of military forces in special situations. The prerequisites for military activities for homeland security are a matter for national determination. Since this topic is discussed in another article in this book, the legal privileges and competencies will not be a subject of this article.

Self-defence

In exceptional cases, the citizen can also use force if he/she finds him-/herself in a self-defence situation. Such a situation is only, if a present unlawful attack against a legally protected right of the citizen cannot be averted in any other way.

The law recognizes various reasons for justified self-defence. These can be violations, among others, against the honour of a person,

against the general personality right, or trying to commit trespassing or criminal damage.

Especially attacks with UAS or drones deliver many threats and violations against common and individual rights, e.g. integrity of the home by unauthorized overflights or landings as well as filming or taking photos without permission. These activities can affect secrecy, economic issues as well as health and life and violate personal rights. A further example of a threat would be preparing or setting off an explosion.

Self-defence is also allowed in cases of threats against third persons' rights. This principle is called necessity as justification.

If a drone is approaching and justifying reasons can be excluded (e.g. inspection flight), as a general rule, one has to assume that a present illegal attack is underway. This is, because it has to be assumed that a violation of rights is immediately impending. A defence is justified, if it is suited to defeat the attack and it represents the least restrictive means available in the present situation. The attacked person, however, does not need to use a means he/she deems insufficient to achieve success, i.e. to defeat the attack. Because informing the respective authorities whilst a drone is approaching and asking for help will normally not work out timewise, the attacked person will regularly be allowed to use robust defences up to shooting down the drone (if he/she cannot find cover). In this situation, neither criminal damages (against the alien drone) nor tort damages are given. This is even the case, if the attacked party overreacts in his/her defence out of confusion or fear or if he/she imagines a situation that would justify a defence, but it is not proven to be the reality (legally considered a mistake in fact). Here, the behaviour cannot be justified, but is excused under the law. Seeing that targeted drone attacks are a new threat,

and further considering the speed with which they happen, misjudgements and irrational reactions are to be expected.

Nevertheless, self-defence is not a sufficient legal framework, especially for enterprises, when trying to establish regular drone defence systems. That is, because the burden of proof (i.e., that a self-defence situation existed and that the act of self-defence can be excused) lies with the attacked. Further, there is a real danger that the rights of third parties might be infringed or violated – be it due to the inexperience of the company's personnel or simply their personnel overreacting. In any case, this cannot be in the interest of the enterprise, namely for publicity reasons. Therefore, as long as there is no legal framework that expressly allows companies the operation of drone defence systems, companies should refrain from using robust defences.

Jamming

This is currently also true for the use of jammers, with which the radio contact between drone and pilot is blocked, disrupted or heterodyned to put the drone into 'fail-safe-mode', which in turn initiates an automated landing. Currently only authorities have the right to jam radio traffic under national law, and only in very narrowly defined exceptions; certainly, citizens or companies are not allowed to do so. This 'destructive use' of radio frequencies would run counter to the general principles of telecommunication law. Furthermore, such a usage would also run counter to the basic principles of the European Radio Equipment Directive 2014/53/EU as well as the Directive on the Harmonization of the Laws of the Member States relating to Electromagnetic Compatibility 2014/30/EU. These regulations demand that electrical means of production have to be designed in a way that guarantees that its electromagnetic interference does not reach a level where the normal use of other

means of production is not possible anymore. Furthermore, radio installations must not represent a danger to the health and safety of its users and third parties. Unsurprisingly, no case has come to light in Europe yet, where the use of a jammer in a civilian, private environment as a protection against drones has been permitted by the respective authorities. Additionally, a basic problem of all jamming techniques is, that its use is only effective if the drone is in remote or GPS navigation mode. In such a case, the radio signal between pilot and drone respectively the data synchronization between GPS and the drone can be detected and then jammed. If the drone, on the other hand, is used to execute a pre-programmed attack, it cannot be diverted from its pre-programmed flight path.

Preventive Systems

On the other hand, the civil usage of preventive systems, that serve to detect, verify or identify drones, is legal. Most of the models available on the market use so-called multisensor-datafusion: this system analyzes the data collected (images, audio, radio frequencies) by running it through its internal software to compare it with technical data about UASs available from a data base. Only in this way it is possible, to not only detect the approaching UAS, but also to allow to separate it from other flight objects that are not considered dangerous. As well, the so-called „drone DNA' can be identified (information regarding type, weight, possibly technical outfit and the load it is carrying).

Nevertheless, the devil is in the (legal!) details here as well. For one, preventive systems are also radio systems under European law, insofar as these devices can receive and analyze radio frequencies respectively Wi-Fi signals. Under the respective legal requirements set by the EU, such devices can only be put on the market and be operated if a conformity assessment test was conducted and the

devices received the respective CE-label. This is true for most of the systems available on the market. Because these systems do not send their own radio signals, but just receive Wi-Fi and radio signals (namely drones and their control units), they are generally in line with national rules on the allocation and use of radio frequencies.

On the other hand, when operating such devices personality rights and data protection laws have to be considered as well, if audio and video data are collected that allow conclusions as to the identity and behaviour/movements of natural persons (so-called personalized data). It should be avoided, e.g., that a drone operator enters the coverage area of a CCTV camera respectively that conversations of personnel or third parties are recorded by the device. In the latter case, there might even be legal consequences in criminal law, since it is generally prohibited by law to record or wiretap the spoken words of other persons (violation on the confidentiality of conversations). However, such potential violations of the law can easily be prevented, because video cameras as well as audio recording devices are directed toward the airspace so that the recording of personalized video images or audio material is effectively nearly impossible.

Localization and Capture of the Drone Pilot

Finally, one part of the preventive measures also is the immediate access to the drone pilot once his/her position has been localized via RF sensors (which can be done via the radio contact of the drone with said sensors). Given the relatively short-range of multi-copters, the range is probably limited to a radius of a few kilometres around the attacked object/premises. If, plant security is well-trained, and is able to move quickly, the localization and securing of the drone should only be a matter of minutes. In this way, an ongoing attack can probably be interrupted and – in any

case – future attacks by the same drone pilot, using the same drone, can be prevented.

Such infringements on individual rights are justified in most legal systems through the institute of self-help/self-defence. If an attacker is caught red-handed, every citizen is allowed to arrest the attacker for the time being -without a warrant- if the attacker could otherwise flee or prevent his identification. Furthermore, the attacked person(s) is justified in taking away an object (which could be a drone for our purposes) or in destroying or damaging the object, hence using robust force, if the following condition is met: the police or other authorities will probably not make it to the scene in time to prevent further damage or infringements to the attacked person and/or his/her property and rights. This includes the right to use direct force (physical violence) against the attacker him-/herself, if said person resisted the arrest; and the right to damage or destroy the drone or its control unit, if the risk of repeating is given. Of course, self-defence is not limitless: it is only allowed to end the immediate threat. Following this, the respective authorities have to be notified to allow them to initiate the necessary measures.

Future Regulations

As presented supra, even under the current law a number of countermeasures against drone attacks are permitted for use by not only state actors, but also by citizens and institutions. Nevertheless, there is a need for further regulations, for one in the field of detecting dangerous attacks, but also in relation to possible defences against them, seeing the steadily increasing number of drones and its potential for dangerous situations. Concerning this field, the new European drone law offers a range of regulations

which could improve the detection and drone defence against uncooperative drones in the member states if the regulations are correctly implemented.

The New European Drone Law

The EU passed two new regulations in 2019, both of which are to regulate the future operation and the technical configuration of UAS in the European member states. These regulations are based on Section VII of the EU Regulation on common rules in the field of civil aviation and established a European Union Aviation Safety Agency ((EU) 2018/1139, 4 July 2018), in which -for the first time- basic rules for UASs are identified including the authorization to pass further regulations on this basis. This refers to the Commission Implementing Regulation on the rules and procedures for the operation of unmanned aircraft ((EU) 2019/947, 24 May 2019), which defines UAS categories of operation, creates rules as to the operation of UASs, names rules and procedures for the competency of remote pilots, illustrates the allocation of operational risk and the process to receive a drone operation license and sets conditions concerning the registration of operators and flight devices, the definition of UAS geographical zones, the tasks assigned to the responsible authorities, the exchange of security information and the adjustments of approvals, declarations and certificates, which have to be met by the member states.

Concerning the definition of categories of operation and the operations allowed in these categories (open, specific and certified), the Commission Implementing Regulation on the one hand refers to an annex which contains further specifications and rules. On the other hand, this regulation refers to Commission Delegated Regulation 2019/945 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems (12 March 2019),

which deals with the technical qualities of UAS and specifications as to the equipment standards of UAS which have to be met in the respective category of operation.

Both regulations are binding in all of their parts and are directly applicable in all member states; however, for the Commission Implementing Regulation (EU) 2019/947 it was ordered that the member states be given sufficient time to establish the structures and processes prescribed in the regulation. The end of this transitional period will most likely be moved to 1 January 2021, due to the Corona virus pandemic. This time is also necessary to allow the member states to complete the mandated tasks, amongst them the future registration duty as well as the obligatory configuration of most UASs with remote identification systems and geo-awareness – both of which are important when it comes to drone defence.

Registration of UAS-Operators and UAS Requiring a Certificate

Pursuant to Article 14 of the Commission Implementing Regulation 2019/947 all member states have to create and maintain systems for the exact registration of UAS-owners and UAS subject to authorization, whose operation can create a risk to public safety, air space security, the right to privacy, personal data or the environment. They have to make sure that the systems are digital and interoperable and are enabled to allow mutual access to its respective data and its exchange via a central database. To allow for individual identification, only one distinct registration number will be handed out for each operator and each UAS that is subject to authorization.

Registration is mandatory for all citizens and legal entities that operate or intend to operate one or multiple UAS if it has a MTOM of 250 g or more, or, in the case of an impact can transfer to a

human an amount of kinetic energy above 80 Joules and/or their operation poses a risk to the right to privacy or personal data (especially if they are equipped with a sensor to capture personal data) or poses risks to state security or the environment. In the future, we estimate that more than 90% of all commercial drone operators will fall into the aforementioned categories. These drone operators have to provide the following data when registering: their full name, date of birth, identification number (legal entities only), address, email, telephone number, insurance policy number and a confirmation on the competence of the drone pilot to operate the drone. Furthermore, existing operating licenses have to be provided. The unique registration number, following successful registration, is to be placed on the drone.

Owners of aircraft which fall under Article 14 (7) of the Commission Implementation Regulation in conjunction with Article 40 of the Commission Delegated Regulation (EU) 2019/945 (12 March 2019), i.e., one, aircraft designed to transport human beings and hazardous goods, and two, aircraft with measurements (wingspan) larger than three meters that were constructed to be used in the sky above gatherings of humans and three, those falling into a special category, where the licensing process is necessary to mitigate certain risks, have to be registered by the operator by providing the producer's name, the product name, the UA serial number as well as information about the identity of the operator.

Because of this duty to register the identification of drone operators that do not stick to the rules will be easier in the near future. By using the drone registration, which must be placed on the drone (see above), deductions can be drawn as to the responsible operator respectively owner – e.g., if a damaged drone or one used in an attack is captured. However, a precondition to this is, that all states adopt suitable measures to guarantee a complete registration of all

potential operators/owners respectively all UASs subject to authorization. Furthermore, this process must be safeguarded against outside manipulation, because criminals want to avoid registering their aircraft in the first place respectively will try to achieve a registration by making false claims.

Therefore, it should be mandatory that buyers have to register digitally at the point in time when they purchase the drone, via a digital means provided by the seller. Alternatively, or additionally, producers could be forced to program the drone software in such a way that initial operation of the drone is only possible if the buyer registers with the responsible authorities first. Furthermore, it should be confirmed via a data comparison process that no cheating takes place. Finally, ignoring this 'duty to register' must result in severe penalties, starting with fines and leading up to the confiscation of the aircraft and the imposition of operational prohibitions for the future.

If we, however, allow the buyer or drone 'tinkerer', who builds his own drone, to register at will and without the option of sanctions, and if the information provided by said persons is not compared within the EU, then the logical consequence will be a registry/data base that is incomplete and, simply put: wrong, since especially those operators that want to use their aircraft to cause harm or damage, will not have been registered.

Remote Identification

Another feature which could facilitate drone detection and drone defence is the so-called 'remote identification method'. The Commission Delegated Regulation makes it mandatory in its annex that UASs (classes C1 to C4) will have to have a direct remote identification feature which allows the uploading of the

UAS-operator identification number (Article 14 of the Commission Implementation Regulation) and the exclusive compliance of the process prescribed with the registration system. It has to be especially guaranteed that during flight a series of UAS data can be transmitted directly and regularly by using an open and documented transmission protocol, which mobile phones must be able to receive. Finally, it must be guaranteed that no recipient can manipulate these data.

The data transmitted contains the following, extremely illuminating information:

- the UAS operator registration number;
- the unique physical serial number of the UA compliant with standard ANSI/CTA-2063;
- the geographical position of the UA and its height above the surface or take-off point;
- the route course measured clockwise from true north and ground speed of the UA; and
- the geographical position of the remote pilot or, if not available, the take-off point.

These data about approaching UASs, which right now can only be identified by detection systems with the right sensors by comparing data bases, will be easily available in the future. This concerns most of the devices available on the market, because only those UAS that weigh less than 250 grams, including payload (compare Commission Delegated Regulation) do not have a duty to allow for remote identification.

In the future, the person responsible for drone defence at a company can retrieve a lot of useful information out of the data transmitted. He/she can calculate the position of the UAS, its previous

flight path and the speed with which it is approaching – and therewith calculate when the UAS will enter protected air space. The geographical position of the drone pilot is of importance to plant security to catch him/her red-handed, arrest him and secure the drone and/or to hinder the continuation of the attack. Furthermore, the UAS identification number allows the identification of the responsible operator/owner, against whom tort claims might be brought.

All of this is of course based on the assumption that the drone used for an attack really uses the technology prescribed by law and does not send incorrect information, e.g., because the software was manipulated. Concerning this, it is the duty of producers in the first place to equip their devices with the respective hard- and software that cannot be manipulated by the operator/pilot. It also seems possible to install detection systems within the software that send a signal to the producer once manipulation takes place (or at the latest the next time the drone is operated). Such precautions are of course useless, if the criminal drone operator uses a drone that he/she has built – without a remote identification system (for good reason from the criminal's point of view).

In this last case, the drone provides a clear sign of its illegality simply by not sending a signal; it will therefore be recognized as a threat. Once such an illegal drone approaches an air space protection zone, it is probably sufficient from a legal point of view to assume that the conditions for self-defence are given.

Geo-Awareness

Pursuant to Article 15 of the Commission Implementation Regulation, every member state has the right to limit or prohibit the operation of drones above certain areas of its territory due to public

and air space safety reasons, hazard prevention, to protect the right to privacy or the environment. Alternatively, the state can allow operation if certain conditions or requirements are met. If the member states identify such a 'UAS geographical zone' they shall ensure that the information on the UAS geographical zones, including their period of validity, is made publicly available in a common unique digital format. Inversely, the annex to the Commission Delegated Regulation states that all UAS in classes C1 to C4 have to be equipped with a geo-awareness system, which has to have an interface through which all information on air space limitations can be uploaded and updated and depending on the geographical zone, be compared to the position and altitude of the UAS. If the system recognizes a possible airspace limitation violation, a warning notice is supposed to go out to the pilot; this is also true, if the positioning or GPS system of the UAS cannot guarantee the proper functioning of the system.

This technical feature, now incorporated into EU law and soon to be implemented by the member states, will contribute to making drone operations safer. Oftentimes even law-abiding pilots steer their drone astray and pose a risk for geographically protected legal assets. In such a case, the warning notice will lead the pilot back onto a legal flight path. If an operator or pilot, however, aims to intentionally enter a geographically protected zone, he/she will not likely be stopped by such a warning notice (if the warning notice was not already disabled). Therefore, it should be discussed whether it is possible to program virtual fences into the drone software in such a way that the aircraft is technically prohibited from entering restricted zones. Such a geo-awareness is envisioned in the annex of the Commission Delegated Regulation (concerning obligatory geo-awareness systems): If the UAS is equipped with a function that limits its access to certain airspace and frequencies, this function has to interact seamlessly with the command module

of the UAS without impairing its flight safety. Furthermore, the drone pilot has to receive clear instructions as soon as this function hinders the UAS to enter certain air spaces and frequencies.

It remains to be seen, whether the EU will come up with further mandatory provisions, or if the member states will mandate that with regard to certain areas geo-awareness systems will have to have integrated virtual fences. One will have to differentiate between permanent lines/borders (e.g., around airports or penitentiaries) and flexible lines/borders (e.g., national parks during breeding seasons). Whether or not the latter can be achieved by uploading the respective orders to the software, would have to be tested by software experts. As could be read in the press, the German federal state of North Rhine-Westphalia plans a legislative initiative to anchor geo-awareness in European law, especially for sensitive areas like penitentiaries and airports. A letter suggesting such a law has already been sent to Brussels.

Cooperation (Aiming at Increased Security) Between Operators of Critical Infrastructures with Law Enforcement Agencies

The current legal situation allows private parties/enterprises in most member states to operate drone detection systems, yet because of the state monopoly on the use of force, they are not allowed to defend themselves using effectors or jamming. Self-defence, as it is an exception to the rule, is not suited to justify the systematic operation of a drone defence system– apart from the fact that private enterprises would not be willing to buy such cost-intense defence system given the unclear legal situation.

On the other hand, law enforcement agencies, seeing their insufficient equipment, are currently hardly able to effectively protect all properties/institutions that are potentially endangered. This

concerns especially those considered critical infrastructure, such as energy, water and heat supply, telecommunications, or transportation infrastructure. If such institutions are attacked, it would not only have a tangible impact on the operator of the attacked plant, but could also present severe consequences for the general public (e.g., power plant accident). It is therefore in the interest of the state to protect such critical infrastructure.

Especially large passenger airports have moved to the fore. The incidents at London-Gatwick in December 2018 and Frankfurt in May 2019 showed how vulnerable air traffic is to uncontrolled drone traffic. It is just sheer luck that up to now no collisions between airplanes and drones have happened, and that no airplane has been brought down yet by such an incident. However, even the temporary suspension of flight operations has grave consequences; not only in economic terms for airlines and airport operators, but also for passengers whose flights are postponed or cancelled. Because of this situation, solutions must be found to deal with such problems in the future - technically and legally.

A feasible solution might be the amending of existing rules and laws to allow for an explicit conferral of responsibility for safety to the responsible bodies/institutions. For airports, this might mean that air traffic management, a state actor, would be entrusted with the task of drone detection. Since it is costly, the equipment necessary to fulfil this task should be financed by the state and/or the airport operator – both do have an interest, especially an economic one, in undisturbed flight operations. In that case, it must be mandated that findings gained by such detection operations are provided to the respective police forces, which in turn will coordinate drone defence measures with air traffic control and the airport operator. To avoid interface problems here, it would be ideal if the drone defence systems contained a subsystem that could only be

operated by airport police. Otherwise, the law enforcement agencies would need to procure their own systems, which might not be compatible with the systems bought by the airport operators. Such cooperation is of course only possible, if all participating parties agree to a financing concept – this might well be a problem in states with a federal structure.

Concerning the protection of other properties/installations of critical infrastructure, for which law enforcement cannot always be present (e.g., power plants), a so-called 'security partnership' between the operator of the plant and the responsible government agency should be installed. Most likely, plant operators will only show an interest in procuring such costly systems if comprehensive drone defence measures are possible. In such constellations, a security partnership could be organized in the following way: the operator receives a permit issued to be the responsible state agency to conduct certain, defined, active drone defence measures by him-/herself if a certain, well defined threat scenario is met. Allowing this could be achieved by transferring certain duties to the operator, if he/she is considered reliable and their personnel are trained for these situations. The state monopoly on the use of force would have to be broken, but drone defence is not about the defence against another human being, but about possible damage to an object, namely the attacking drone – which seems acceptable considering the severe consequences a successful attack could cause.

Conclusion

The current civil law allows certain protective measures and defines the requirements to gain the approval for extended countermeasures against threats delivered by UAS. It was the intention of the author to show opportunities for the cooperation of

stakeholders in two areas: one, detection and two, defence in certain scenarios as described above.

There is legal leeway for effective drone detection and defence, yet on the state side there needs to be determination to develop the law further and use the leeway available. This is especially true with regard to the new legal requirements of the EU drone regulations. The registration obligation in this new regulation, as well as the mandatory remote identification and the rule to respect certain geographical zones are well suited to separate the wheat from the chaff, i.e. to separate cooperative, legally operated drones from uncooperative, illegally operated drones. The latter group generally poses a threat to air space safety and in most cases also for public safety on the ground, especially when committed with criminal intent. In such cases, robust defences are justified, because it cannot be expected that the attacked party can question the reason for the irregular operation of a drone approaching with high speed. Furthermore, the operator/owner of the drone who does not stick to the law has to expect defensive measures by potentially endangered third parties. Whether the operation of defensive measures should remain exclusively with the governmental agencies responsible for the safety and security or whether it should be opened up to private parties via special permits (security partnership) is up for discussion.

22

By Heleen Huijgen LLM BSc, NE
By Liisa Janssens LLM MA, NE
The Netherlands Organisation for Applied Scientific Research (TNO),
Unit Defence, Safety and Security Department Military Operations

The Juridical Landscape of Countering Unmanned Aircraft Systems

Introduction

Countering Unmanned Aircraft Systems (UAS) in international armed conflict is a difficult task, since it can be hard to determine the scope of a threat. There is no single threat scenario: the threats come in various shapes, formats, and applications. A major complication in countering UAS for defence purposes is caused by emerging technologies such as autonomous applications implemented in UAS.

An example of a UAS for military purposes that makes use of advanced autonomous applications is the 'Harpy', developed by Israeli Aerospace Industries (IAI). The 'Harpy' is designed to attack targets by self-destructing into these targets or, if no target could be engaged

during the duration of the mission, return home. An undisclosed number of 'Harpy's' were bought by China in 1994. China created its own system, the ASN-301, which appears to be a near copy of the 'Harpy'; it was unveiled at a military parade in 2017. Examples of autonomous applications can be found in consumer products as well, such as active detecting, tracking and following of persons and objects, or waypoint navigation with autonomous trajectory calculation and active obstacle avoidance based on the device's sensor inputs.[1] *'Both categories, commercially available drones as well as military UAS, should be considered 'autonomous' in the way that they probably no longer require a permanent command and control link to fulfil their mission. This eliminates many of the current countermeasures which rely on jamming their radio transmissions.'*[2]

Against the background of these already existing examples of advanced autonomous applications in UAS we will focus, without delving into specific (advanced) autonomous capabilities, on countering UAS that make use of autonomous applications in general. Our point of departure is Counter-UAS (C-UAS) systems with autonomous applications within the scope of military operations for defence purposes in armed conflicts. The developments on the autonomy of UAS imply that current countermeasures, such as jamming, will not be sufficient. Moreover, time can be a factor that limits the possibility to counter UAS adequately. The difficulty to detect and determine if a UAS is being used as a weapon -in an early stage- is high, and countering a UAS is a time critical operation. It is possible that the time window to response is too limited to leave the countering task solely to a human decision-maker and therefore it might be necessary to implement autonomous applications in C-UAS operations as well.

In this chapter we investigate how the operational use of C-UAS systems is connected to the Rule of Law and International

Humanitarian Law (IHL) in general. Additionally, we will elaborate on the review process of new weapons, means or methods as described in article 36 of Additional Protocol I of the Geneva Conventions (AP I), with a particular focus on emerging technologies. We also propose some considerations with regard to the novelty of emerging technologies and how -and under which rules, regulations and procedures- new countermeasures can be shaped. We will especially reflect on how the review process of the study, development, acquisition or adoption of new means and methods of warfare, in article 36 AP I, might have to evolve with regard to C-UAS systems that make use of emerging technologies such as data- and code-driven applications. Our chapter will be divided into three sections.

In the first section, we will give a short introduction to the relevant legal framework and a short explanation of the Rule of Law. We will provide a general outline of the legal basis and the legal regime of using countermeasures for defence in armed conflicts.

In the second section, we will discuss article 36 AP I and point out some difficulties in C-UAS systems that incorporate data- and/or code-driven applications, such as machine learning and artificial intelligence. We will also reflect on the question as to whether data- and/or code-driven applications in C-UAS can be seen as *new*.

Our considerations will culminate in the third section with reflections on the acquisition procedures, which leads to suggestions for how to shape emerging technologies such as data- and/or code-driven applications and how to provide safeguards in the acquisition procedures of C-UAS systems. We place emphasis on the fact that it might be desirable to mandate a preregistration of the research design as a requirement – without disclosing classified information in these acquisition procedures – in order to provide

transparency. More specifically, we will state that transparency is needed with regard to future claims on the safety, security and reliability of such applications, while transparency is also key in enabling the contestability of decisions based on such applications in terms of potential violations of fundamental rights.

Legal Framework and the Rule of Law

The purpose of a legal system is to have rules that bind all people living in a community.[3] These rules are there to protect the general safety and to ensure that the rights of citizens are protected against abuses by other people, organizations or governments. Two basic principles of any legal system are first, to have a code of conduct that enables all relevant actors to know what their rights and obligations are, thereby enabling a more predictable and efficient interaction in any particular sphere of activity; and second, to set out norms that are considered to be essential to protect basic shared values. To find out which countermeasures can be employed in situations of an armed conflict, it is necessary to establish a legal basis and to determine the relevant legal regime. The legal basis will answer the question of whether the use of force is legal, the legal regime regulates the where, how and against whom the use of force can be employed.[4] The legality of C-UAS systems will not be discussed in front of a court, when there is no legal basis for the operational use to begin with.

Legal Basis

Jus ad bellum refers to the conditions under which a state can legally resort to the use of force.[5] The UN Charter states *'All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of*

any state, or in any other manner inconsistent with the Purposes of the United Nations'.[6] This provision is considered as binding upon all states in the world.[7] However, there are three important exceptions to this provision: (1) individual or collective self-defence, as described in article 51 of the UN Charter,[8] (2) a mandate of the UN Security Council, as described in articles 39 to 42 of the UN Charter[9] and (3) aid to the authorities of a state, in other words the use of force on the territory of a third state requested by its government.[10] When it is determined that there is a legal basis for the use of force, the next step is to determine which rules are there to obey during the deployment of C-UAS systems.

Legal Regime

In addition to *jus ad bellum*, international law also seeks to regulate the conduct of hostilities, also called *jus in bello*. This relevant legal regime is primarily based on IHL.[11] IHL limits the right of parties to an armed conflict to freely choose any means and methods of warfare.[12] There are certain principles in an armed conflict that are valid at all times and have as their purpose to strike a balance between humanity on one hand and military necessity on the other.[13] This balance is stated by the International Court of Justice as 'cardinal' principles of IHL as, inter alia, basic norms of targeting.[14] These basic norms of targeting set rules on the use of certain types of weapons. The main principles relating to targeting in IHL are (1) distinction, (2) precautions and (3) proportionality.

Firstly, in order to protect the civilian population, the means and methods used should be able to make a distinction; meaning that no civilians or civilian objects may be attacked, but only combatants and military objects.[15] As a consequence, a state is never allowed to use means and methods that are incapable of distinguishing between civilians and military targets.[16]

Secondly, precautions in attack, which entails the prohibition of the use of means and methods of warfare that are of a nature to cause superfluous injury or unnecessary suffering.[17] As a consequence, all feasible measures should be taken to avoid or at least minimize damage or injury to civilians from the effects of an attack on a military objective.

Lastly, proportionality: in attacking a military objective in situations where civilians and civilian objects are likely to be affected, the attack may not be carried out if the estimated collateral effects would be excessive in relation to the anticipated military advantage resulting from the attack. In 1996 the International Court of Justice has addressed the issue of the IHL principles in the context of the use of weapons and confirmed that these principles of IHL apply [...] to all forms of warfare and to all kinds of weapons, those of the past, those of the present and those of the future.[18]

Although the relevant legal framework of C-UAS systems -the legal basis and legal regime- is quite clear, we are questioning which problems in acquisition procedures might arise with regard to data- and/or code-driven applications. As stated in the introduction, our point of departure is the assumption that C-UAS systems are likely to need to contain these emerging technologies, since current countermeasures such as jamming will not be sufficient in some situations. *'The fact that a weapon system did not exist at the time a particular treaty rule of IHL came into force or customary international law norm crystallized into binding law does not preclude application of the rules.*'[19] To make sure that future means or methods of warfare adhere to the rules of IHL, it is necessary to have a meaningful review of these new means and methods.

Article 36 Additional Protocol (I) to the Geneva Conventions

The question of whether data- and/or code-driven applications can be seen as *'new'* depends on the role these applications play in C-UAS systems. This involves not just an understanding of the technology itself, but also of the military use of that technology.[20] If the application solely collects data, without altering the nature or content of the data, and does not further use that data, then it would not be considered as falling within the scope of means or methods of warfare. However, if the application would provide an integral part of the targeting decision process, it becomes part of means or methods of warfare.[21]

An existing legal instrument to review the legality of new weapons and weapon systems used in armed conflict can be found in article 36 of the first additional protocol to the Geneva Conventions (AP I).[22] The article states that '*In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party.*'[23] This article is an example of a provision of IHL that is also relevant and applicable in peacetime, because the process from the development to the employment of new weapons does not usually take place during the armed conflict itself. New weapons and means and methods of warfare should be reviewed with respect to meeting the IHL targeting rules *before* being employed, to ensure that these new weapons employed during armed conflict are capable of meeting the IHL targeting rules. IHL is the only legal regime that has an instrument to review new weapons. For example, there is no comparable obligation under human rights law, the legal regime which would be applicable in a peacetime situation.

Article 36 binds all parties and for all parties to AP I there is an unequivocal duty to conduct reviews of weapons that are being employed in an armed conflict. Moreover, article 36 reflects – customary law, as it is argued that the obligation of a legal review of new weapons, described in article 36 AP I, is only a codification of a pre-existing customary obligation.[24] This entails that it is a binding obligation on (nearly) all NATO members. Subsequently, there is no legal distinction between weapons used in international armed conflict, a conflict between two or more opposing states, and non-international armed conflicts, a conflict between governmental forces and non-governmental armed groups, or between such groups only.[25] In this regard, the International Criminal Tribunal for the former Yugoslavia rightly determined *'What is inhumane, and consequently proscribed, in internal wars, cannot but be inhumane and inadmissible in civil strife'*.[26, i]

Unmanned combat aerial systems are already a reality, for example the Predator and the Reaper, and can be qualified as systems that are operated remotely.[27] Given the current state of technology and the nature of the threat of a UAS, it is to be expected that some form of autonomy in C-UAS systems is necessary to effectively eliminate, for defence purposes, the threat

[i] We would like to make two side notes, firstly, the mere fact that a state is not a party to AP I, does not automatically mean that they do not conduct a review of new weapons. For example, the United States of America is not a party to AP I, but the US Department of Defence (DOD) has a longstanding policy that requires a legal review of the intended procurement or acquisition of DOD weapons. Secondly, article 36 is only applicable for weapons employed in an armed conflict, so it would be desirable that a national government creates a policy driven application, other than those who form the basis of article 36 AP I, of review of new weapons to ensure compliance with legal norms when they want to take countermeasures against UAS attacks within national security. [ref. M.N. Shaw, International law, Cambridge University Press, Seventh Edition, 2014, 5, 60; Protocole additionnel aux Conventions de Genève du 12 août 1949 relatif à la protection des victimes des conflits armés internationaux (Protocole I) ; Sipri 18.].

of a UAS. The rules of IHL apply fully on such a C-UAS system, although the means of complying with the applicable rules may differ as a result of the fact that the operator is not co-located with the system. This implies that the operator must be able to verify that the target is a military objective to a reasonable level of certainty, especially when relying upon information provided by onboard sensors.[28] Moreover, the fact that a weapon is unmanned does not relieve those who plan, decide, and execute attacks from the obligation to fully consider collateral damage in assessing the proportionality of an attack.[29]

'The transformative potential of autonomy derives, first and foremost, from the fact that autonomy can help the military to overcome a number of operational and economic challenges associated with manned operations.'[30] For instance, to overcome the problem of the short time window wherein a UAS threat should be eliminated. Moreover, autonomous applications change the means and methods of warfare on the aspects of greater speed, agility, accuracy, persistence, reach, coordination and mass.[31] It is self-evident that the same principles of the rule of targeting apply to C-UAS systems that make use of autonomous applications. This system must be capable of distinguishing between civilians and combatants and civilian objects and military objectives.[32] It might be argued that new technologies would make it easier to make this distinction, since they can be programmed to identify military targets. However, at the moment this is only possible in a limited number of circumstances; for instance, when the intended target is unmistakably military and the operational environment is predictable.[33] An autonomous C-UAS system should also be able to make some kind of qualitative assessment to determine whether an attack is proportionate or excessive in relation to the military advantage anticipated.[34]

It is questionable whether an autonomous system will be capable of assessing military advantage, since this often requires the assessment of the broader context, rather than only the physical engagement of a target. Military advantage can extend beyond the technical level, to the tactical and or even to the strategic level. A well-known example of a counter weapons system that already exists and uses autonomous applications, in order to provide military advantage, is the 'goalkeeper' of the Royal Netherlands Navy. Collateral damage in the open sea is negligible, since a ship equipped with a 'goalkeeper' is operating in an environment with few to none civilian objects. Moreover, the consequences of protection against an attack are a case of life and death, since it is the moment of last resort.

'Goalkeeper is an autonomous and completely automatic weapon system for short-range defence of ships against highly manoeuvrable missiles, aircraft and fast manoeuvring surface vessels. The system automatically performs the entire process from surveillance and detection to destruction, including selection of the next priority target.'[35]

However, in the (onshore) world with many civilians and civilian objects you will face several problems; (1) the C-UAS system deals with a highly unpredictable and complex world, where many factors have to be taken into account, (2) therefore, the data- and/or code-driven applications in the C-UAS system must be able to collect and interpret sufficient information in order to classify threats and make a distinction between civilian and military personnel and objects, and (3) even if a reliable distinction can be made, the algorithms must also be able to make an assessment of (the probability of) collateral damage resulting from engaging the threat, and whether this collateral damage is not excessive in relation to the defensive objective.

How to Provide Safeguards in the Acquisition Procedures of C-UAS Systems

'Before examining the manner in which legal reviews can be conducted it is first important to understand the process by which weapons are acquired. If the legal review of a new weapon is to have any impact on the acquisition process of that weapon, then it must not only be cognizant of the process of acquiring it, but also be a part of that process. The acquisition process is complex but can be broken down generically into several distinct phases: [...] a. concept [...], b. assessment [...], c. demonstration [...], d. manufacture [...] and e. in-service [...].'[36]

In this section we will focus on the first two phases in the acquisition process, namely the phase of the 'concept' and the phase of the 'assessment'. This specific process is not officially guided or determined by a legal process. Nevertheless, the system to be acquired needs to comply with IHL, and therefore we would like to emphasise the fact that in the case of emerging technologies such as data- and/or code-driven applications, the legal normative impact might be severe. With this taken into account it is desirable to open the dialogue with legal experts as early as possible in the acquisition process. Since as soon as functional decisions in the design are made, without a dialogue with legal experts, the review of the legal normative impact afterwards can become a difficult task since the design choices can entail a 'black box'. As a result, the aim of the operational use of these applications within C-UAS systems can become problematic, since the normative impact within the juridical landscape cannot be overseen.

'a. Concept: The military will first have to assess what the 'capability gap' is that they wish to fill, i.e. what it is that the military

wants the new system to do that its current equipment does not allow it to do. Thereafter a concept for the weapon, weapons system, platform or equipment will be developed. The acquisition process will deal with the whole spectrum of equipment to be acquired for military use, from beds to sophisticated weaponry.'[37]

We would like to point out that there exists a capability gap, since the current equipment in C-UAS systems, such as jamming, is not sufficient to counter the threat of autonomous UAS, and there is a pressing need for better defence to adequately counter these systems. The problem that needs to be solved is closing this capability gap, and the problems related to distinction, proportionality and transparency are problems that need to be focused on in the acquisition process to counter the threat of autonomous UAS, and there is a pressing need for better defence to adequately counter these systems. The problem that needs to be solved is closing this capability gap, and the problems related to distinction, proportionality and transparency are problems that need to be focused on in the acquisition process.

'b. Assessment: After the concept has been developed, it is further refined and its characteristics delineated. If the equipment being acquired is being purchased 'off the shelf', it may be possible to seek data on its performance from the manufacturer.'[38]

We would like to point out that if data- and/or code-driven applications are procurable as 'off the shelf' acquisitions, it may be desirable to include a specific review process in the pre-conceptual phase for the (research) design of data- and/ or code-driven applications, which become part of a C-UAS system, in order to be able to justify the countermeasures for defence in military operations.

Transparency of the Assessment

C-UAS systems equipped with data- and/or code-driven applications might introduce new risks regarding the decision support, due to decreased transparency on how the data- and/ or code-driven applications for decision support exactly function. It is desirable that the assessment takes place early in the development process of the concept and not at the stage when the concept is fully developed. Monitoring the research design in the conceptual development of data- and/or code-driven applications is key in order to be eventually able to adapt these applications in C-UAS systems in a responsible way. Without knowing how the analyses exactly function, these applications can become a black-box and cannot be used in a responsible way during military operations. Hence, the transparency of the data- and/or code-driven applications must be guaranteed.

The research design contains the framework of research methods and techniques chosen by a researcher. Several requirements in the process of the research design can be imposed in order to provide transparency and in the case of data- and/or code-driven applications determine the performance of a system.[39] The goal of these requirements is to ensure that such studies remain transparent and to guarantee quality of the studies. The imposed requirements make it easier to identify any research results that were found by chance. In addition, these requirements enhance the replicability, and falsifiability, of the research design.[40] Whoever procures or acquires a data- and/or code-driven application for a C-UAS should require in the acquisition procedure that the research design is preregistered (preferably with a highly trusted party). This preregistration includes the subsequent updates that were used to develop the application. This will contribute to the contestability of claims regarding the safety, security and reliability of such applications,

while also enabling the contestability of decisions based on such applications in terms of potential violations of fundamental rights.[41]

In terms of rules and regulations, there is currently no explicit legal requirement for the preregistration of research designs in the acquisition procedures of systems with data- and/or code-driven applications for military purposes. We would like to state that this requirement can also be a good example of how the review process in article 36 AP I could evolve with these data- and code-driven applications taken into account, and how these new means or methods should be designed. In the acquisition of these applications the officials should be able to review the research design of these applications, preferably via a highly trusted party, from the very first moment in the development stage to the final implementation of the application.

The preregistration of research designs would create openness regarding the processes involved in developing a data- and/or code-driven application's capabilities. This approach makes the details of an algorithm's history, including its development history, and performance clear for review during the acquisition procedure. Preregistration of the research design is required to prevent opaque data- and code-driven applications. It is important that the choice of the data, the types of error it may contain and the way it has been curated are explained in advance. The points that need to be clarified during preregistration of the research design include:[42]

- *'The type of datasets used;*
- *The relationship between training data and validation data;*
- *How frequently testing took place, and what kind of sample data were used for this purpose;*
- *How the hypothesis (about how the machine can learn most effectively) was developed;*

- *All pre-processing choices – in addition to the choice of data, this concerns the way data are cleaned up, how they are labelled, and the range of potential labels (or alternative labels);*
- *The types of algorithms used, or the use of which use is planned.*'[43]

Who Should Review the Research Design?

When autonomous applications are applied in C-UAS systems and used in military operations, these systems become part of the juridical landscape. The developments on autonomy can be traced back in applications that are data- and/or code-driven, such as machine learning and artificial intelligence. These forms of emerging technologies are becoming more and more part of our daily lives. Therefore, these developments require us to take auxiliary precautions in order to protect what is at stake: to prevent implementing opaque data- and/or code-driven applications in C-UAS systems. It is desirable to include in the review process of data- and/or code-driven applications the standard of a research design and it is recommendable to appoint reviewers who monitor the development of the research design from the very first moment in the acquisition procedure. Since transparency and classification of information are at odds with each other, these reviewers need to be highly trusted parties, who are allowed to work at the proper level of classification.

'For security reasons, such a thorough process necessarily precludes its being completely transparent. Nonetheless, for those countries conducting it, its impact is keenly felt and this must be considered a measure of its success. The answer to the need to widen implementation of the legal review process is not the creation of an international agency to conduct or monitor such reviews, but the strict adherence of States to the obligation imposed under Article 36.'[44]

It is desirable that legal experts are involved in the different phases of acquisition, even though this is not a legal process in itself. Decisions will be taken throughout the acquisition process on the basis of military requirements and commercial prudence,[45] it is highly recommended that scientists who are involved in shaping these emerging technologies and officials who lead the acquisition procedures have a sustainable dialogue guided by legal experts, in order to provide insights and theoretical reflection on the legal normative impact of these emerging technological applications.

The review of the research design can be done by a highly trusted party and a committee should be appointed with several experts from different fields, especially legal experts need to be involved in this committee, to ensure that the legal issues are addressed properly.

Conclusion

For operational efficacy, it might be necessary to deploy technologically innovative C-UAS applications that tend to use data- and code-driven applications. These applications come with the presumption, or promise, of enhancing capabilities, efficiency and accuracy to counter UAS attacks.[46] In this chapter we focused on technological developments to counter UAS within the scope of the rule of law and also on C-UAS systems via a dual analysis. The dual analysis involved a delicate balancing act; on the one hand we need -for defensive purposes- protection against the threat of UAS in armed conflicts; on the other hand, we need to counter UAS in a way that the chosen means or methods are in compliance with the existing legal framework, and safeguards values and rules within IHL. The delicate balancing act mentioned above entails that it is necessary to take auxiliary precautions towards emerging technologies in the acquisition process.

Legal aspects such as transparency and contestability within the juridical landscape, when these applications are used in C-UAS systems, are important to take into account. Several requirements need to play a role during the design phase and interrelated design choices and should be connected to the acquisition procedures of C-UAS systems.

Requirements on the design of applications are needed in order to provide safeguards which endorse legal norms and values such as contestability of the data- and/or code-driven applications in a court of law. Requirements can include, for example, the obligation that scientists who are involved in shaping these emerging technologies and officials who lead acquisition procedures have a sustainable dialogue, in order to provide insights and theoretical reflection on the legal normative impact of these emerging technological applications. It is also desirable that legal experts are consulted in an early stage of the acquisition, and that a highly trusted party will review the applications independently, since in-depth reflections on these applications and presumed accuracy are needed.

Endnotes

1. A. Haider, 'Unmanned Aircraft System Threat Vectors', in 'A Comprehensive Approach to Countering Unmanned Aircraft Systems', JAPCC, 2020.
2. Ibid.
3. What is a Law?, Judicial learning center, https://judiciallearningcenter.org/law-and-the-rule-of-law/ [visited 9-5-2020]
4. Advies inzake Bewapende Drones, Commissie van Advies Inzake Volkenrechtelijke vraagstukken, Advies NR 23, Den Haag, Juli 2013, 4.
5. M.N. Shaw, International law, Cambridge University Press, Seventh Edition, 2014, 847.
6. Article 2(4), United Nations, Charter of the United Nations, 24 Oct. 1945, 1 UNTS XVI.
7. Ibid. 5, 814.
8. Article 51, United Nations, Charter of the United Nations, 24 Oct. 1945, 1 UNTS XVI.
9. Article 39, United Nations, Charter of the United Nations, 24 Oct. 1945, 1 UNTS XVI.
10. Ibid. 5, 834.
11. Advies inzake Bewapende Drones, Commissie van Advies Inzake Volkenrechtelijke vraagstukken, Advies NR 23, Den Haag, Juli 2013, 21.

12. Ibid. 5, 861.
13. ICRC, The Law of armed conflict, basis knowledge, slide 21.
14. ICJ, Legality Of The Threat Or Use Of Nuclear Weapons Advisory Opinion Of 8 Jul. 1996, para. 78.
15. Article 41, 48, 50, 52, International Committee of the Red Cross (ICRC), Protocol Additional to the Geneva Conventions of 12 Aug. 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 Jun. 1977, 1125 UNTS 3.
16. M.N. Shaw, International law, Cambridge University Press, Seventh Edition, 2014, 861; V. Boulanin & M. Verbruggen, Article 36 Review Dealing with the challenges posed by emerging technologies, Stockholm International Peace Research Institute (SIPRI), Dec. 2017, 22.
17. Article 51 (2), 57 (2), International Committee of the Red Cross (ICRC), Protocol Additional to the Geneva Conventions of 12 Aug. 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 Jun. 1977, 1125 UNTS 3.
18. Ibid. 14, 259.
19. Gill & Fleck, The handbook of International law of military operations, Oxford University Press, 2015, 2nd Ed., 299.
20. McClelland, The review of weapons in accordance with article 36 of Additional Protocol I, IRRC, Jun. 2003, Vol 85, N 850, 405–406.
21. Ibid.
22. Article 36, International Committee of the Red Cross (ICRC), Protocol Additional to the Geneva Conventions of 12 Aug. 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 Jun. 1977, 1125 UNTS 3.
23. Ibid.
24. W.H, Parks Conventional Weapons and Weapons Reviews (2005)8 Yearbook of International Humanitarian Law.
25. How is the Term 'Armed Conflict' Defined in International Humanitarian Law?, International Committee of the Red Cross (ICRC) Opinion Paper, Mar. 2008, p.1.
26. Prosecutor v Tadic, No IT-94-1-I Decision on Defense Motion for Interlocutory Appeal on Jurisdiction, para 119, 127 (ICTY) (2 Oct. 1995).
27. Ibid. 19.
28. Ibid. 19.
29. Ibid. 19.
30. SIPRI, 18.
31. SIPRI, 18, 19.
32. Ibid. 19, 301.
33. SIPRI, 21.
34. SIPRI, 21.
35. Thales, Goalkeeper, www.thalesgroup.com.
36. The review of weapons in accordance with Article 36 of Additional Protocol I, JUSTIN MCCLELLAND, 401–402.
37. Ibid.
38. Ibid.
39. Hofman, Sharma & Watts, Prediction and explanation in social systems, 2017, Science, 355, 486–488.
40. Essential Health & Safety Requirements For Industrial Machines Equipped With Machine Learning, Jansen, Steijn, Beek, Janssens, Kwantes, Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference.
41. Ibid.
42. Ibid.
43. Ibid.
44. The review of weapons in accordance with Article 36 of Additional Protocol I, JUSTIN MCCLELLAND, 415.
45. Ibid., 401–402.
46. SIPRI, 19.

References

Books

- Gill & Fleck, The handbook of International law of military operations, Oxford University Press, 2015, 2nd Ed.
- Shaw, International law, Cambridge University Press, Seventh Edition, 2014

Articles

- ICRC, How is the Term 'Armed Conflict' Defined in International Humanitarian Law?, International Committee of the Red Cross (ICRC) Opinion Paper, Mar. 2008
- Boulanin & Verbruggen, ARTICLE 36 REVIEWS Dealing with the challenges posed by emerging technologies, Stockholm international peace research institute, Dec. 2017
- Haider, 'Unmanned Aircraft System Threat Vectors', in 'A Comprehensive Approach to Countering Unmanned Aircraft Systems', JAPCC, 2020
- Hofman, Sharma & Watts, Prediction and explanation in social systems, Science, 355, 486-488, 2017
- Parks, Conventional Weapons and Weapons Reviews (2005) Vol. 8, Yearbook of International Humanitarian Law
- McClelland, The review of weapons in accordance with article 36 of Additional Protocol I, IRRC, Jun. 2003, Vol 85, N 850.
- ICRC, How is the Term 'Armed Conflict' Defined in International Humanitarian Law?, International Committee of the Red Cross (ICRC) Opinion Paper, Mar. 2008

Conventions

- United Nations, Charter of the United Nations, 24 Oct. 1945, 1 UNTS XVI
- International Committee of the Red Cross (ICRC), Protocol Additional to the Geneva Conventions of 12 Aug. 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 Jun. 1977, 1125 UNTS 3
- Protocole additionnel aux Conventions de Genève du 12 août 1949 relatif à la protection des victimes des conflits armés internationaux (Protocole I)

Judicial rulings

- ICJ, Legality Of The Threat Or Use Of Nuclear Weapons Advisory Opinion Of 8 Jul. 1996 – International Court of Justice
- ICTY, Prosecutor v Tadic, No IT-94-1-I Decision on Defense Motion for Interlocutory Appeal on Jurisdiction (2 Oct. 1995). – International Criminal Tribunal for the former Yugoslavia

Websites

- Thales, Goalkeeper, www.thalesgroup.com [Accessed 15 Jul. 2020]
- What is a Law? Judicial learning center, https://judiciallearningcenter.org/law-and-the-rule-of-law/ [Accessed 9 May 2020]

Other

- Advies inzake Bewapende Drones, Commissie van Advies Inzake Volkenrechtelijke vraagstukken, Advies NR 23, Den Haag, Juli 2013
- International Committee of the Red Cross, The Law of armed conflict, basis knowledge [Accessed 21 Jul. 2020]

23

By Dr Christian Alwardt, GE
Institute for Peace Research and Security Policy
at the University of Hamburg

Arms Control of Unmanned Weapons Systems: Facing the Challenges

Introduction

Research and development within modern information technologies has resulted in rapid technological progress that is also reflected in the strategic and tactical considerations of military and security policy decision-makers. Efforts to advance the automation and digitalization of warfare can be observed in a growing number of countries over the past few years. A prominent example of this trend is the development, procurement and employment of Unmanned Weapons Systems (UWS). Today, especially Unmanned Aircraft Systems and drones are becoming more and more widespread and commonly used throughout the international community as they are setting the pace for progress. Aside from the military advantages that can be expected, UWS also raise a number of

new issues with regard to the danger of armament dynamics, as well as the destabilizing effects of these weapons, and their legitimacy under international law. How should the advantages and disadvantages of UWS be balanced, and how could adverse consequences be limited? Due to their specific nature, UWS pose a challenge for international arms and export controls.

UWS are highly complex and comprised of a variety of technological components. It is no longer hardware alone, but to an increasing degree system control software, the interaction with external infrastructure, and the synergies resulting from the interaction of various technological components that decisively define the military capabilities of unmanned systems. Thus, military effectiveness arises rather from 'system complexity' and is less due to the individual components of an unmanned system. Most of the technological components of UWS are so-called dual-use technologies, which predominantly originate from civilian developments. The proliferation of this civilian dual-use technology and its military employment is very difficult to regulate or track, which poses significant problems for export control measures. On the other hand, fully civilian unmanned systems can also have the potential for military applications and, possibly following some modifications, could be employed as weapons carriers. Only a few unmanned systems have unique and unalterable military attributes, or a design that obviously implies that they are purely used for military purposes (an example would be the X-47B prototype of a stealth drone). High payload capacities of unmanned systems used to be a reliable indication of an intended armament and military employment. However, many of the civilian systems are now also designed in the first place as carrier systems with high payloads, which is mainly due to their increasingly broad range of tasks, such as scientific research and the transport of goods. Obvious indications for the military employment of an unmanned

system would be existing armament, weapons stations, respective targeting systems, or attack control software. However, sometimes it is possible to simply remove or replace weapons payloads and software, so that only an individual snapshot of the system's actual configuration may point towards the intended use of an unmanned system. By taking such measures, military unmanned systems could also be concealed as civilian systems, for example. A purely external, unambiguous distinction between civilian and military unmanned systems is therefore considerably exacerbated by their system complexity and dual-use character.

With absolute certainty, the military character of some unmanned systems will probably only become apparent through their use and the resulting effects. Such a potential 'military indeterminacy' of unmanned systems confronts the traditional verification approaches of arms control with almost insurmountable obstacles, and an apparently continuous verification of unmanned systems for their civilian or military character by using the existing instruments seems impossible or infeasible. So far, traditional arms control has been based mainly on the numerical, regional, and type-related limitations of clearly defined and unambiguously identifiable weapons categories. In most cases, verification of arms control agreements was performed by detecting and counting weapon systems. By using such traditional instruments of arms control, it will be possible to detect UWS today only if they expose unique and unalterable military characteristics, as it is the case for, e.g. manned tanks, combat aircraft, or warships.

For this reason, arms control of modern UWS has to face new requirements, and thus, is in need of conceptual adaptations. Proven approaches should be adapted to the extent possible, and supplementary instruments should be developed where required. New ideas must be elaborated, and creative solutions applied. With

regard to UWS, future arms control must, on the one hand, cope with the dual-use issue and address the blurred borderline between civilian and military systems, and, on the other hand, must be flexible enough to respond to new technological development trends. It is becoming apparent that in the future, software (e.g. program codes, algorithms, data) will affect and define weapon systems performance more greatly than hardware. In conjunction with this knowledge, a critical consideration of the potential impacts of increasingly software-supported decision-making processes, which will be a consequence of increasing automation, is strongly recommended. In this context, the risk of a possible loss of human control over future UWS requires special attention, which must be considered with regard to both the provisions of international humanitarian law and the security policy implications of these weapons.

Arms and export control are still limited, particularly regarding the various software components of modern weapons systems. As yet, there is a lack of reliable instruments that can be used to regulate and verify software codes, algorithms and data sets, and that are capable of gaining international consent. Very similar circumstances and also overlaps can be seen with regard to arms control efforts in the cyber domain and in space. In all these fields, arms control research and the international discourse by experts are only just beginning, and have to this point received too little attention.

Above all, there is still a lack of international awareness of the risks and security policy implications of UWS. In this regard, the essential lessons from the East-West confrontation era should be recalled: On the one hand, the negative lessons learned and hazards that originated from the arms race and the potential for military escalation. And on the other hand, the stabilizing value and mutual benefit of cooperative arms and export controls. Both aspects must be likewise taken into consideration, so that a serious

interest by all parties in regulatory measures within the field of UWS may evolve.

The path to the future regulation of UWS is a rocky and challenging one. Coordinated cooperation within the community of nations, under participation of decision-makers, technological experts and scientists, will be vital to achieving that objective. In the course of this process, regulatory approaches developed, negotiated and decided on the basis of international discourse must be repeatedly put to the test. The leap of faith provided within the scope of arms control agreements must be substantiated by agreed and reliable verification instruments.

For such a future arms control process, the underlying challenges, preconditions required, and some bold starting points will be outlined below.[i]

Strengthening the International Discourse and Establishing the Required Basics

As a subject, UWS are 'difficult to grasp'. So far, there has been no generally accepted definition or classification nor is there a clear civilian-military distinction of unmanned systems. The international discourse on the future military employment of UWS, the resulting risks, consequences as well as the regulatory need has come to a standstill. The causes for these difficulties lie, among others, in:

- the dual-use character of the individual technological components;

[i] The following sections are based on considerations of the author, which were first published in: Alwardt, Christian. (2019). Unbemannte Systeme als Herausforderung für die Rüstungs- und Exportkontrolle. In: Werkner IJ., Hofheinz M. (eds). Unbemannte Waffen und ihre ethische Legitimierung. Gerechter Frieden. 85-109. Springer VS, Wiesbaden.

- a missing basis of information – such as insufficient knowledge of characteristics, synergies, and capabilities originating in the underlying technologies;
- the use of different terms and notions;
- deviating political interests that in some cases contradict the regulatory efforts.

A mutual understanding of what, on the one hand, defines UWS in a broader sense, and on the other hand, how they might be more easily classified would be an important foundation and precondition for a purposeful international discussion on arms control and the non-proliferation of UWS. A discourse on the conformity of fully autonomous weapons systems with the international humanitarian law has been ongoing since 2014 within the scope of the UN Convention on Certain Conventional Weapons (CCW). This discourse, however, has also been characterized by the difficulties described above. A broader international debate on the peace and security policy implications of these weapon systems is still pending. At the beginning of such a debate, awareness must be raised, whether and to what extent, today's and/or future UWS will impact international security, jeopardize regional and/or strategic stability, and expedite armament dynamics. A comprehensive international consensus on the type and effects of the negative consequences which may be associated with the increasing proliferation and employment of UWS will be the basic precondition and motivation to commence future negotiations on arms and export controls, and to later promote them successfully.

Verification: Arms Control is Particularly a Matter of Trust

The success of arms control significantly depends on the contracting nations' trust in compliance of the agreements made and their

verifiability. For this purpose, it is essential to clearly determine in advance what exactly should be regulated, and how this can be validated. This is the traditional approach within arms control.

However, considering the missing definitions and clear civilian-military distinctions, this proves to be difficult with regard to UWS. Reliable verification of the quantity of unmanned weapons is barely possible in this manner. The military characteristics of unmanned systems are also difficult to validate as they are less linked to distinct military attributes but rather emerge from the interaction of various dual-use technologies, the system software in particular. With regard to weapons systems, this dual-use issue is not a new one, however, as it relates to unmanned systems, it is particularly severe. Distinct identification of certain UWS and verification of their military capabilities (such as the level of automation or the abilities to get a situational picture) are yet unresolved problems that require new approaches as well as an increased awareness of the problem space itself.

On the one hand, in order to identify appropriate starting points for future arms control and (technical) verification instruments in the area of unmanned systems, knowledge and understanding of software technologies and their increasing share in the build-up of capabilities and the automation of unmanned systems must be consolidated. On the other hand, the potential paths of conversion of civilian to military unmanned systems should be mapped and analyzed in technological terms. In this way, essential insight may be gathered as to where future regulatory and verification measures can best be applied.

A potential solution might also be to conduct 'in-depth' examinations, which could lead to more detailed detection and analysis of the individual system components – maybe even of the system

software. Based on this, more accurate conclusions might be drawn as to the military potential and the characteristics of an unmanned system. However, the fact that nations want their weapon systems to be understood as 'black boxes' within the scope of arms control – means, they do not allow profound insights into the system or its functioning – makes a broad acceptance of this type of verification seem unlikely. Moreover, such time-consuming verification might quickly reach the limits of its feasibility in case of a large number of systems to be verified.

Further, discourse on arms and export control of UWS should not pause simply because there are no reliable verification instruments yet. In order to counter the dilemma of confidence, at least in the beginning, and to advance the discourse, voluntary transparency measures carried out by those states developing and/or operating UWS could be an interim solution to establish confidence.

Helping to Resolve the Conflict Between 'Autonomy' and 'Control'

In the course of nearly any discussion about the future development of UWS, the terms of 'automation' or 'autonomy' are used at some point and the conditions for adequate 'human control' are debated. There is no international consensus today as to what is meant by 'autonomy' or 'human control', nor as to which system functions these concepts apply and, above all, how they relate to one another. It seems obvious that there is a conflict between the concepts of 'autonomy' and 'control'. Any attempt to clearly define these terms on an international level and in a manner generally applicable to UWS failed thus far and seems to be a hopeless pursuit in moving forward. Instead of continuing to focus on terminology, the discourse on UWS could also be based on potential

scenarios of deployment. Such a scenario, for example, could be drawn on the following four factors, each to be assessed in relation to the weapons system used and to be weighted with respect to one other:

[F1] the technological capabilities of the weapons system (determined by hardware, software, and supporting infrastructure);
[F2] the operational context (objective and sturdiness of the military operation);
[F3] the complexity of the operational environment (such as battlefield or dynamic urban environment);
[F4] the level of human control (e.g. with regard to system guidance, the generation of a situational picture or dedicated decision processes, such as target selection and weapons employment).

By analyzing the combination of these different factors, the objective would now be to identify deployment scenarios that are problematic on legal, ethical or security policy levels, and to regulate them accordingly. An example scenario would be the employment of an UWS featuring only simple sensor equipment and limited analytic computing performance (F1) that should be used to identify and eliminate enemies (F2) in an urban environment (F3), but is not operated or monitored by a human operator at the same time (F4). Now, the question arises whether a problematic scenario of deployment will emerge from this combination of factors, and if so, how could such a scenario be avoided by applying specific regulations?

Such a scenario approach requires detailed elaboration, and in particular, must be feasible. Preliminary work that might be helpful with regard to assessing and describing the factors has already been done.[1] Building upon this, it may be possible in a second step to better comprehend the conflicting relationship of autonomous

acting and 'human control' of unmanned systems, and to differentiate operational forms of 'autonomy' from one another without getting lost in rigid definitions. In addition, it might be possible in such a manner to find feasible solutions that may serve to ensure the required measure of 'human control' for unmanned systems.

Traditional Arms Control – Regulation of Today's and Consideration of Future UWS

In the past decades, arms control of conventional weapon systems and weapons of mass destruction had been subject to a number of bilateral and multilateral arms control treaties. For example, strategic nuclear weapon systems were limited (New START treaty),[2] carrier systems were disarmed (INF treaty),[3] or conventional weapon systems were limited in terms of their numbers and locations of employment (CFE treaty).[4] There are also a number of transparency- and confidence-building measures, such as the Vienna Document or the UN Arms Register.[5] In most cases, these treaties do not explicitly distinguish between manned and UWS, which means that – at least in theory – they are applicable to today's UWS. Unfortunately, these traditional arms control agreements have been increasingly questioned for some years now; once pioneering and successful agreements such as the CFE treaty or the INF treaty are already a matter of the past. Nevertheless, today's UWS should be examined with regard to the options for their regulation in terms of traditional arms control. In case of the agreements still in existence, doubts as to their scope must be eliminated and, where necessary, specific additions to today's UWS must be made. Although this step may initially only be successful with regard to those UWS that have a clear military typology (main weapon categories, such as tanks, combat aircraft), it would be an important measure to strengthen the overall basis of trust in conventional arms control. Within the framework of current efforts to revive conventional arms control,

e.g. in the form of a CFE successor agreement for Europe, current and future UWS must be addressed from the outset. The issues that will arise in connection with the dual-use character of the underlying technologies and the issues in differentiating between civilian and military unmanned systems, but above all whether and how conventional arms control can keep pace with technological developments in the future must be clearly addressed in this instance. Within the scope of nuclear arms control, for example, in the negotiations on an extension of the New START treaty or a successor agreement, new unmanned carrier systems or future hypersonic weapons must be taken into consideration in addition to existing carrier systems, such as strategic bombers and ballistic missiles.

With development and automation progressing, UWS will no longer fit specified frames as clearly as previous main weapon categories. In addition to the dual-use issue, the reason for this is their non-physical military potential, which will be determined less by hardware and more and more by software and networking features. For this reason, the categorization of weapons systems would have to be re-considered to take these additional criteria into account, and to be able to design new types of verification measures based on them.

Arms control could increasingly move towards regulating military potentials as a whole instead of the number of previously defined major weapon systems as in the traditional sense. To this end, unmanned systems would in the future have to be categorized on the basis of their individual military capabilities and characteristics in order to determine their individual military potential. Such an assessment would be possible by examining their design and technological components. Conclusions could be drawn on (1) general performance parameters (velocity, agility, range), (2) armament capacity (depending on design and payload), (3) special military characteristics (stealth, armour) and (4) the individual degree of

automation or autonomy (based on software, sensor technology, data links). However, it seems rather unlikely today that nations will grant such deep insight into their military systems. Conclusions on the military potential could also be drawn by performing an external inspection of the unmanned systems (with regard to design, size, special characteristics) and a systematic demonstration of their capabilities. One approach to this could be a 'Weapon Review Process' developed and standardized on an international level, as is already in place in many cases on a national level. In this manner, however, the capabilities and characteristics of unmanned systems could only be estimated by tendency, and there is generally a very high potential for deception. It is also not clear yet how individual capabilities would have to be evaluated, or how military potential would ultimately be calculated. It will not be possible to assess the software capabilities of an UWS from the outside. In addition, such an approach would probably require a very large number of single unmanned systems to be examined and verified individually for their capabilities and characteristics, which would quickly push arms control to its capacity limits. So far, traditional arms control will probably only be feasible with regard to UWS if military potentials can be clearly identified on the outside and verified with existing methods, but this issue should not prevent us from 're-thinking' arms control.

Developing New Approaches to Regulation

Traditional arms control must be extended by new approaches to meet the new challenges. Rules of engagement for UWS applicable throughout the world might be a reasonable and effective addition to arms control. The particular attraction of such rules is that they would not be applied directly to an unmanned system or its individual technological components, but would regulate the use and operational context of unmanned systems in general, with the objec-

tive of regulating certain military effects. Such an impact- and context-based regulation would not be confronted with the dual-use issue and the difficulties of categorizing UWS. An international arrangement on clear rules of engagement could thus help contain the potentially destabilizing effects of the use of unmanned systems in terms of arms control. On the one hand, the result of such rules could be the deceleration of machine-based decision-making processes with regard to certain military operations, which would otherwise be too dangerous to rely on being time-critical. On the other hand, it could be agreed that certain analysis processes, conclusions or decisions will be reserved for human beings only, that operation with UWS in urban areas will be restricted, or that military operations must take place exclusively in a battlefield environment. There are three potential categories for rules of engagement: (1) spatial restrictions in deployments, (2) operational restrictions in deployments, and (3) capability restrictions. Such rules of engagement also offer a link to the international discourse on autonomous weapon systems within the scope of CCW, where demands for 'meaningful human control' or an 'appropriate level of human judgment' are already being discussed. So far, there is a lack of workable concepts of implementation. An essential challenge is the verification of compliance with the rules of engagement. Up to now, there have been no proven verification mechanisms for this. Initial considerations have been made as to how, for example, an independent, international monitoring of the employment of UWS could be made workable.[6] There is still a considerable need for research on this complex set of issues.

Regulation of Weapons-relevant Key Components

In most cases, the focus of traditional arms control is on entire weapons systems. However, modern weapons systems are becoming increasingly complex, and consist largely of dual-use components, which makes their regulation as a whole more difficult. However, if

specific technological components or armaments could be identified that are significant for certain categories of UWS and their military capabilities, these key components alone would create a lever for arms control regulations. In the future, arms control could then concentrate to a greater extent on these weapons-relevant key components instead of a complex weapons system per se. Examples of the specific identification and description of relevant key components can already be found within export control. For instance, the Missile Technology Control Regime (MTCR) lists subsystems and technological components that are relevant for the construction of military ballistic missiles or drones, and are therefore subject to export restrictions or bans.[7] Applying arms control to weapons-related key components could be an interesting approach that could benefit from previous lessons learned in export control.

Prohibition and Ban of Certain Future Weapons Developments

The need for arms control is often only realized when weapons systems have already been fielded, and their implications for security policy and international law can be observed immediately. The traditional approaches to arms control, therefore, revolve primarily around the regulation and limitation of existing weapons systems. However, once weapons systems have been stationed 'throughout the world' and on a broad scale, it is much more difficult to prohibit or regulate them. Nevertheless, there are also arms control approaches which aim at intervening in the development of certain weapons or prohibiting them in advance. On the one hand, there are the negotiations within the scope of the UN Convention on Weapons (CCW), whose task it is to discuss the unlawfulness of certain weapons or weapon applications, and, if necessary, to prohibit them, as it was the case, e.g. with regard to blinding laser weapons. From this point of view, CCW has also been holding expert talks on Lethal Autonomous Weapon Systems (LAWS) since

2014. On the other hand, the concept of Preventive Arms Control (PAC) provides an approach that focuses on the security policy implications of future weapons.[8] The objective of PAC is to identify in advance the potentially destabilizing consequences of future UWS and to regulate their technological research as well as development paths in such a way that critical systems will not even be fielded and employed.

In both cases, an awareness of future UWS risks under international law or security policy must first be raised on a broad international front and their containment must be seen as a win-win situation for all parties concerned. In addition to the willingness to engage in intensive political debate, this process requires in particular a comprehensive analysis and technology impact assessment of both new weapons technologies and future UWS.

In the end, it is conceivable, that automated UWS that are capable and intended to make a life-or-death decision in a mission without human intervention could be prohibited or banned. Conversely, the question arises under what circumstances would sufficient human control be guaranteed? The current discourse on meaningful human control reveals numerous obstacles and shows how difficult it is to achieve a common international understanding of this. However, a pragmatic solution could also lie in encouraging UWS to be programmed in such a way as to encourage rule-based and fundamental protection of human life. Such 'laws on robotics' were first formulated in literature by Isaac Asimov.[9] An automated UWS could thus be prohibited from self-directed target analysis or selection, and the killing of humans in general. However, a human operator would still be free to take full control of the system to carry out a lethal weapons employment. The difference to many previous control approaches is significant. In most cases, the human operator only had the right of veto, for example to stop a machine target

selection or an automated weapons employment. However, if UWS are programmed to protect human life in all cases of doubt, this programming would have to be overridden for a lethal attack by a human being consciously taking over full control of the unmanned weapons system. It is then up to human operator to analyze the situation, determine goals, and initiate the employment of weapons, which means that in the end the human really bears the direct responsibility for the act of killing. However, ensuring that such programming of UWS is permanently secure and verifiable is not trivial, and so far, trusted ideas for implementation have been lacking. For this reason, Isaac Asimov's laws on robotics will remain science fiction for the time being.

Limitation of the Proliferation?

Over the last decade, unmanned military systems have experienced considerable proliferation, and the number of actors operating with UWS has steadily increased (horizontal proliferation). In addition, a number of nations are making increased efforts to further develop the technology of UWS, and to advance their automation. The progressive integration of these systems into various military domains and the emergence of new spheres of operation can also be observed in this context (vertical proliferation). The steady proliferation of UWS goes hand in hand with the proliferation of their security risks.

The commitment and interest of the international community in the non-proliferation of UWS has not been very strong so far. On the contrary, for some years now there has even been an erosion of existing export control regimes (e.g. the MTCR) since economic interests in the export of UWS are gaining increasing influence in many nations.[10] In addition to the export of complete military unmanned systems, it is primarily dual-use technologies that contribute significantly to the proliferation and military adaptation of

unmanned systems, and open up various proliferation paths. How this dual-use issue can be better addressed in export control is thus far an unsolved problem. A starting point for this could be provided by previous lessons learned from the 'general-purpose' criteria used in the field of biological and chemical weapons regulation. It is also conceivable that an international export monitoring system could be established to track the global export/import of such dual-use key components that are not only significant for the development of UWS but also considered problematic. If a critical combination of such key components were then assigned to a single actor, this could be interpreted as an indication of the desired development of such a weapons system. As a reaction, international export restrictions on the actor and related dual-use technologies could then be put into effect. To this end, however, it is first necessary to clarify internationally, which kind of UWS should be regulated, and which would be the critical combination of key components. It should always be borne in mind that export controls can quickly develop a discriminatory character if they do not apply equally to all nations, and thus may lose their legitimacy.

Conclusion

The proliferation and automation of UWS is increasing worldwide. While the international legal dimension of the use of autonomous weapon systems has been discussed for several years within the scope of the UN CCW, the security policy implications of UWS have so far lacked the necessary attention. In a time of increasing international tensions and a weakened international security architecture, the security policy risks potentially associated with UWS pose a particular threat to stability and peace. Arms control can successfully contain this danger – a lesson learned from the Cold War, but which now seems to have been forgotten. However, the

traditional approaches to arms control alone can no longer meet the requirements posed by modern UWS. Arms control must, therefore, be rethought and should not hesitate to take bold steps. But there is no reason to gloss over anything; this will be neither an easy, nor a fast process. In this respect, many questions are still pending, and creative solutions must be worked out, so that confidence in arms control can also be ensured in the future. Some more or less realistic approaches have been presented here. An important first step would be to raise awareness of the security policy risks of UWS and to recognize the benefits and necessity of arms control internationally. If there is the will to do so, then answers to the many open questions will be found – this much mankind has always proven in the past.

Endnotes

1. For examples, see: Dickow, Marcel, Anja Dahlmann, Christian Alwardt, Frank Sauer & Niklas Schörnig (2015). First Steps towards a Multidimensional Autonomy Risk Assessment (MARA) in Weapons Systems, IFAR Working Paper 20, Dec. 2015, https://ifsh.de/file-IFAR/pdf_deutsch/IFAR-WP20.pdf (Accessed 7 Aug. 2020). / Alwardt, Christian & Martin Krüger (2016). Autonomy of Weapon Systems, Food for Thought Paper, Feb. 2016, https://ifsh.de/file-IFAR/pdf_english/IFAR_FFT_1_final.pdf (Accessed 7 Aug. 2020).
2. New START Treaty, for further information see: https://www.armscontrol.org/factsheets/NewSTART (Accessed 7 Aug. 2020).
3. The Intermediate-Range Nuclear Forces (INF) Treaty, for further information see: https://www.armscontrol.org/factsheets/INFtreaty (Accessed 7 Aug. 2020).
4. The Conventional Armed Forces in Europe (CFE) Treaty, for further information see: https://www.armscontrol.org/factsheet/cfe (Accessed 7 Aug. 2020).
5. For Vienna Document, see: https://www.osce.org/fsc/86597 (Accessed 7 Aug. 2020) & for UN Arms Register, see: https://www.un.org/disarmament/convarms/register/ (Accessed 7 Aug. 2020).
6. Altmann, Jürgen & Mark Gubrud (2013). Compliance Measures for an Autonomous Weapon Convention, ICRAC Working Paper #2, May 2013, https://www.icrac.net/wp-content/uploads/2018/04/Gubrud-Altmann_Compliance-Measures-AWC_ICRAC-WP2.pdf (Accessed 7 Aug. 2020).
7. For examples refer to the Missile Technology Control Regime (MTCR) website, https://mtcr.info/mtcr-annex/ (Accessed 7 Aug. 2020).
8. Mutz, Reinhard & Götz Neuneck (eds.) (2000). Vorbeugende Rüstungskontrolle. Ziele und Aufgaben unter besonderer Berücksichtigung verfahrensmäßiger und institutioneller Umsetzung im Rahmen internationaler Rüstungsregime, Nomos, Baden-Baden.
9. Asimov, Isaac (1942). Runaround, Astounding Science Fiction, Vol. 29, Issue 1, 94–103.
10. CNAS (2017). Drone Proliferation–Policy Choices for the Trump Administration, Center for a New American Security, Jun. 2017, http://drones.cnas.org/wp-content/uploads/2017/06/CNASReport-DroneProliferation-Final.pdf (Accessed 7 Aug. 2020).

Part V

Future Perspectives

24

By Christoph Müller, GE
By Dr Martin Hellmann, GE
By Dr Hans-Albert Eckel, GE
By Dr Thomas Neff, GE
By Dr Dirk Zimper, GE
German Aerospace Center (DLR)

Research, Development, and Acquisition of Counter-UAS Technologies

Introduction

In general terms, Research, Development and Acquisition (RD&A) can be loosely defined as the efforts undertaken by companies and governments to innovate and introduce new products to achieve or enhance specific capabilities. Therein Research and Development (R&D) can be understood as the process towards the maturing of technologies, while acquisition is widely recognized as the bureaucratic management of the procurement process that deals with the investment in technologies, programs and products.[1]

Commonly, RD&A is separate from most operational activities not expecting immediate benefit but aiming for long-term advantages of the sponsoring entity. That accounts even more for defence-

related RD&A, which are typically not constrained by classical market rules mainly due to the much greater complexity of the user and a general absence of a profit motive by governmental agencies.[2]

While the definition of necessary capability requirements is an inherent part of acquisition processes, R&D cycles are less the subject of outside demands than of focused investments and time. The following chapter shall show basic observations and trends of RD&A in the past, highlighting findings specific to C-UAS RD&A. Moreover, it will outline acquisition and cost-related aspects important for C-UAS technologies and finally drawing conclusions specific to the future development of such systems.

Technology Development

To grasp the complexity of RD&A, it is necessary to understand the individual maturity stages, their integration and transfer towards products as well as the targeted market. Neither Research nor the Development of individual Technologies or Systems is a linear process of which the timelines or end states can be accurately predicted.

One prominent example can be found in Graphene[i] and related applications. After its first discovery in the early 2000s, it was quickly attributed with a game-changing nature. Despite Graphene's superior properties such as electrical and thermal conductivity, barrier properties and high strength, the research struggled to utilize it in a larger scale. This is mainly due to the fact that it is not trivial to upscale Graphene technologies in an affordable way.

[i] Graphene is a modification of carbon in the form of a single layer of atoms in a two-dimensional honeycomb lattice in which one atom occupies each vertex.

Hence, the initial 'hype' was followed by smaller steps than expected leading to partial disillusion.

Assessing the Maturity of Technologies

The concept of Technology Readiness Level (TRL) is well understood and commonly used by the scientific community to describe the maturity of technologies ranging from the observation of basic principles (TRL 1) to the prototype demonstration in a relevant environment (TRL 6) towards 'mission-proven' systems (TRL 9). Originally introduced by the National Aeronautics and Space Administration (NASA) in the late 1980s, the nomenclature is also used to evaluate specific research projects or individual technologies.

While the taxonomy of TRL is best suited for individual technologies, it lacks the structure to assess the maturity of complex systems comprising multiple emerging technologies. Instead, other methodologies such as the System Readiness Level (SRL) are used to provide a qualitative and quantitative estimate of the level of readiness of a system. Those models, based on matrix algebra approaches, are the attempts of individual organizations to quantify and mitigate risks related to technology developments. In contrast to TRL other Readiness Levels are relatively new and not that commonly used.[3]

Even if technologies mature, successful transition to neither applications nor capabilities is certain. A phenomenon known as *Valley of Death* symbolizes the challenges for academia, governmental research and industry to operationalize ideas. While precise definitions vary, the principle problems can be summarized as the lack of funding, the cultural differences between academia and industry, the absence of customer awareness or an ever-changing requirement space.[5] Governmentally funded research institutions such as the German Aerospace Center (DLR) are designed and

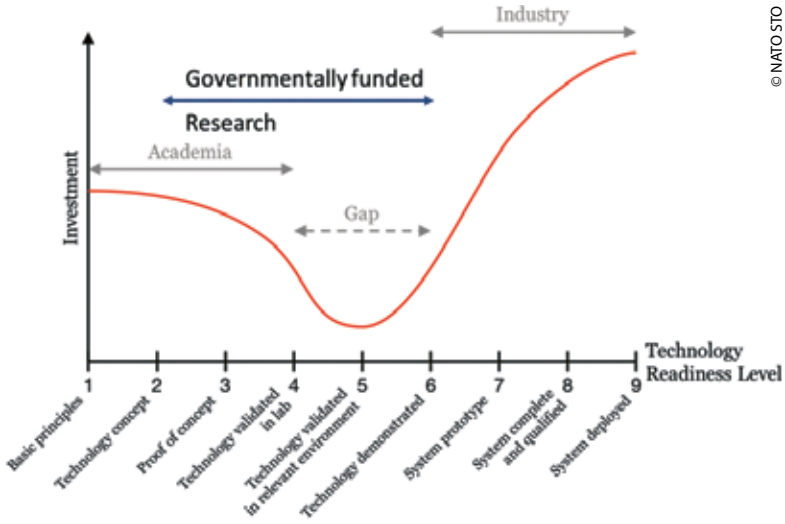


Figure 24.1: Bridging the Valley of Death by Governmentally Funded Research.[4]

tasked to carry out the necessary Technology Transfer towards a real-life product in close cooperation with academia and industry.

From Technology to Capability

To be successful, an emerging technology or a novel system will not only need to be mature, rather it requires a broad understanding and adoption by the user. If not forced, that is more a function of time and costs rather than the technology itself. Today's widely used technologies such as landlines or washing machines needed more than 50 years from entry to the market to full market penetration.[6]

In other words, technological driven military disruptions often need decades to mature and to be operationally effective. That can anecdotally be illustrated by the 36 years necessary from the

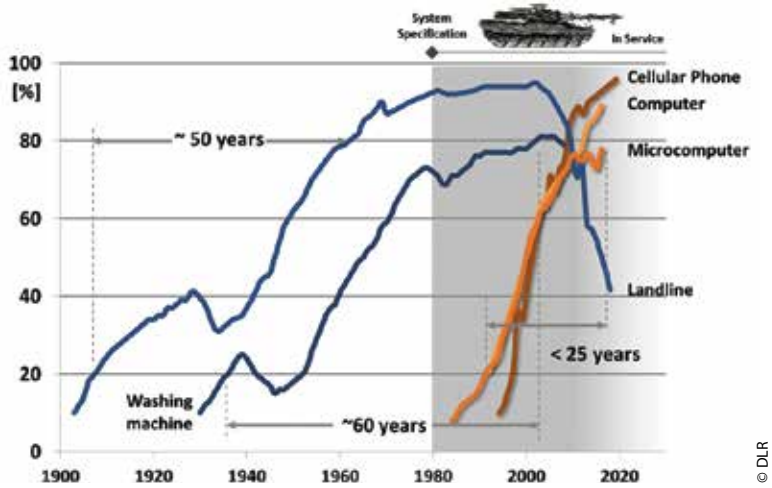


Figure 24.2: Technology adoption rates measured as the percentage of households in the United States using a particular technology.[5]

Baldwin Patent for an internal combustion engine in 1879 to the first tanks entering the military inventories in 1915 resulting in Mechanized Armour; or the appearance of first operational Jet Aircraft, the German Messerschmitt 262, on the battlefield in 1944 rooting back to the 1910s Coandă Ducted Fan.

In the last forty years, the adoption of new products by the market has accelerated as has the pace of technology developments in specific fields. Moore's Law is one of the most illustrative examples based on the observation that the number of transistors in a dense integrated circuit doubles about every two years. Microprocessors being the basic technology for numerous applications, their exponential growth in performance leads to numerous of other new technologies. Unlike common market mechanisms, military acquisition programs had struggled to adapt at the same pace.[7]

To be truly relevant for or successfully utilized by the military, RD&A has to be closely aligned with doctrinal and conceptual developments. The current Chairman of NATO's Military Committee, Air Chief Marshall Sir Stuart Peach, argued for the necessity of the militaries to define *'[...] the relevant military use [...] rather than technology telling people what they can do, [...]'*.[8]

Specifics to C-UAS Technologies

As it is possible to draw general conclusions for RD&A, it is also possible to have a closer look into specific key technologies relevant to countering Unmanned Aircraft Systems (UAS). Aside from the specific technologies, we must also include the UAS and C-UAS ecosystem to understand the dynamic that is characteristic for this market and has to be considered for any RD&A decisions.

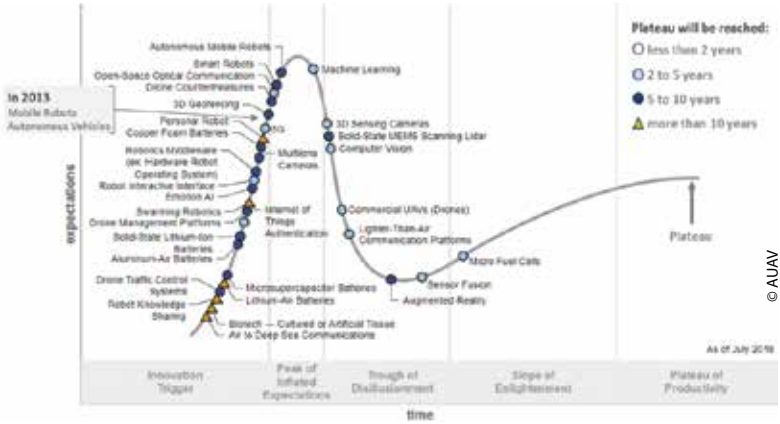


Figure 24.3: Selected emerging technologies relevant for (counter) UAS technologies projected on Gartner Hype Cycle as of July 2018.[12]

Since the acceleration of the United States' global UAS operations in the beginning of 2008, the numbers and types of UAS have rapidly evolved.[9] While the military user was the major driving force behind the utilization of UAS in the very beginning, the rise of commercial manufacturers and the introduction of new business models have shifted that situation. A broader technological basis and decreased costs have allowed a wider utilization of the required technologies allowing defence related RD&A to focus on add-on research.

Maturity of Counter-UAS – Reality Check

A first indication of the current maturity and expected advancement of related technologies can be derived from strategic technology assessments such as the Gartner Hype Cycle model. It characterizes the exemplary progression of emerging technologies from an enthusiastic innovation trigger through a period of disillusionment to an understanding of the technologies utilization.[10] Although not fully congruent for some technologies, those general trends give a good understanding and comparison over time.[11]

According to Gartner, *Mobile Robots and Autonomous Vehicles* reached their peak of expectations for civil applications in 2013. Half a decade later, technical and non-technical obstacles remain preventing them from utilization for day-to-day operations such as integration in the civil airspace or performing long-haul flights, especially for small UAS and drones. Nevertheless, a steadily growing number of market entries beyond private customers indicates growing maturity.[13]

Highly Dynamic Interaction Between Market and RD&A

Following a similar pattern, exemplary C-UAS technologies such as 3D Geofencing or general Drone Countermeasures are experiencing

their medial overenthusiasm while others have already claimed to be operational ready reaching their plateau in the near future.[14] Taking into account that successful C-UAS operations require the interplay of the whole processing chain stages, maturing only isolated stages will make them not operationally effective.[15] For the very reason that the advancement of commercial and military Unmanned Aircraft will result in more performant systems, numerous research questions around technology, safety, practicality, policy, and legality of C-UAS measures continue to be of high importance.[16]

Meanwhile, the market of C-UAS systems and the number of manufacturers have skyrocketed. As of September 2019, at least ninety-five countries operate UAS and the number of market available C-UAS systems or sub-systems has exponentially increased from about 12 in 2015 to 537 in 2019. At the same time, the number of manufacturers increased to about 277.[17] Furthermore, a steadily growing number of tier suppliers at all levels has resulted in multi-level partnerships accelerating innovation for both Unmanned Aircraft and Counter Systems, in hardware, software and services.[18]

Multifaceted and Multi-layered Threat – No Single Solution

The current non-technological as well as technological landscapes including industrial solutions do already indicate the fast amount of future challenges posed to C-UAS Systems. Given the multifaceted and multi-layered threat environment, the response cannot be based on single solutions in any of the processing chain stages or for any given military scenario.[19]

'[...] it has proven difficult to identify and mitigate threats using currently fielded technologies',[20] which is mainly due to drawbacks such as camera systems being degraded by weather conditions, radar systems picking out low flying small UAS and drones very

late or interdiction methods only working for specific entry modes.[21] However, the aforementioned dynamics in R&D and market demand indicate that the rapid advancement of individual technologies will be very likely, but the effectiveness of countermeasures will still rely on the 'weakest' stage in the process chain. Hence, even if all individual elements of C-UAS or air defence capabilities are well developed and in place recent developments in UAS operations in Libya show that the effectiveness of C-UAS can be limited if confronted with an overwhelming number of UAS.[22]

Challenges for Technology Research – the Cat and Mouse Game

'This threat is evolving every three to six months – it is just that adaptive … This is going to be a continuing challenge due to the adaptive nature of the problem of being able to use small drones in so many different ways and you cannot rely on one technique to respond to them.'[23]

Vayl S. Oxford
Director, US Defense Threat Reduction Agency, March 2019

In the absence of fully autonomous capabilities operating drones still relies on the smooth interplay of all Unmanned Aircraft System Components as introduced in Chapter 1 (cf. p. 13 f.). The complexity of comprehensive C-UAS operations has been introduced in Chapter 4 (cf. p. 55 ff.), show-casing numerous possible entry modes to disrupt that interplay of technologies.

Since militaries are generally depending on most of those technologies, not only for UAS operations, significant efforts and resources are devoted to ensuring their smooth operations also in

contested environments. A kind of an arms race has already started either intentionally by the defence and security sector or unintentionally by manufacturers improving their products. Some of those efforts can be already found in the available literature and current research portfolios of nations.[24]

Robust Navigation – Current Effectors Might Fail

To navigate a UAS and drones properly, accurate values of its position and orientation are needed. Therefore, usually data from a space-borne navigation system like the Global Positioning System (GPS) are used. The signals coming from such systems can be jammed or spoofed, causing the loss of the system or at least a mission failure. Besides, GPS signals are degraded or absent in many areas hampering the operational use of UAS.[25]

The majority of market available effectors of C-UAS systems use these two aforementioned countermeasures. Hence, great efforts are currently underway by militaries but also civil UAS and drone manufacturers to harden their products towards more resilient modes of navigation.[26] Countermeasures dealing with this problem are described in the following paragraphs.

Jammers can be countered by using a Controlled Radiation Pattern Antenna (CRPA), which either can steer the radiation pattern of the array to form a spatial null towards the jammer or to provide additional gain towards the satellites. A notch filter in the receiver front-end can mitigate Continuous Wave (CW) signals, adaptive notch filters can be used to counter chirp signals[ii] to a certain extent.

[ii] Chirp signal frequency increases or decreases with time. That mode of signals is commonly applied to sonar, radar, and laser systems, and to other applications, such as in spread-spectrum communications.

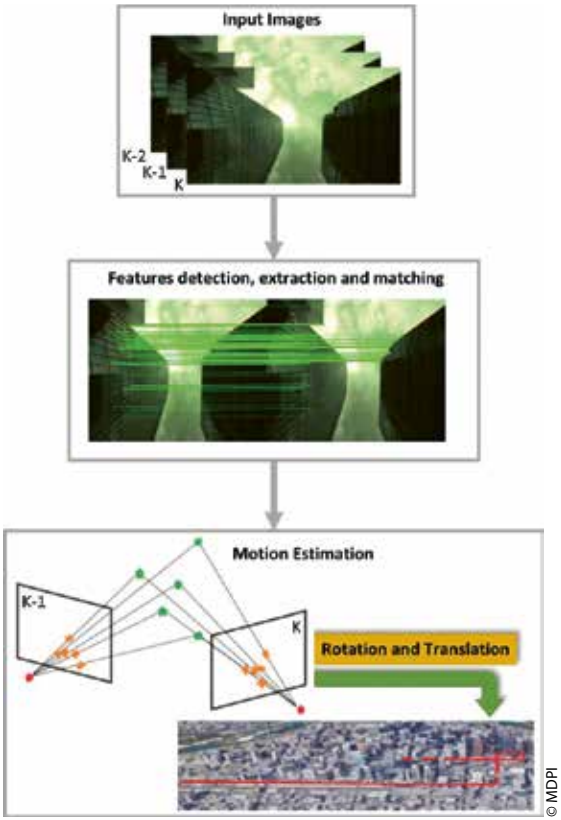


Figure 24.4: Principle function of Visual Odometry.[27]

In this context, it has to be mentioned that low-cost Commercial off-the-Shelf (COTS) receivers are often more robust against chirp jammers than professional receivers. COTS receivers often have very narrow front-end filters, so that the most part of the chirp ramp is suppressed by these filters. Professional receivers usually use front-ends with a broader bandwidth. This allows a more

accurate measurement but also increases their vulnerability to chirp jammers. To fill this gap, wideband Global Navigation Satellite System (GNSS) signals like Galileo E5 or Galileo PRS allow advanced mitigation techniques.

To counter **Spoofing**, the use of array antennas is a feasible method. So the footprint of the signal can be as small as possible, and a side interaction suppressed. More actively, arrays can be used to assess the directions of incoming signals indicating whether the signal is artificially created or from different satellites. Also, internal information generated by a UA's or drone's inherent sensors can be used to identify a spoofing attempt and to react. Meaconing[iii] can be countered by the same techniques used to navigate in GNSS denied environments.

On-board Navigation and Positioning – Hampering External Manipulation

In the absence of external navigation information, an onboard initial measurement unit has to provide the required data. A localisation and mapping algorithm can build up a live map which, in combination with a visual sensor, can be matched to the currently captured image of that sensor. Another possibility is Visual Odometry (VO), a procedure which estimates the position and orientation of the UA analysing the deviation induced by the motion of the vehicle regarding images captured by onboard visual sensors (cf. Figure 24.4, p. 447).

[iii] Meaconing is the interception and rebroadcast of navigation signals. These signals are rebroadcast on the received frequency, typically, with power higher than the original signal, to confuse enemy navigation.

Figure 24.5: The DLR developed transportable optical ground station (TOGS) and the 'Free-space Experimental Laser Terminal II' will allow secure data communications between the aircraft and the ground.

Future techniques will use not only visual cameras but also information coming from microwave sensors like radar images. In combination with information generation based on Artificial Intelligence (AI) algorithms, the position and orientation of the UA can be calculated more accurately. New technologies with respect to quantum navigation and timing can also lead to accurate, independent positioning and navigation of UAS.[28]

New Command and Control links – Expanding UAS Performance

Safe operation of UAS requires a stable command and control link between the pilot on the ground and the UA. Conventional links will gradually deteriorate when the distance increases, making the link more vulnerable to interference and sudden condition changes, which in turn can compromise safe flying. New network technologies offer promising solutions. An example is the usage of Internet Protocol (IP) datalinks based on commercial Long-Term Evolution (LTE) networks or specific Information Technology (IT) infrastructure. Multi-static transmitters, robust coding schemes as well as the very high sensitivity of receivers offer unique conditions for robust communication to small UAS and drone swarms.[29]

UAS carrying a variety of sensors for monitoring and surveillance generate new needs for large data transfer in real-time. Free Space Optics (FSO) communication provides data rate capabilities of up to several Gbit/s at unprecedented distances with low transmitter power and therefore is superior to all possible microwave and Radio Frequency (RF) solutions. FSO allows for very narrow and directional beams, is immune against electromagnetic interference, and cannot be detected with RF meters or spectrum analyzers. It is the ideal technology for robust, secure air-to-air and air-to-satellite data links.[30]

Distance and Speed – Shrinking the Response Window

Slow-moving and non-stealthy UAS are easily targeted by state-of-the-art C-UAS. However, the effective detection range, especially for low, slow and small (LSS) UAS, can be only a few hundred meters or less given the terrain characteristics and height. Even with high detection effectiveness, the response window for the operator can be very small.

Future generations of UAS will benefit from higher speeds and unprecedented agility since the designers need not worry too much about the 'g' effects and push the aircraft to its absolute limit. Greater speed is clearly an advantage in combat. UAS will dominate the OODA (observe-orient-decide-act) loop and operate faster than a defender can observe the threat, orient himself, decide how to respond and act on that decision.

That will apply to all classes of UAS. Highly agile rotary-wing aircraft with tricky trajectories, jet-powered fixed-wing aircraft in combination with stealth technologies, and of course the upcoming threats, hypersonic glide vehicles and hypersonic cruise missiles. Likewise, novel developments such as distributed sensor-to-

shooter networks as well as AI-supported or automated decision making will shorten timelines to counter UAS.

Hardening of Drones – No Clay Pigeon Shooting in the Future

For all military vehicles, plating is the usual countermeasure against mechanical threats. For airborne systems, weight aspects are important. Therefore, new plating materials like carbon-reinforced resins were and will be designed which are light and strong. Openings for sensors or engines within the UA's airframe are weak points for mechanical cracks.

The ongoing miniaturisation for almost all components helps to reduce critical structural elements, to use and distribute multiple components with the same function making the overall system resilient against failure and to integrate most components into the structure shielding them.

Furthermore, military tests have shown that striking drones by conventional projectile weapons is difficult especially if the vehicle is fast and flying at an acute angle to the defence. Also, the UA only will be influenced if relevant components like the navigation system or the engine will be hit. Otherwise, the UA's mission is impeded.[31]

As in most military equipment, the hardening against electro-magnetical threats is a standard requirement advancing survivability. High Power Microwave (HPM) threats against UAS and drones can cause three major impacts on the system. Pulse energy can disturb or destroy the sensors as well as important electronics of the drone, huge energy induction can degrade the power system or the structure and architecture effects can hit the combination of the electronic components within the vehicle.

Countering pulse energy specifically designed components with high resistance against Electro-Magnetic Impulses (EMI) were and will be designed. Also, metallic shielding of components or the whole vehicle is an effective countermeasure. Additionally, miniaturization of components will allow designs that can help to reduce a possible energy flow through structural openings. Using shielding, reflectors and heat pipes within the vehicle reduces the electromagnetic and thermal influence of energy flow. To counter architectural effects, the distribution of relevant components and their distances within the vehicle are important. Using a larger size UA makes it easier to distribute the energy impact, and intelligent design of the system helps to harden it against HPM.[32]

Avoiding Detection – The Invisible Drone

While most UAS in militaries' inventories are designed in a 'traditional' way, next generations such as the French NEURON or the US Navy's MQ-25 will incorporate stealth features. The adapted structure of the surface and the inlet reduces the reflections within the radar frequency bands. Specially designed metamaterials can further support this behaviour. Miniaturisation and/or mission-specific varnishing reduce optical visibility. Infra-Red (IR) emissions can be decreased by distributing the occurring thermal energy away from hot spots with heat pipes or radiators.

Low observability flight path planning in the presence of multi-static radar detection systems is a new controls challenge that will increase capabilities for UAS. Current flight path optimization relies on simple aircraft models coupled with detection models with a limited efficiency if confronted with an increasing number of path dependencies and multiple minima requirements. Explorations with variations of the non-linear trajectory generation methods are capable of producing solutions that satisfy observability constraints in the future.[33]

Likewise, noise detection for surveillance gained more attention in recent years. Passive noise can be reduced by modifying the aircraft structure. Therefore, various vibration-absorbing materials can be used in a limited frequency band. Also, the design of UAS with favourable drag coefficient usually creates less noise during flight than other designs. This can be done, e.g. by modifying the geometry of the wings or the blades. Reduction of low-frequency noise (< 200 Hz) is more challenging than the reduction of higher frequencies. Acoustic metamaterials can support to manipulate the acoustic behaviour in the right way.

Active noise behaviour can be influenced by electromechanical systems which can control the structure, the isolation against sound radiation, or the noise itself. Some of those systems use piezoceramic actuators attached to the skin of the drone or manipulate the engines in a way to actively shape the noise pattern emitted by the drone.[34]

Quantity Has a Quality All Its Own – Overwhelming the Countermeasures

The threat posed by single UAS and drones has been acknowledged and sophisticated C-UAS technologies have been developed to counter threats from LSS to High Altitude Platforms. The alarming trends for increasingly available, cheap, and operational UAS was showcased in coordinated operations such as the attacks on the Saudi Arabian oil facilities in 2019 or the use of drone swarms at the Winter Olympic Games in 2019.

Swarms of UA and drones in combination with the ability of vehicles to follow a pre-programmed flight-path or to autonomously make decisions based on shared information have the potential to revolutionize the dynamics of conflict in near terms. Swarm size

will grow significantly, enhancing the swarm's behaviour and decisions. A swarm of both large and small drones equipped with different payloads will create a whole that is more capable than the individual parts.[35]

State-of-the-art C-UAS technology may be able to cope with a bunch of attacking drones, but an offensive swarm is much worse because the drones might be able to adapt to whatever is done to counter them or simply saturate the whole processing chain of countermeasures.

Electronic warfare seems to be the most promising technology to counter swarms since swarm functionality inherently depends on the ability of the drones to communicate and share information. Vulnerabilities to electronic warfare depend on the composition of the drone swarm. Swarms may incorporate drones specifically designed to counter jamming, communication drones serving as relays to share information, or drones equipped with anti-radiation missiles and other anti-jamming weapons.[36]

Procurement and Costs

'Governments purchasing defence equipment have a bad record because buying military hardware isn't like other types of procurement.'[37]

As an example, the United States' Defense Acquisition Guidebook describes military acquisition as the bureaucratic management and procurement process dealing with a nation's investments in the technologies, programs, and product support necessary to achieve its national security strategy and support

its armed forces including the sustainment of necessary industrial capabilities.[38]

Similar holistic approaches might vary in granularity across NATO and Partner nations, but in the end, they put required military capabilities in perspective to resources available. Here it is not important what particular acquisition process is used; each has its advantages and disadvantages. Finally, the uncertainties of the future operating environment and the characteristics of defence acquisition will always be challenging, and disappointments are inevitable.[39]

Market Characteristics

Unlike the commercial markets, the defence procurement process has to operate in a market with limited buyers and limited sellers. That basically results in major tenders occurring on an irregular basis with a variety of well-defined but conflicting objectives pushing the technology envelope. In contrary, the industry has to

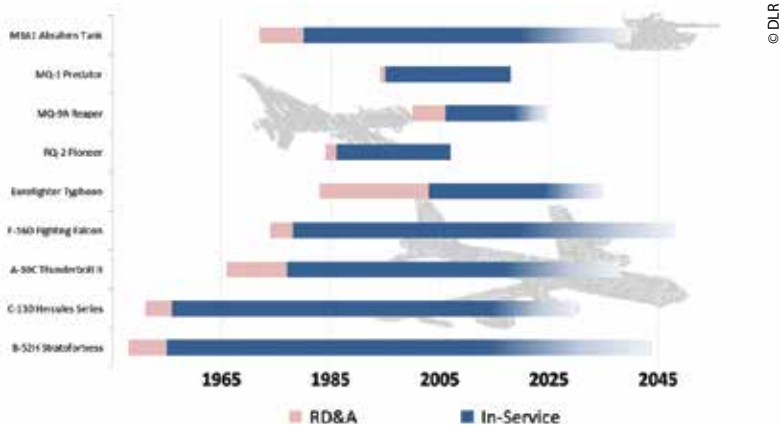


Figure 24.6: RD&A and projected In-Service timespans of exemplary defence projects.

aggressively bid on military procurements, *'even if a particular offering doesn't quite meet the requirements.*'[40]

RD&A has to develop equipment requirements based on a very dynamic security environment with limited knowledge of the future. In combination with very long in-service times of 20 or more years, this can often result in fastidious requirements that probably only one or no supplier can meet. In any case, planners are requested to agree on a well-defined set of requirements as a key element of a successful procurement.[41]

Furthermore, military requirements plus other technical, regulatory and industry policy tend to multiply complexity, risks and costs challenging governmental budgets even further. Even if reasonable, in case secondary objectives overtake the primary ones, project success is jeopardized in most of the cases. The distribution of governmental budgets, yearly planning cycles and appropriation do the rest.

An Example of a National C-UAS Approach – US DoD Procurement

One of the most prominent examples for national C-UAS RD&A can be found in the United States Department of Defence (DoD). *'In Fiscal Year (FY) 2021 the DoD plans to spend at least USD 404 million on C-UAS research and development and at least USD 83 million on C-UAS procurement'*[42] making it one of the most vital RD&A environments for C-UAS technologies in NATO.

To account for robust defence capabilities, the DoD is developing and procuring several different C-UAS technologies across their four operational services – Air Force, Army, Marine Corps and Navy. This multi-agency approach explicitly includes the assessment

and validation of defence capabilities and concepts in real life exercises looping the feedback in the national RD&A process.

Similar to bigger RD&A projects the DoD has adopted its new 'Design-Build-Fly' philosophy to C-UAS technologies accounting for the broad range of challenges outlined in the previous paragraphs. Given the DoD's strong market position and its user diversity, a wide range of technologies are under consideration. Even if individual products procured by one branch might be obsolete in the near future, complementary technologies from other services would allow for fast adoption and closing capability gaps in relatively short times. In addition, the philosophy does not necessarily include a procurement end-state allowing continuous further development of C-UAS technologies.

Procurement in the EU – National and Future Cooperation?

A fundamentally different problem set can be found in the European Union (EU) where the total or relative spending on RD&A are by far lower and nationally scattered compared to the United States. Besides, most European nations do have very specialized services pooling capabilities such as C-UAS in only one branch, resulting in a situation that one service has to provide this specific capability for all services.

When combined, the EU member nations have the second-largest defence budget in the world; a general assessment concluded that the broad diversity significantly hampers military capabilities. Inadequate cooperation amongst the nations results in losses of about EUR 25 to 100 billion each year mainly caused by nationally centric RD&A processes, and, in turn, entailing duplication of work and capabilities. The lack of common defence-related R&D under the umbrella of the EU was worrisome in 2018.[43]

Furthermore, those scattered national RD&A activities tend to be overloaded with competing requirements and, unlike the services-based US RD&A initiatives, those national procurements cannot be easily adopted by other nations if necessary. Hence, once individual national C-UAS capabilities become obsolete, better-suited solutions from other nations could not be easily operationalized. Also, multi-national RD&A cooperation remains isolated to efforts mainly limited to flagship projects.

Consequently, the EU has implemented the Permanent Structured Cooperation (PESCO) framework complemented by regular capability reviews[iv], capability development priorities[v] and the common European Defence Fund (EDF) slowly developing national RD&A towards multi-national ones. Providing common funding of its research window and co-financing of its capability window the EDF aims towards higher interoperability and strengthening European RD&A in general from 2021 to 2027.[44]

One of the ongoing PESCO projects aims *'to develop an advanced and efficient system of systems with C2 dedicated architecture, modular, integrated and interoperable with C2 info-structure, able to counter the threat posed by mini and micro Unmanned Aerial Systems'*.[45] With only two participating nations this project illustrates the difficulties of common sense and longer-term co-operations. Interestingly, future initiatives such as the European Defence Industrial Development Programme (EDIDP) does not include an individual call dedicated to C-UAS technologies missing the opportunity to collectively focus on this urgent matter.[46]

[iv] Coordinated Annual Review on Defence (CARD).

[v] Capability Development Plan (CDP).

Need for Harmonization Between Nations, EU & NATO

While there is a clear need for harmonization of C-UAS capabilities within individual nations, but especially within the two big Alliances, initiatives start to emerge targeting doctrinal and policy-making in this specific area. Stakeholders have recognized that interoperability is more a matter of common requirement sets and standardization rather than a technical challenge. Once that framework is achieved national or multi-national RD&A will be able to provide exchangeable solutions.

While the EU follows a centralized approach capitalizing on its aforementioned toolset as well as common EU funding, in NATO the warfare development of military structures, forces, capabilities and doctrines are led by the Allied Command Transformation (ACT). Compared to the EU, the available budget of NATO ACT or other NATO S&T stakeholders is relatively small and not suited to steer RD&A projects only to support decision making.

NATO relies more on focused initiatives with limited funding and voluntary contributions of its member states to further develop common capabilities. Two prominent examples are the C-UAS Working Group sponsored by the NATO Headquarters that has recently issued its *NATO Countering Class I C-UAS Handbook* collecting best practices across nations[47] and the *Low, Slow and Small Threat Effectors study* issued by the NATO Industrial Advisor Study Group 200 investigating C-UAS solutions, particularly in the area of soft and hard kill effectors, together with associated Tactics, Techniques & Procedures (TTP).[48]

Backdrop of C-UAS From a Cost-Benefit Perspective

The outlined dynamic of the C-UAS R&D environment as well as the absence of widely accepted standards results in disadvantageous

cost ratios between countermeasures and unmanned air systems. For instance, the unit price per complete FLIR Systems' Black Hornet Nano can be found between USD 15,000 and USD 20,000,[49] while the majority of C-UAS systems cost more than USD 100,000 but covering mainly Class I UAS.[50]

Currently, UAS are commonly used by militaries as well as non-state actors across the globe and this is expected to grow in the years to come, significantly impacting military operations. Hence, the required area or point defence capabilities need to be deployed in high numbers to cover all necessary altitudes and distances. The combination of relatively high costs and a rather high number of systems will make comprehensive C-UAS capabilities costly as indicated by an initial estimate by the 'Deutsche Flugsicherung' for civil airports in Germany.[51]

So What?

This chapter outlined some basic characteristics of RD&A, which impact the fielding, utilization and effectiveness of C-UAS in general. From the perspective of the authors, there are three major conclusions that can be drawn from it:

The Volatile 'Silver Bullet'

Even if RD&A would come up with a 'silver bullet' to counter Unmanned Air Systems, it might not last long and could become obsolete in several months, setting the C-UAS efforts back to the starting point.

Technological Pace vs Traditional Procurement

If C-UAS solutions are volatile, constant RD&A efforts have to be undertaken to keep up the pace of technology developments leaving traditional procurement processes behind.

No Cost Shortcuts

The necessity of constant efforts has resulted in a relatively high cost ratio to the disadvantage of C-UAS Systems draining military budgets in peacetime and during conflicts.

Since UAS operations are going to play a major role in conflicts, countering those systems will be a key element for successful operations. From an RD&A perspective those efforts can be supported by a constant information flow between the R&D environment and the C-UAS operator to ensure new findings will be addressed immediately. That includes regular experiments and demonstrations as a natural part of military exercises, mutually bringing together researcher, industry and operator.

Furthermore, the reality of C-UAS might require multiple parallel systems or sub-systems to balance individual capability shortages and to make it harder for UAS to succeed. While for bigger nations that approach seems to be feasible, overall national budget constraints will generally limit the number of C-UAS systems that can be fielded by individual nations. Interoperability amongst individual C-UAS systems and nations embedded in defence frameworks such as NATO and/ or EU will become another key element.

Finally, RD&A cycles for C-UAS need to be shortened to keep pace with the technology development of UAS and drones. In 2019, the current Assistant Secretary of the US Air Force for Acquisition,

Technology and Logistics, Dr William Roper, pitched an idea to *'adopt a rapid approach to developing small batches of fighters with multiple companies, much like the Century Series of aircraft built in the 1950s'*.[52] Capitalizing on available commercial off-the-shelf systems and sub-systems would allow to field operational C-UAS in shorter periods, probably resulting in a limited capability set of individual systems. By fielding multiple systems and capitalizing on frequent updates, those limits can be overcome and new capability requirements can be addressed immediately.

Endnotes

1. F. G. Patterson Jr, 'Systems Engineering Life Cycles: Life Cycles for Research, Development, Test, and Evaluation; Acquisition; and Planning and Marketing', in Andrew P. Sage (Ed.) and William B. Rouse (Ed.), 'Handbook of Systems Engineering and Management', 2nd Ed., John Wiley & Sons, Inc., 2009, 65–115. [Online]. Availlable: https://media.wiley.com/product_data/excerpt/30/04700835/0470083530.pdf. [Accessed 18 Jul. 2020].
2. Benjamin Zycher and David Morton, 'Transportability in the Defense Department Research, Development, and Acquisition Process', RAND Corporation, 1991. [Online]. Available: https://www.rand.org/pubs/reports/R4107.html. [Accessed 18 Jul. 2020].
3. Michael Knaggs, John Ramsey, Alfred Unione, Dennis Harkreader, John Oelfke, Dale Keairns, and William Bender, 'Application of Systems Readiness Level Methods in Advanced Fossil Energy Applications', in Jon Wade (Ed.) and Robert Cloutier (Ed.), 'Procedia Computer Science', Vol. 44, 2015, 497–506. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050915003075?via%3Dihub. [Accessed 18 Jul. 2020].
4. Jan Hensen, Roel C.G.M. Loonen, Maria Archontiki, and Michalis Kanellis, 'Using building simulation for moving innovations across the Valley of Death', REHVA Journal, Vol. 52, 2015, 58-62. [Online]. Available: https://www.researchgate.net/publication/276205251_Using_building_simulation_for_moving_innovations_across_the_Valley_of_Death. [Accessed 18 Jul. 2020].
5. Hannah Ritchie and Max Roser, 'Technology Adoption', Our World in Data, 2020. [Online]. Available: https://ourworldindata.org/technology-adoption. [Accessed 18 Jul. 2020].
6. Alan Shaffer, 'NATO Technology Trends For Disruption', NATO Science & Technology Organisation (STO), 2018.
7. Sir Stuart Peach, 'Defence Implications of Emerging Technologies' at '16th Asia Security Summit: The IISS Shangri-La Dialogue', International Institute for Strategic Studies (IISS), 3 Jun. 2017. [Online]. Available: https://www.iiss.org/-/media/images/dialogues/sld/sld-2017/documents/special-session-3-defence-implications-of-emerging-technologies-as-delivered.pdf. [Accessed 18 Jul. 2020].
8. Ibid.
9. Helen Warrell, 'From Desert Strom to Soleimani: how US drone warfare has evolved', Financial Times, 9 Jan. 2020. [Online]. Available: https://www.ft.com/content/6346dd78-322d-11ea-9703-eea0cae3f0de. [Accessed 18 Jul. 2020].
10. Jackie Fenn and Alexander Linden, 'Understanding Gartner's Hype Cycles', Gartner, Inc., 20 May 2003, 88.
11. Ozgur Dedehayir and Martin Steinert, 'The hype cycle model: A review and future directions', in 'Technological Forecasting and Social Change, Vol. 108, 2016, p. 28-41. [Online]. Available: https://www.researchgate.net/publication/301757818_The_hype_cycle_model_A_review_and_future_directions. [Accessed 18 Jul. 2020].

12. James Rennie, 'Have we reached Peak Drone?', Australian UAV (AUAV), 4 Jun. 2019. [Online]. Available: https://www.auav.com.au/articles/auav-predictions-peak-drone-2019/. [Accessed 26 Apr. 2020]
13. Joline Culus, Yves Schellekens, and Yannick Smeets, 'A drone's eye view - Overview of the Belgian UAV ecosystem & the development of commercial drone applications in Belgium', PwC Belgium and Agoria, May 2018. [Online]. Available: https://www.pwc.be/en/documents/20180801-drones-eye-view-v2.pdf. [Accessed 26 Apr. 2020].
14. 'Military air base protection: Safeguarding troops, assets and supply lines', Hensoldt. [Online]. Available: https://www.hensoldt.net/what-we-do/security/military-base-protection/. [Accessed 4 May 2020].
15. Bruno Oliveira Martins, Arthur Holland Michel, and Andrea Silkoset, 'Countering the Drone Threat – Implications of C-UAS technology for Norway in an EU and NATO Context', Peace Research Institute Oslo (PRIO), 2020. [Online]. Available: https://www.prio.org/utility/DownloadFile.ashx?id=2013&type=publicationfile. [Accessed 4 May 2020].
16. 'Interim Report of the Emerging Technologies Subcommittee', US Homeland Security Advisory Council, 21 May 2019, 20. [Online]. Available: https://www.dhs.gov/sites/default/files/publications/ope/hsac/19_0521_hsac_final-hsac-emerging-technology-interim-report.pdf. [Accessed 26 Apr. 2020].
17. Arthur Holland Michel, 'Counter-Drone Systems', 2nd Ed., Center for the Study of the Drone at Bard College, Dec. 2019. [Online]. Available: https://dronecenter.bard.edu/files/2019/12/CSD-CUAS-2nd-Edition-Web.pdf. [Accessed 26 Apr. 2020].
18. 'One Year of Drone Partnerships', Drone Industry Insights (DRONEII), Aug. 2017. [Online]. Available: https://www.droneii.com/project/drone-partnerships-gone-wild. [Accessed 4 May 2020].
19. Ibid. 15.
20. 'Tech Area of Interest: Installation Counter Unmanned Aerial Systems (CUAS)', NC Deftech, 11 Mar. 2019. [Online]. Available: https://deftech.nc.gov/blog/2019/03/11/tech-area-interest-installation-counter-unmanned-aerial-systems-cuas. [Accessed 26 Apr. 2020].
21. Ibid. 17, 11.
22. Stephen Bryen, 'Russian Pantsir systems neutralized in Libya', Asia Times, 23 May 2020. [Online]. Available: https://asiatimes.com/2020/05/russian-pantsir-systems-neutralized-in-libya/. [Accessed 18 Jul. 2020].
23. Kristina Hummel, 'A View from the CT Foxhole: Vayl S. Oxford, Director, Defense Threat Reduction Agency', CTC Sentinel, Vol. 12, Mar. 2019, p.10-14. [Online]. Available: https://ctc.usma.edu/view-ct-foxhole-vayl-s-oxford-director-defense-threat-reduction-agency/. [Accessed 18 Jul. 2020].
24. Ibid. 17.
25. Ibid. 14.
26. Ibid. 16.
27. Paul Verlaine Gakne and Kyle O´Keefe, 'Tightly-Coupled GNSS/Vision Using a Sky-Pointing Camera for Vehicle Navigation in Urban Areas', MDPI, 2018. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5948580/. [Accessed 18 Jul. 2020].
28. Ganesh Balamurugan et al., 'Survey on UAV navigation in GPS denied environments', 2016, 198–204.
29. F. Maiwald et al., 'Using LTE networks for UAS-communication', in '36th European Telemetry and Test Conference', 2016, 3958–3963.
30. Mi Li, Yifeng Hong, Cheng Zeng, and Yuejiang Song, 'Investigation on the UAV-To-Satellite Optical Communication Systems', in 'IEEE Journal on Selected Areas in Communications', Vol. 26, no. 9, Sep. 2018. [Online]. Available: https://www.researchgate.net/publication/327000758_Investigation_on_the_UAV-To-Satellite_Optical_Communication_Systems. [Accessed 18 Jul. 2020].
31. Akhilesh Kumar Jha, S. Sathyamoorthy, and ViswaPrakash, 'Bird strike damage and analysis of UAV's airframe', in 'Procedia Structural Integrity', Vol. 14, 2019, 416–428. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S245232161930054X. [Accessed 18 Jul. 2020].

32. Coningsby J. Burdon, 'Hardening Unmanned Aerial Systems against High Power Microwave Threats in Support of Forward Operations', Air Command and Staff College, Air University, Apr. 2017. [Online]. Available: https://apps.dtic.mil/dtic/tr/fulltext/u2/1042082.pdf. [Accessed 18 Jul. 2020].
33. K. Misovec et al., 'Low-observable nonlinear trajectory generation for unmanned air vehicles', in '42nd IEEE International Conference on Decision and Control', Vol. 3, IEEE, Dec. 2003, 3103–3110. [Online]. Available: https://ieeexplore.ieee.org/document/1273100. [Accessed 18 Jul. 2020].
34. Balemir Uragun and I.N. Tansel, 'The noise reduction techniques for Unmanned Air Vehicles', in '2014 International Conference on Unmanned Aircraft Systems (ICUAS 2014) - Conference Proceedings', May 2014. [Online]. Available: https://www.researchgate.net/publication/268982899_The_noise_reduction_techniques_for_Unmanned_Air_Vehicles. [Accessed 18 Jul. 2020].
35. Scott N. Romaniuk and Tobias Burgers, 'China's Swarms of Smart Drones Have Enormous Military Potential', The Diplomat, 3 Feb. 2018. [Online]. Available: https://thediplomat.com/2018/02/chinas-swarms-of-smart-drones-have-enormous-military-potential/. [Accessed 16 Jun. 2020].
36. Zachary Kallenborn, 'The era of the drone swarm is coming, and we need to be ready for it', Modern War Institute at West Point, 25 Oct. 2018. [Online]. Available: https://mwi.usma.edu/era-drone-swarm-coming-need-ready/. [Accessed 16 Jun. 2020].
37. Pierre Lagueux, 'The defence procurement market is unlike any other', Policy Options Politiques, 12 Jan. 2016. [Online]. Available: https://policyoptions.irpp.org/magazines/january-2016/the-defence-procurement-market-is-unlike-any-other/. [Accessed 10 May 2020].
38. 'Defense Acquisition Guidebook', Defense Acquisition University, 2010. [Online]. Available: http://www.acqnotes.com/Attachments/Defense%20Acquisition%20Guidebook.pdf. [Accessed 10 May 2020].
39. Harvey M. Sapolsky, 'Let's Skip Acquisition Reform This Time', Defense News, 9 Feb. 2009, 29.
40. Ibid. 37.
41. Ibid. 37.
42. John R. Hoehn and Kelley M. Sayler, 'Department of Defense Counter-Unmanned Aircraft Systems', Congressional Research Service, 29 Jun. 2020. [Online]. Available: https://fas.org/sgp/crs/weapons/IF11426.pdf. [Accessed 18 Jul. 2020].
43. 'Europäischer Verteidigungsfonds', Europäische Kommission, 19 Mar. 2019. [Online]. Available: https://ec.europa.eu/commission/news/european-defence-fund-2019-mar-19_de. [Accessed 10 May 2020].
44. Ibid.
45. 'Counter Unmanned Aerial System (C-UAS)', European Permanent Structured Cooperation Framework (PESCO). [Online]. Available: https://pesco.europa.eu/project/counter-unmanned-aerial-system-c-uas/. [Accessed 6 Jun. 2020].
46. '2019 calls for proposals: European defence industrial development programme (EDIDP)', European Commission, 19 Mar. 2019. [Online]. Available: https://ec.europa.eu/research/participants/data/ref/other_eu_prog/edidp/wp-call/edidp_call-texts-2019_en.pdf. [Accessed: 6 Jun. 2020].
47. NATO Countering Class I Unmanned Aircraft Systems Handbook, NATO C-UAS Working Group, 2020.
48. Final Report on NIAG Study Group 200 on Low, Slow and Small Threat Effectors, NATO Industrial Advisory Group, 2017.
49. Joseph Trevithick, 'The Pocket-Sized Black Hornet Drone Is About To Change Army Operations Forever', The War Zone, 6 Feb. 2019. [Online]. Available: https://www.thedrive.com/the-war-zone/26359/the-pocket-sized-black-hornet-drone-is-about-to-change-army-operations-forever. [Accessed 8 Jun. 2020].
50. Ibid. 17.
51. Ibid. 17.
52. Valerie Insinna, 'The US Air Force's radical plan for a future fighter could field a jet in 5 years', Defense News, 16 Sep. 2019. [Online]. Available: https://www.defensenews.com/digital-show-dailies/2019/09/16/the-us-air-forces-radical-plan-for-a-future-fighter-could-field-a-jet-in-5-years/. [Accessed 18 Jul. 2020].

25

By Captain Dan Cochran, US N
By Lieutenant Colonel Andreas Schmidt, GE AF
Joint Air Power Competence Centre

Employing Friendly UAS for Counter-UAS Operations

Introduction

Unmanned aircraft (UA) are an established technology that continues to expand. Over the past decade, UA have become an integral component in most militaries and future military operations must consider Friendly-UA (F-UA) and Opposing-UA (O-UA) capabilities. It has to be assumed that O-UA have similar capabilities to F-UA, able to deliver kinetic and non-kinetic effects in addition to Intelligence, Surveillance, and Reconnaissance (ISR). Therefore, O-UA actions must be planned for in all operations, including considering contingencies. As described in Chapter 7 (cf. p. 107 ff.) about the role of Surface-Based Air and Missile Defence (SBAMD) systems, there currently exists an initial capability to target the majority of Unmanned Aircraft System (UAS)

components individually. In addition to SBAMD, manned aircraft performing Defensive Counter-Air (DCA) missions train to engage larger UA in the Class II and Class III[i] categories, however, both of these defence assets are scarce resources within NATO and Counter-Unmanned Aircraft Systems (C-UAS) is just one of their many requirements. In order to augment relatively limited SBAMD systems and DCA aircraft, F-UA have the potential to be an excellent C-UAS platform for many scenarios. The following paragraphs will look at F-UA applications for the C-UAS mission. Once these applications are described broadly, the paper will address how F-UA may be employed to defend against O-UA conducting DCA and Offensive Counter-Air (OCA) missions.

In an attempt to counter opposing unmanned aerial systems, friendly forces may target any one or many of its critical system components (cf. Figure 1.1, p. 13).

Although there is work being done to build a capability to target components other than the UA,[1] Allied tactics currently focus on targeting the O-UA with SBAMD and manned DCA aircraft at ranges that are sufficient to prevent the O-UA from completing its mission. Since this approach relies upon defeating a single component of the UAS, which is also the component that often has a large number of required targets, this approach may be considered inefficient compared to targeting more critical components such as the C2 element or the data link. Hence, after discussing the challenges of targeting O-UA, this chapter will expand on countering the other components of the opposing UAS by utilizing F-UA for OCA missions.

[i] The NATO UAS classification methodology is described in Annex A.

Detecting the Unmanned Aircraft

Detecting the threat is the first link in the kill chain. Surface-based detection assets such as active radars and passive receivers are generally very powerful and work well to detect Class II and III UA. The primary deficiencies of using ground-based detection assets are that they are susceptible to target terrain-masking (blind zones) due to topography and that they are also relatively slow to redeploy as compared to O-UA and other manoeuvrable enemy forces. Detecting the target from an airborne asset can greatly reduce these issues. Although manned aircraft are capable of executing the C-UAS mission against Class II and III UA, there are many reasons to look at using F-UA for C-UAS missions. F-UA are more tailorable to specific mission requirements in terms of size and function, including options that, due to small physical size, could not carry a human. In addition, unmanned platforms can be tasked for higher risk missions in that they are perceived as more expendable. F-UA employed in tactically advantageous positions, with active or passive sensors, would be able to substantially reduce blind zones in the coverage provided by ground-based sensors. Additionally, F-UA have the potential to deploy and reposition as required to counter adversarial manoeuvres much more quickly than ground-based detection systems. In addition to those advantages, UA create the potential for more effective, highly-automated tactics to be employed through the use of artificial intelligence and machine learning. Vulnerabilities of UAS include the requirement for multiple data links that need to be maintained at various levels (which can be exploited), in addition to smaller antennas and substantially less energy available for transmissions as compared to ground-based assets (especially for Class I and II UA). The optimal solution to enable O-UA detection is likely a combination of tactically placed ground units augmented by the appropriate number of F-UA sensors, based on the topography and size of the area being defended.

Classifying the Unmanned Aircraft

Once a potential target is detected, it must be classified and identified, based on Rules of Engagement (ROE) and supplemental plans and procedures to determine the correct response. This determination is so critical in the kill chain that automated classification is often a concern due to trust issues as well as legal, moral and ethical principles. Although many nations are comfortable with machine derived classifications[2], they require these systems to be supervised by human operators who interpret the complex tactical and strategic situations to determine the classification. Although this current approach may reduce the occurrence of collateral damage and fratricide, there are some obvious drawbacks. The first drawback to requiring humans in the classification process is that in future scenarios, with fast-paced operational tempos, humans could slow down the decision making process, hence decreasing effectiveness. The second is if communication is lost from the forward-deployed UA, the human commands would not be issued to the UA. With fully-automated classifications allowed, F-UA may be able to classify the contact as hostile and work with other assets to neutralize the threat in situations that necessitate quick actions. The level of human control over UA classification systems in the future must continue to be evaluated to weigh the risk between fratricide and failure to provide adequate defence from a credible threat.[3]

Engaging the Unmanned Aircraft and Payload

Once a contact is classified such that it can be engaged, the appropriate actions to neutralize the threat need to be determined. Again, surface-based solutions have the potential benefit of having more capable defences such as long-range interceptors or high-power

directed energy weapons. As previously mentioned, blind zones and relatively limited manoeuvrability can be supplemented by F-UA to mitigate the gap and to create a layered defence. When defending against O-UA, especially swarm and emergent attacks, the use of F-UA is desirable as they are more plentiful, agile, and likely cheaper than traditional air defence assets. The use of F-UA could also lead to optimized weapons for C-UAS, including a self-destruction option that involves directly impacting O-UA.[4] F-UA may provide a better defence as compared to manned aircraft, especially when the mission requires long 'on-station' or dwell time or necessitates operating in highly contested airspace. In addition, the flexibility of F-UA allows for air operations to be conducted in areas with limited access to logistic support, where conducting manned flight operations isn't feasible. Synchronizing the use of unmanned and manned assets, while prioritizing the unmanned assets to complete the most hazardous missions, will allow for more creative, flexible, and effective engagement solutions.

It is always preferable to engage offensive aircraft before they are able to release their payload since this approach is more efficient and survivable. In most cases, the offensive aircraft will release multiple individual weapons that may be more difficult to engage than the aircraft itself, in addition to the reduction in available friendly response time once the weapon is employed. If weapons are released, then F-UA may be critical to the survival of the defended asset. Utilising characteristics of UA already discussed, they could be positioned in tactical locations, supplementing existing manned defences. If adversarial tactics involve saturating friendly defences with a high number of weapons, F-UA may be employed as a flexible response in numbers sufficient to negate the threat. When large numbers of credible threats need to be prioritized and eliminated quickly, high-automated defences could be the most survivable option and will be discussed next.

Acknowledging known concerns, engaging all threats (both hostile aircraft and incoming weapons) through highly-automated systems has many advantages. With a high concentration of threats executing complicated tactics and composed of a variety of weapons, a properly monitored autonomous system may be the best solution. A highly-automated architecture may be more effective at managing the Command and Control (C2) of vast friendly offensive and defensive systems simultaneously than human-in-the-loop systems. Legal and ethical concerns remain within many nations when employing any effects without human consent.[5] In addition, highly-automated C-UAS C2 systems will need to be interoperable with all other overarching and potentially coexisting C2 systems.

Employing Friendly-UA for the Defensive Counter-Air Mission

Defensive Counter-Air (DCA) operations protect friendly forces and vital interests from adversary air and missile attacks. It consists of all active and passive air defence operations to detect, identify, intercept, and destroy or make ineffective, adversary air and missile forces attempting to attack or penetrate friendly airspace.[6] In a typical DCA scenario, a high-value asset (mobile or stationary) is defended from threats originating from a specific direction. Many aspects of a typical DCA mission indicate UA may be well equipped to fill the defender role. These aspects include relatively short distances for communication and support, with F-UA either prepositioned or launched upon threat detection. For example, if the threat is assessed as capable of launching an O-UA swarm attack with little friendly indication and warning (I&W) capacity, F-UA assets could be placed in multiple layers along the threat sector in order to provide layers of defence

as well as relaying initial indications of the threat to follow-on layers. Forward deployed positions of F-UA also offer the opportunity to detect and engage from behind the attacking aircraft once the attacking aircraft has passed their location and are between the F-UA and the defended asset. Considering that the majority of low observable technology (which will also be incorporated into future O-UA[ii]) concentrates on reducing detectable signatures in an aircraft's forward quadrants, having F-UA able to detect (and potentially engage) from the rear quadrants could greatly improve overall air defence capabilities.

Employing Friendly-UA for the Offensive Counter-Air Mission

Offensive Counter-Air (OCA) consists of offensive operations to destroy, disrupt, or degrade adversary air and missile capabilities, either before or after launch.[7] With regard to C-UAS, this involves the enemy's ground control stations and satellite ground terminals as well as other communication nodes. Moreover, it includes all the logistics and supporting infrastructure which is necessary to operate O-UA. Therefore, a typical OCA mission will involve friendly missiles and/or aircraft entering contested airspace in order to engage enemy aircraft and missiles in their own territory. OCA by manned aircraft in support of C-UAS is also discussed in Chapter 8 (cf. p. 129 ff.). An OCA mission can be characterized as involving longer flight distances than typical DCA missions, which may be more of a challenge for small, inexpensive F-UA. Typical inexpensive UA have somewhat limited range and speed in addition to

[ii] Annex B lists some examples of Russian and Chinese low-observable UAS.

substantial vulnerability to EMS jamming, since they are utilizing less secure or even unprotected data links for mission accomplishment than larger, more expensive UA. A possible solution to these limitations could be enabling the F-UA to proceed autonomously after launch (minimizing the consequences of EMS attacks) in addition to planning 'one-way' missions where the entire range of the system can be utilized without saving fuel for the return trip. These kinds of missions could enable F-UA OCA missions to be effective at degrading O-UA capability before they can be used against friendly forces.

One concept for employing F-UA[8] while optimizing logistics and minimizing costs for the OCA mission is to utilise 'plug-and-play' payloads in a standard F-UA airframe and employ them to create synergistic effects. The type and number of mission-configurable F-UA platforms would be determined based on anticipated enemy defences and desired effects, similar to today's (manned) Composite Air Operations (COMAO) strike planning. F-UA could supplement or completely replace manned aircraft for certain missions within the OCA package. For instance, instead of sending multiple manned Airborne Electronic Attack (AEA) aircraft along with manned escort aircraft to provide Suppression of Enemy Air Defences (SEAD), an OCA package could utilize F-UA configured for the AEA mission to accomplish the task. With potentially a larger number of F-UA available to complete the SEAD mission, combined with being able to assume more risk to adversary air defences (able to operate in more contested airspace and without escort aircraft), F-UA may prove to be a much better solution than the current manned options. The challenges to this kind of coordinated attack include strike planning with assets possibly having large differences in transit speed and other characteristics. However, considering the benefits of using F-UA for other missions within the COMAO, it's feasible to imagine an OCA

package being made up completely of (mission-configurable) F-UA at some point in the future. The majority of the F-UA in the COMAO could be designed from the same basic UA but loaded with mission-specific interchangeable payloads and connected to a sophisticated C2 system. The F-UA could be programmed with contingency plans, including various levels of lost communications. If the link to human monitored C2 was severed, the COMAO could be programmed to make decisions autonomously based on shared information within the 'swarm'. If the inter-flight link was severed, each F-UA would individually execute their lost-communications contingency orders, tailored to the tactical scenario. The future degree of human control required for large scale operations, such as COMAOs, should continue to be evaluated based on the level of trust of the systems being employed and acceptable risk to unintended actions of these systems if automated.[9]

F-UA for Self-Defence

F-UA may be well suited to help defend systems and personnel from O-UA in a self-defence scenario.[10] O-UA have the potential to be employed against aircraft from short distances and with little warning, especially when the location of the manned aircraft is predictable due to the use of standard air routes and regularly scheduled missions. For example, O-UA could be employed under airport approach corridors or near frequently flown paths such as low-altitude training routes. Rotary-wing aircraft are especially vulnerable since they are typically slower and lower than most fixed-wing aircraft. In addition to air assets, ground-based assets are also vulnerable to no-warning attacks, when their future locations are predictable. Even if some level of early warning is available, it seems feasible that specially designed O-UA could be capable of defeating most layers of friendly defences. It is

reasonable to assume that F-UA could be highly effective in providing self-defence, in a similar fashion to traditional expendables such as chaff or flares that are used in a final attempt to defeat an incoming weapon. If a threatened asset, from a major weapon system to an individual soldier, senses an O-UA attack, they could employ their own UA in self-defence. Self-defence F-UA is not the only solution to C-UAS, but should be considered as a complement to other defences and could provide a very versatile and affordable option. For example, 'Hunter' F-UA which are capable of catching O-UA and safely manoeuvring them to a safe spot, could also augment the perimeter of Short-Range Air Defence Systems if the ROEs are very restrictive and collateral damage or public safety is a concern.[11]

Engaging the C2 and Operator Elements

One significant benefit of unmanned systems is that the C2 element and operator are not primarily affected by the destruction or detection of the UA itself. Deploying a new UA restores full operational capability. The C2 component is not as redundant as other components (such as the UA), which makes locating and neutralising them paramount. In the case where the C2 element is controlling the UA via RF transmissions, the C2 element or transmission hubs may be located by passive RF detectors. F-UA are especially qualified to perform the detection mission, since their elevated position enables them to detect transmissions over a wide field-of-regard and they can provide target location via triangulation. Additionally, once transmissions are sensed the F-UA may be able to call for additional F-UA in order to obtain more precise triangulation coordinates or execute a coordinated mission.

Engaging the Data Link

Having already discussed how F-UA may be used to defeat the other components of an adversary's UAS, F-UA could also be used to target the data link and other communications between the UAS nodes. The effects of the attack could result in data link denial or manipulation of transmissions to disrupt their operations. These kinds of effects may be easier to achieve on traditional omnidirectional emitter-receiver systems, but they may also be possible for directional communication links. Especially with agile F-UA, it could be feasible to position them in between the O-UA and its C2 element or relay hub. Even when the data link is relayed by satellite, a very high-altitude UA (also known as Pseudo Satellites) might be able to cause the same effect.

Summary

Unmanned platforms show significant promise in conducting effective C-UAS operations in conjunction with surface-based and airborne manned platforms. F-UA are able to complement or supplement existing efforts to defeat the individual components of an adversary's UAS, while also bringing new capabilities. The use of F-UA has the potential to dramatically increase overall C-UAS capacity while increasing survivability of manned offensive and defensive assets. Since all future adversaries, from small terror organisations to peer competitors, are currently using or plan to use UAS, a reliable, modern, and robust set of answers needs to be developed. Due to the wide variety of UAS and potential missions, C-UAS will also require a comprehensive range of counter-techniques. During this analysis, the level of automation afforded to human-machine-teaming must be considered, including balancing the operational, ethical, and legal aspects.

Endnotes

1. André Haider, 'A Comprehensive Approach to Countering Unmanned Aircraft Systems', Joint Air Power Competence Centre (JAPCC), 2019. [Online]. Available: https://www.japcc.org/portfolio/a-comprehensive-approach-to-countering-unmanned-aircraft-systems/. [Accessed 13 Aug. 2020].
2. Robin Geis, 'The International-Law Dimension of Autonomous Weapons Systems', Friedrich Ebert Stiftung, Oct. 2015. [Online]. Available: http://library.fes.de/pdf-files/id/ipa/11673.pdf. [Accessed 13 Aug. 2020].
3. Considerations for Combat UAS, Automation and Human Interaction can be found in André Haider, 'Remotely Piloted Aircraft Systems in Contested Environments', JAPCC, Sep. 2014, p. 101 ff. [Online], and further in André Haider, 'Future Unmanned System Technologies - Legal and Ethical Implications of Increasing Automation', JAPCC, Nov. 2016. [Online]. Both available: https://www.japcc.org/publications/. [Accessed 13 Aug. 2020].
4. David Hambling, 'See Raytheon's Jet-Powered Interceptor Drone In Action', Forbes, 7 May 2020. [Online]. Available: https://www.forbes.com/sites/davidhambling/2020/05/07/raytheon-coyote-drone-jet-powered-interceptor/#4bc9d9704885. [Accessed 13 Aug. 2020].
5. Ibid. 3.
6. Allied Joint Doctrine for Air and Space Operations (AJP-3.3), Ed. B, Ver. 1, NATO Standardization Office (NSO), Apr. 2016.
7. Ibid.
8. Zachary Kallenborn, 'The era of the drone swarm is coming, and we need to be ready for it', Modern War Institute at West Point, 25 Oct. 2018. [Online]. Available: https://mwi.usma.edu/era-drone-swarm-coming-need-ready/. [Accessed 31 Jul. 2020].
9. Ibid. 3.
10. Ibid. 4.
11. 'Drone Hunter: The World's Premier AI-enabled Interceptor Drone', Fortem Technologies, 13 Aug. 2020. [Online]. Available: https://fortemtech.com/products/dronehunter/. [Accessed 13 Aug. 2020].

26

By Dr James Rogers, UK
Centre for War Studies at the University of Southern Denmark

Future Threats: Military UAS, Terrorist Drones, and the Dangers of the Second Drone Age

Introduction

The State of the Art of War

The world has entered the 'second drone age'.[1] Defined by the global proliferation of military Unmanned Aircraft Systems (UAS) and weaponised commercial drones, this new era of drone warfare has seen, and will continue to see, both state and non-state actors competing for power in the skies above (and beyond) designated zones of conflict. Hostile actors, with threatening remotely operated air power components, now vie for command of the air against NATO and allied forces. Civilian populations are at increased risk in this adjusted state of war. Ethical controversies from the first drone age have been exacerbated by the widespread use of distant lethal robotics, making

it difficult to distinguish between the perpetrators of drone atrocities and attacks or accidents. This 'deniability' has important political, legal, and strategic implications. Holding actors to account, or retaliating against belligerents, is difficult in this deniable, multi-user context, where similar, if not identical systems, are deployed by myriad disparate actors. The second drone age also poses broader implications for international security, stability, and Great Power politics. Decisions about who joins the 'global drone club' are not made by accident, especially where the transfer of military UAS is concerned. The unrestricted supply of armed UAS to surrogate, partner, and proxy actors by state suppliers – of which China is one of the most prolific – will influence the fate of nations. As recent 'State versus State' drone wars in the Caucasus and Libya show, the politically motivated supply of military UAS has contributed to international instability and conflict escalation. The supply of both commercial and military-grade remote technologies to non-state actors, allegedly by countries like Iran or through commercial shell companies, exacerbate the manifest threats present in this altered security environment. The relaxation of commercial drone regulations in reaction to COVID-19 will only exacerbate this problem as belligerents seek to move against perceived weak-points. Put simply, new 'Drone Powers', and the 'new drone world', present fundamentally different challenges to those faced during the first drone age.[i]

The First Drone Age

The American monopoly over the use of military UAS defined the first drone age, with Western powers deploying remote aerial

[i] In line with the stated aims of this book, all cases chosen within this chapter reflect current and emerging challenges faced by the NATO allies. The inclusion of non-state and state drone threats to cities is includes to highlight the broader threat to NATO member states and the threat manifest within urban environments in zones of conflict. Finally, the inclusion of the term 'unmanned' is in line with the editor's definition of UAVs and drones.

technologies in largely uncontested airspace. Operated by the United States (US) military, the Central Intelligence Agency (CIA), and the militaries of select allies, these systems were used to hunt and kill those defined as terrorists and insurgents inside and outside designated regions of active conflict. They were (and are) also used to provide close air support and over-watch for friendly forces deployed as part of the Global War on Terror (GWOT). UAS like the Predator, Reaper and unarmed Global Hawk became symbolic of a post-9/11 period where military robotics surged forward to become the spearhead of American and allied force deployment. There can be little doubt that these systems were deemed to be both politically and militarily effective. By the time President Obama came to power in January 2009, the US had lost at least 625 soldiers in Afghanistan and 4,221 personnel in Iraq.[2] In 2010, the Improvised Explosive Device (IED) was responsible for 60 per cent of American casualties in Afghanistan alone.[3] In this high-risk and dangerous context of Asymmetric Warfare, UAS provided the ability to transcend the threats on the battlefield, whilst simultaneously extending the operational reach of American military power to regions previously deemed too hostile or too difficult to operate in with large deployments of American personnel. As part of a broader 'Remote Warfare',[4] or as Thomas Waldman has termed it a 'Vicarious Warfare' modus operandi, UAS were used in tandem with small detachments of Special Operations Forces (SOF), military training units, manned air power assets, and larger groups of local forces who bore the brunt of the risk.[5] In this context, UAS played a central role as a 'panacea weapon' for President Obama, who was faced with a mounting fatality count and growing public unease about the wars America was committed to.[6]

The rise of UAS, went hand in hand with – or as Clausewitz may have put it, 'was a continuation of' – the casualty-fatigued politics of the 2010s.[7] Yet, whilst these unmanned systems remained

popular with the American people and many political leaders,[8] concerns were raised by human rights groups who argued that the increasing use of UAS made killing too easy.[9] This 'easiness' was mostly due to concerns over lowering the threshold in the use of force, as raised by organisations like PAX.[10] Alongside this, NGOs concerned with civilian protection claimed that UAS had broader gendered, traumatic, and economic effects on the populations they operated high above; well beyond those of the initial kinetic precision strike.[11] Claims of statistical inaccuracy were also made. When it came to the counting of the dead, Non-Governmental Organizations (NGOs), such as AirWars and The Bureau of Investigative Journalism (TBIJ), asserted that American and allied UAS strikes were responsible for killing thousands more civilians than officials would admit.[12] Even senior administration staff worried about the growing reliance on UAS. Former US Secretary of Defence Robert Gates noted that US defence leaders had the tendency to view the use of force by UAS as 'bloodless, painless, and odourless',[13] meaning deadly strikes may be used more frequently and as a first resort.[14] Despite these concerns, however, during the first drone age, the prevailing wisdom was that UAS fulfilled an effective military and political role for the US. This role continued into the Trump administration, where UAS were consolidated in their position as the go-to military assets when facing America's foes. Most notably, during the Trump era, new regions of active armed conflict were defined and there were re-interpretations of those designated as a terrorist.[15] The Trump Administration also loosened the restrictions on the use of drone strikes, decentralizing command over strike decisions. One consequence of these changes was an increase in UAS strikes in places like Somalia and the first targeted killing of a state actor – General Qassem Soleimani, the head of the Iranian Revolutionary Guard Corps (IRGC).[16] In the second drone age, such precedents will lead to new norms in the deployment of UAS by other state and non-state actors, ones which are likely to travel full

circle and challenge the security of NATO states, state representatives, and civilian populations. These are the first of many worrying trends that will emerge with the global spread of UAS.[17]

The Global Spread of UAS

Power, Proliferation, and Escalation

It will come as no surprise that the perceived successes and sheer scale of the US and allied UAS deployments have combined to make UAS systems an attractive military investment. If the first drone age was defined by the US and its allies setting broad standards and norms for UAS use, then the second drone age will be defined by a diverse mix of new UAS actors – some friendly and some hostile – copying established forms of deployment and pushing those very same standards and norms to their limits. Whole new practices – some troubling and some improved – will also be formed, altering the character of conflict. As this section explains, the second drone age will see nation-states capitalizing on the global proliferation of military UAS, providing state militaries with a viable, and often far too easy capacity to deliver death from above. This will challenge traditional notions of Asymmetric Warfare and the effectiveness of a NATO-allied deterrence posture.[18]

To be specific, 102 nation-states now operate a various assortment of military UAS.[19] In 2010, just 60 nations possessed these unmanned aerial technologies.[20] To put these figures into perspective, this equates to a 70 percent increase in the number of state militaries operating armed or unarmed UAS capabilities. When we drill down a little deeper into these statistics, provided by the Centre for the Study of the Drone, it can be seen that out of these 102 states, around 40 possess, or are in the process of purchasing, large UAS

with the capacity to launch deadly attacks.[21] These include, but are not limited to, Israel, Iraq, Iran, the United Kingdom, the US, Turkey, France, the United Arab Emirates, Saudi Arabia, Egypt, Nigeria, and Pakistan, all of whom have, according to the United Nations (UN), operated UAS for targeted killings or close air support.[22] Such figures are useful, as they help highlight the extent to which the skies above contested regions have become more congested in recent years. For example, in June 2020, Azerbaijan was added to the select list of nations who have deployed armed UAS in anger as the Caucasus descended into a novel state of warfare where all actors deployed and shot down each other's UAS. Armenia and Azerbaijan re-ignited old border clashes, fighting in close proximity to Nagorno-Karabakh.[23] In the second drone age, the choice to resort to military UAS as a low-cost, and seemingly low-risk, option is becoming an increasingly common decision. Yet, any precision UAS strike has broader political implications, unintended consequences, and unforeseen 'costs'. No matter how kinetically precise and 'surgical' a UAS strike may be, it always generates ripples that can exacerbate conflict or spark broader hostilities in the longer term. This is something to keep in mind as we examine the motivations behind the supply of military UAS.

Supply and Demand

In this new epoch of UAS proliferation, the old interconnected issues of state power projection and the supply of military technologies have re-emerged. As with any international arms deals, especially those concerned with high-tech weapons systems, strategic considerations and state power interests combine to influence the procurement process. It just so happens that China, a Great Power known for playing politics with technology, is one of the world's top three suppliers of military UAS and with each sale comes an attempt at Chinese power projection.[24] According to data from

September 2019, '[t]hirty-two countries operate at least one drone made in China'.[25] These include Egypt which operates 60 UAS, Saudi Arabia which has 70, and the UAE which owns 40.[26] This group of states has been specifically selected for analysis within this chapter as they are all involved in the Libyan Civil War. Combined, they provide considerable operational or air power support to the forces of Field Marshal Khalifa Haftar in the Libyan National Army's (LNA) fight against the UN-recognized Government of National Accord (GNA).[27] As this conflict has raged on, it has become clear that visions of the second drone age are being played out in front of an international audience of concerned states, NGOs, and Intergovernmental Organizations (IGOs).

This is not to say that China wishes to push a particular outcome in the Libyan Civil War, in a traditional proxy fashion, by supplying UAS to these allied states. Instead, it comes back to economics and the correlating factor that each state supplied by China is a member of the Chinese Belt and Road Initiative (BRI). As one recent study by the London School of Economics (LSE) found '[...] the Belt and Road Initiative (BRI) has gradually come to assume the status as China's flagship global development strategy [...] UAVs have been part of an attempt to develop and consolidate diplomatic relationships with recipient states'.[28] In fact, when it comes to the Middle East and North Africa most specifically, the LSE study found that the key drivers of Chinese UAS sales relate to Beijing's 'overseas investments in potentially volatile markets, and [are used to] potentially consolidate diplomatic relationships'.[29] The key takeaway here for NATO countries is that in future conflict, where there are Chinese economic interests or Chinese BRI partners, Chinese UAS will be present. Another point worth noting here is that these UAS are not entirely separate from Chinese personnel upon their sale to the recipient state. As interviews with US military officers deployed in Iraq reveal, it is possible to have

Chinese contractors helping to support Chinese-supplied UAS.[30] This was evident in Iraq, where the Iraqi military purchased, and deployed, Chinese made CH-4B armed UAS in the fight against the so-called Islamic State of Iraq and Syria (ISIS). This led to a situation where Chinese personnel were cohabiting on-base with US personnel and allied assets as both missile defence and offensive UAS systems were deployed against a common enemy.[31] At a time when there are concerns about US government-owned Chinese commercial drones and the communications provider Huawei sending information back to Beijing – as well as hacking and state espionage – this process of UAS providing a gateway to on base Great Power cohabitation may wish to be reviewed and limited.[32] In essence, the Chinese sales of UAS are a continuation of the economic ambition, military nouse, and shrewd political manoeuvring that defines Chinese power projection. If we return to the analysis of the Libyan Civil War, it can be seen how these elements combine to fuel tension and pose serious threats to NATO member states.

The Libyan Crucible[33]

The Libyan Civil War can be recognized as one of the first few conflicts where a UAS armed state has faced another UAS armed state in conflict. As such, it presents a window into the future of how UAS will be supplied, deployed, and countered by state militaries. As the UN's Special Representative to Libya, Ghassan Salame, stated, the conflict has grown to become 'the largest drone war in the world'.[34] UAS have played a major role in the conflict. It was no coincidence that up until December 2019 Field Marshal Haftar's forces were making considerable gains against the GNA thanks to support from Chinese-manufactured, Chinese-supplied, yet UAE and Saudi-operated armed Wing Loong-IIs with a range of 4,000 km.[35] Haftar's fate, nevertheless, changed as of mid-2020, with the increasing impact of Turkey in the conflict on the side of

the GNA.[36] Indigenously manufactured Turkish UAS have had a major influence on the conflict. UAS, like the armed Bayraktar TB2, have helped the GNA push to take back major airfields, strike supply lines, and target opposing forces.[37] There are, however, some technical limitations to the Turkish deployment of TB2 UAS.

Turkish manufactured TB2s have a shorter signal connection range when compared to Chinese manufactured Wing Loong-II systems. The Bayraktar TB2 may have an impressive flight time of up to 27 hours and can carry a 150 kg payload (according to the manufacturer), yet its range is limited to 150 km.[38] This is because these indigenously made Turkish UAS are reported to have a 'line-of-sight datalink'.[39] Ground Data Terminals (GDT), which act as a communication relay between a Ground Control Station (GCS) and the TB2 UAS, have been used in the field to extend the operational range and reliability of the system.[40] Nevertheless, here lies a serious vulnerability, one that is worth noting by all NATO members in the second drone age. In a conflict where all actors have UAS precision strike capability, UAS that rely on GDT or GCS situated close to the region of active hostilities are detectable, in range, and vulnerable to attack. Iranian precision missile strikes on US and allied military targets at Ain Al Assad Airbase in Iraq in January 2020 highlighted this threat to UAS operators from hostile precision air power.[41] The attacks on NATO forces, in Libya and Iraq, illustrate the need to consider questions about where best to locate airbases, the protection of airbases, and air defence. Until recently, such considerations were confined to the hottest days of the Cold War, but with the air power threat now faced by NATO states, they are once again relevant.[42]

In fact, since Turkey has entered the fray in Libya and increased its number of deployed UAS, there has been a back and forth battle for ever more advanced air defence systems. The UAE's Wing Loong-IIs

have been especially effective at striking Turkish UAS infrastructure.[43] The downing of at least sixteen Turkish UAS occurred alongside strikes on Misurata Airbase (East of Tripoli) where Turkish UAS were operated from.[44, 45] According to the conflict monitoring, assessment, and transparency NGO (AirWars) after these strikes, Turkey attempted to move UAS operations to 'Zuwara in Libya's far east, or to Ghardabiya airbase south of Sirte'.[46] Turkey's aim was to reposition its UAS, affording the GNA 'the capability of striking targets deeper into Libya's Haftar-occupied east'.[47] Nevertheless, the sites in Zuwara and Ghardabiya were struck by forces backing the LNA, making it difficult for Turkish UAS to move there and provide effective support.[48] This being said, in July 2020 the tide appeared to turn back again in Turkey's favour, prior to UN talks due to be held in October and November 2020.

In a practice which is likely to feature in all future UAS conflicts, Turkey has reportedly bolstered its air defence systems with 'medium-range US-made MIM-23 Hawk missile systems, Hisar short-range SAMs, and Korkut antiaircraft guns' to create a 'layered defence'.[49] On top of this, Turkey has deployed its KORAL Electronic Warfare System (EWS) which is alleged to have the ability to jam the UAE's Russian made Pantsir-S1 missile radars and 'the datalink frequencies of Wing Loong drones'.[50] According to Ben Fishman and Conor Hiney at the Washington Institute, '[t]his dual jamming capability could account for the increased survivability of the GNA drone force and recent disruptions to LNA drone operations'.[51] Not only this, but in reaction to their drone deficits, Turkey has also begun advanced testing of long-range, beyond-line-of-sight satellite-guided drones like the Akinci and Aksungur.[52] Overall, therefore, the Libyan Civil War can be seen as possessing key characteristics that are indicative of future UAS conflicts. Where all major actors possess military UAS, there will be escalatory battles over air defence, electronic warfare, and UAS hardware. Yet, these

battles are not merely confined to the actors engaged in active hostilities. As the supply of Chinese, US, and Russian offensive and defensive technologies into the Libya conflict demonstrate, future 'UAS Proxy Wars' are also likely to become test grounds for rival Great Power technologies that seek to gain the advantage-edge over each other's UAS and Counter-UAS systems. The simple truth is that the ability to effectively counter and disable an enemy's UAS will help decide who wins or who loses future battles, be they during proxy or peer on peer conflicts.

The Rise and Fall of Drone Powers

The deployment of military UAS, by competing states, to regions deemed strategic chokepoints or politically important to NATO, further exemplifies the role UAS will play in future tensions. With this in mind, NATO members should look with concern at the Chinese supply of CH-92A 'Rainbow' armed UAS to Serbia.[53] Supplied with six UAS in total and operated by a Mobile Ground Control Station (MGCS), this sale further signifies Chinese power projection through the sale of UAS.[54] As NATO Secretary General Jens Stoltenberg stated in June 2020, 'this is [...] about taking into account that China's coming closer to us'.[55] The fact that Serbia, a NATO partner country, is the first European nation to deploy armed Chinese UAS is of considerable concern. According to Sebastien Roblin (Forbes), the Chinese supply of UAS reflects 'Belgrade's deepening relationship with Beijing and its plans to domestically manufacture its own armed drones'.[56] It is no coincidence that Serbia is seen by China as a major hub for its BRI in the Balkans, once again highlighting the relationship between BRI states and UAS sales.[57] With Serbia in the process of applying for European Union (EU) membership as a candidate country, there are worries in Brussels that 'Beijing could turn countries in the region into Trojan horses that would one day be European Union members'.[58] As Sten Rynning

has argued more broadly, 'China is more than just business, it's geopolitics'.[59] One final concern here should be that as part of the agreement with China, Serbia will be open to selling its own indigenously produced, yet Chinese assisted, UAS weapons technologies upon manufacture, thus further exacerbating the proliferation of Chinese UAS technologies. Significant questions need to be addressed about to whom these Chinese-Serbian made UAS will be sold, where they will fly, and how the intelligence information they collect, likely from the skies around European nations, will be used.

Looking beyond Chinese activity, the burgeoning Russian UAS market should also be of concern to NATO members. With a niche focus on both armed and unarmed military UAS that can operate in sub-zero frontiers, the growing presence of 'remote systems in remote places', is worthy of attention. The High North and Arctic regions are of specific interest here. Moscow has adopted an ambitious 15-year plan to rebuild Soviet infrastructure and construct new civil and military installations in the Russian Arctic.[60] Over 400 infrastructure projects – including revamped military bases, airports, and ports – have been completed since 2012.[61] Most notable of these – for the purposes of this chapter – are President Putin's 'Arctic UAS Squadrons' and a renewed set of Arctic airbases.[62] There are at least four Cold War-era airfields that have been converted for military UAS deployment across the mainland coastal rim of the Russian Arctic.[63] From Naryan-Mar (Nenets) in the west, 'all the way to Anadyr (Chukotka) overlooking the Bering Sea in the east', Russia has built a UAS capability that allows it to survey and track all passage through the economically expanding Northern Sea Route (NSR).[64] The Russian Okhotnik stealth UAS has also been tested in sub-zero weather conditions. According to Defence One '[a] January test flight of the 20-ton Okhotnik long-range combat UAV near Novosibirsk raised eyebrows because it took place in 10-degree Fahrenheit (-12° C) weather' signalling the

likely future deployment of this armed system to the Russian Arctic.[65] The hope for President Putin is that an economically stagnant Russia can benefit from the global climate crisis as regions of the Russian Arctic warm faster than most other parts of the world.[66] Russia's development of Arctic UAS is about deterring external interference, securing economic interests, and improving operational effectiveness in a region which is difficult for humans to operate in. Yet, with the Trump administration's decision to expand military operations in the Arctic,[67] the deployment of Global Hawks from Alaska,[68] Iceland's leasing of Israeli Hermes UAS,[69] the Danish military's continued deployment of surveillance UAS to secure Greenland,[70] and the flexing of Russian military strength towards the Scandinavian Arctic, it is clear that broader battles over information security, jamming, kinetic UAS threats, and counter-UAS seen emerging in the second drone age will spill over into the Arctic in the years to come.[71] These are not the only regions of the world where NATO powers will continue to be threatened by remotely controlled airborne technologies. The spread of hostile UAS and drones is a truly global phenomenon that will stretch from distant zones of conflict to the towns and cities of NATO members.

Hostile and Terrorist Drones

As the world trudges through a turbulent period of economic depression, increased Great Power tensions, and social unrest – much of which has been exacerbated by the novel coronavirus – it seems fitting to mention how commercial drones have risen up to take on a role of social benefit, but also social harm, in these tumultuous times.[72] Much like in war, the drone can take the place of a human on the frontline of a fight. Since the emergence of the coronavirus in 2019, drones have been used to resupply the most vulnerable, help enforce lockdowns, screen people's temperature, and deep clean a nation's streets.[73] The aim here is to remove medical

workers, community workers, and patients from other contagious human beings. Drones have succeeded in these limited roles, and as a predicable consequence, policymakers and manufactures have lauded the drone, pushing for relaxed restrictions and rapid rollout so that resilient robotic societies can flourish.[74]

It is undeniable that there is a certain utility to the drone, which in some cases can be virtuous.[75] Nevertheless, any rapid relaxation and mass roll-out of drone technologies across towns and cities should be met with caution. The dilemmas of effective drone countering in urban environments have yet to be 'fixed'. It is not known how frequency jamming counter-drone systems will impact air traffic high above populous cities,[76] or interfere with intensive care units within hospitals many miles away.[77] Counter-drone technologies currently pose as much of a legal and security threat as the drone itself in civil urban environments. In addition, there is still no comprehensive and foolproof way to distinguish 'bad drones' from 'good drones' in an urban setting. With this in mind, it is important to consider what would happen if whole new modes of national logistical,[78] transport,[79] healthcare,[80] and distribution infrastructure[81] – built around thousands of drone technologies, some identical, and others differing in size, weight, and shape – were to be quickly taken offline. Hacking, infiltration, spoofing, and nefarious use by hostile actors seeking to take advantages of the vulnerabilities of the drone age would lead to the grounding of all drones in the network, no matter how vital their role.[82] How would medical supplies continue to get to the sick and infirmed, or goods move from rural distribution centres to inner-city hubs? To what extent would safe and secure drone commuter transit be compromised, and how would a disquieted public learn to put trust back into a drone infrastructure? National, regional, and local drone management structures need to be constructed and counter technologies adequately tested and invested in, so that they can

keep pace with high-tech, high-cost commercial advancements.[83] Until these measures are in place, the social and economic 'costs' of a rushed en masse embrace of drone technologies will vastly outweigh the proposed benefits.[84]

There are countless examples that help illustrate the above-mentioned risks and threats. The Japanese 'atomic drones' flown on to the Japanese Prime Minister's residence in 2015,[85] the ISIS 'Trojan Horse drones' used against allied forces in Iraq and Syria,[86] the 2018 Venezuelan 'assassination drones' used against President Maduro,[87] and the drone chaos that occurred at London's Gatwick airport later that same year, all offer pertinent reminders of how the drone can violate the most secure governmental or military sites.[88] Nevertheless, in more recent years commercial drone technologies, and their related control software, have advanced at a pace opening a whole new range of novel threats and further exacerbating drone dangers. Whereas commercial drones were once low, slow, short-range, and flown in ones and twos, they now fly faster, further, higher, and can be piloted in synchronicity with many other drone systems. Take the latest DJI Mavik 2 as a starting point. Although regarded as an easy to use and readily available commercial drone technology, it is actually far more advanced than the previous generation of commercial drones that emerged from 2013.[89] The DJI Phantom-1 is a key example. This early commercial drone had a maximum flight time of 10-mins and no built-in camera.[90] In contrast, the new Mavik 2 can fly for up to 31 minutes, at a maximum speed of 72 km per hour, over a range of 8-kilometers, with built-in live video transmission.[91] Yet this is merely the new normal when it comes to drone capabilities. With improvements in battery technology, ever more advanced transmitters, High Definition (HD) and thermal cameras, payload, and powerful motors, today's drones are more 'fast and furious' rather than 'low and slow'.[92]

Illustrative of this new generation of drone threats are the recent cases of commercial drones being used as biological weapons and in hostile rudimentary swarms. In terms of the former, the extended range, speed, video transmission, and payload capacity afforded by the latest commercial drone technologies allowed criminal gangs in China to help spread African Swine Flu. In January 2020, as families across China prepared for Chinese New Year and the purchase of holiday favourites – like pork dumplings, braised pork, and pork knuckles[93] – a sinister drone operation exacerbated an ongoing African Swine Flu pandemic.[94] In an attempt to engineer a pork scarcity, gangs in North-eastern China packed commercial drones full of tainted pork meat.[95] They then flew the meat onto distant uninfected farms. It is believed that the aim was to trigger the cheap sale of infected meat by desperate farmers.[96] The gangs would then resell the meat as uninfected produce to unsuspecting customers far away from the source.[97] Although now largely forgotten due to COVID-19, this disquieting bio-attack raises concerns about how commercial drones can be used to easily spread diseases by hostile actors and how hard it is to effectively counter this threat. In this case, farmers did purchase and operate their own counter-drone technologies, only to be found in breach of the law as their system's 'transmitter had disrupted the GPS [Global Positioning System] signal in the area' potentially interfering with air traffic.[98] In light of these counter-drone challenges, it is worth noting that terrorist actors, such as Aum Shinrikyo and ISIS, have previously experimented with the spread of biological agents, yet the hostile use of Ebola, SARS, COVID, or Smallpox still remains a difficult to deploy weapon for malign actors.[99] Swarms, on the other hand, are a novel threat that have been achieved.

Free to download software and online tutorials now combine to make it possible for everyday drone users to launch rudimentary 'swarms'.[100] More accurately described as multi-drone deployments,

between five and ten drones can be 'hooked-up' to a single device and flown beyond the line of visual sight. When this capacity is combined with readily available mobile apps 'that allow drone pilots to pre-set their drones' final destination', it is clear to see how open-access, automated drone swarms have been born.[101] In 2018, for instance, the FBI was operationally blinded when a criminal gang made 'high-speed low passes' at agents with multiple drones.[102] The head of the FBI's Operational Technology Law Unit, Joe Mazel, stated that the gang buzzed FBI hostage teams with multiple drones all at once and even 'had people fly their own drones up and put the footage to YouTube'.[103] Cases of multi-drone deployment have also been noted in Mexico, with drug cartels targeting the home of the public safety secretary for the Mexican state of Baja California.[104] Not only this, but in Arizona, the Palo Verde Nuclear Power Plant, the largest nuclear plant in the United States (in terms of power produced), had a 'drone-a-palooza' of five or six drones hovering above its pressurized water reactor for multiple nights.[105] Despite the involvement of the local police, the FBI, Department of Homeland Security, and counter-drone specialists, no one has been held to account.[106] During their offensive against allied forces, ISIS was also adept at drone swarm deployments. By utilising commercial front companies and cells in the UK, Spain, Bangladesh, and Denmark – along with smuggling channels through Turkey – ISIS was able to access some of the most sophisticated drone hardware and high-tech 'add-ons' like thermal imaging cameras, transmitters, and motors.[107] As has been documented previously in the Bulletin of the Atomic Scientists, in one series of attacks that occurred within a 24-hour period, 'there were no less than 82 drones of all shapes and sizes' dropping bombs at Kurdish, French, and US forces.[108] Operated as part of multi-wave coordinated attacks, ISIS drones were used along with suicide bombers, vehicle-borne IEDs, and sniper fire, to cause maximum damage and chaos for coalition forces.[109] Such attacks indicate that in

future conflicts NATO and allied forces will face a potent challenge at the tactical air power level bringing hostile air power threats, not seen for a generation, back to the field of battle.[110]

To finish, it is important to mention the most impactful drone 'swarm' to-date. In September 2019, numerous drones and cruise missiles struck the ARAMCO oil processing facilities at Abqaiq and Khurais in eastern Saudi Arabia, taking 6 per cent of the world's oil supply offline.[111] It is still not known for certain if this attack was conducted by Houthi terrorists or directly by Iran. This is because the two actors (one state and one non-state) are able to deploy almost identical systems, thus raising an important and timely issue. It is believed that Iran supplies the Houthi's in Yemen with its military UAS hardware, and in doing so, Iran has surrounded its own UAS activities with a certain level of deniability. NATO actors should note that in future conflict, there will be numerous duplicate state and non-state technologies in the air, making attribution, accountability, and retaliation difficult to correctly and effectively ascertain or achieve. Nevertheless, the Iran-Houthi supply of drones also raises a second important emerging trend in drone warfare; namely how non-state actors can now harness military UAS capabilities and combine them with commercial capacity, creating adaptable and easy to manufacture hybrid systems. As the 2019 inspections of captured Houthi drones revealed, these weapons technologies were a mix of state-supplied military UAS hardware, state-designed yet locally produced fibreglass chassis, and additional smuggled commercial elements that expand the drone's technical capabilities.[112] These include high-power and longer-range petrol motors, information and connection transmitters, HD cameras, electrical wiring, tail wings, and wing flaps.[113] The ability to combine these commercial elements with state systems and to indigenously reproduce state designs, means that non-state actors will be able to continue weaponized drone manufacture, even

when states supplies are cut off. These non-state actors will also be able to share their drone knowledge with aligned groups, leading to an uncontrolled drone proliferation at a non-state level.

To conclude, therefore, in future warfare it will be difficult to tell a state drone strike and swarm from a terrorist drone strike and swarm as states engage in a deliberate attempt to 'muddy the waters' and create an air of deniability by supplying identical systems to non-state actors. Non-state actors will make up for lapses in state supply by combining military hardware with easy to obtain and ever more advanced commercial drone elements that they will in turn supply to other terrorist actors. This trend will also make it difficult to delineate between commercial drones and state military UAS, especially as state actors also begin to harness their own commercially inspired technologies and incorporate them into their ranks.[114] Put simply, in future drone wars, the landscape will become increasingly complex, congested, and dangerous for all as both allied forces and urban settings face a difficult to counter and ever-evolving hostile threat from the skies.

Endnotes

1. Callamard, A (2020). Report of the UN Special Rapporteur on extrajudicial, summary or arbitrary executions to the Human Rights Council Forty-fourth session', A/HRC/44/38, Jul. 2020. The term 'Second Drone Age' was originally coined by the founder of Air Wars, Chris Woods. See interview in Farooq, U. May, 2019. The Second Drone Age. The Intercept, retrieved from: https://theintercept.com/2019/05/14/turkey-second-drone-age.
2. The Associated Press (2009). '08 saw shift in Iraq, Afghan troop death toll. NBC News, retrieved from: http://www.nbcnews.com/id/28449062/ns/us_news-military/t/saw-shift-iraq-afghan-troop-death-tolls/#.XxW1qygzZPY.
3. Nolin, PC (2011). Countering the Afghan Insurgency: Low-tech Threats, High-Tech Solutions. Special Report, Brussels: NATO Parliamentary Assembly. Also see Icasualties (2011), Operation Enduring Freedom (2011), retrieved from: http://icasualties.org/OEF/index.aspx.
4. Rogers, J & Goxho D (2020). The Changing Character of Remote Warfare: Proliferation, Politics, and Military Power in Niger, (Forthcoming 2021). Also see Watson A (2019). Planning for Future Operations: Learning Lessons from Remote Warfare. Oxford Research Group, retrieved from: https://www.oxfordresearchgroup.org.uk/Blog/planning-for-the-next-war-making-the-case-for-remote-warfare.
5. Waldman T (2018). Vicarious warfare: The counterproductive consequences of modern American military practice, Contemporary Security Policy, Vol. 39 (2), 181–205.

6. Rogers J (2018), The Origins of Drone Warfare. History Today, retrieved from: https://www.historytoday.com/history-matters/origins-drone-warfare.
7. Clausewitz Cv [1832] (1976). On War. Howard M and Paret P, eds. And trans. Princeton, NJ: Princeton University Press.
8. As documented by CNAS in 2016 '[a] February 2013 Gallup poll . . . reported that 65 percent of Americans agreed with the US government's decision to launch drone strikes against terrorists overseas. In the same month, 75 percent of respondents to a Fairleigh Dickinson University PublicMind poll approved of the US military's use of drones to carry out attacks overseas on targets deemed a 'threat to the United States'. And in May 2015, a Pew public opinion poll reported that 58 percent of US adults approved of the use of drones to carry out missile strikes against extremists in Pakistan, Yemen, and Somalia: a 2 percent increase from the same Pew poll of February 2013. See Schneider J and Macdonald J (2016). US Public Support for Drone Strikes: When Do Americans Prefer Unmanned over Manned Platforms? CNAS, retrieved from: https://s3.amazonaws.com/files.cnas.org/documents/CNAS-Report-DronesandPublicSupport-Final2.pdf?mtime=20160929153710.
9. Ignatieff M (2001). Virtual War: Kosovo and Beyond, London: Vintage.
10. PAX (2011). Does unmanned make unacceptable? Retrieved from: https://www.paxforpeace.nl/publications/all-publications/does-unmanned-make-unacceptable.
11. Kennedy-Pipe C, Rogers J & Waldman T (2016). Drone chic: The precision myth. London: ORG, retrieved from: https://css.ethz.ch/en/services/digital-library/publications/publication.html/196761. Also see Nemar R (2017). Psychological harm. In Acheson R, et al. (eds.). The Humanitarian impact of drones. Women's International League for Peace and Freedom. retrieved from https://reliefweb.int/sites/reliefweb.int/files/resources/humanitarian-impact-of-drones.pdf. Accessed 10 Jul. 2019.
12. The Bureau of Investigative Journalism (2019). Drone War. TBIJ, retrieved from https://www.thebureauinvestigates.com/projects/drone-war. Also see AirWars and the work of its founder Chris Woods. Woods C (2015). Sudden justice: America's secret drone warfare. Oxford: Oxford University Press.
13. The Financial Times (2014). Robert Gates hits out at Obama foreign policy. The FT, retrieved from: https://www.ft.com/content/a4e7e2bc-77ef-11e3-afc5-00144feabdc0.
14. Obama B (2013). Remarks by the President at the National Defense University. Office of the Press Secretary: The White House, retrieved from: https://obamawhitehouse.archives.gov/the-press-office/2013/05/23/remarks-president-national-defense-university.
15. Rogers J (2017). Drone Warfare: The Death of Precision. The Bulletin of the Atomic Scientist, retrieved from: https://thebulletin.org/2017/05/drone-warfare-the-death-of-precision/.
16. Pompeo M (2020). UN Special Rapporteur Gives More Cause to Distrust UN Human Rights Mechanisms. Press Statement, Department of State, retrieved from: https://www.state.gov/un-special-rapporteur-gives-more-cause-to-distrust-un-human-rights-mechanisms/.
17. In line with this volume's definition of drones, 'Unmanned Aircraft Systems (UAS)' will refer to those drones broadly defined as the larger military systems often placed under the 'Class 2' and 'Class 3' NATO demarcation. In addition, this chapter will, from this point onwards, utilise the term 'drone' solely for reference to much smaller unmanned systems, usually commercial in origin or augmented by commercial technologies and utilised by non-state actors.
18. Boyle MJ, Horowitz MC, Kreps S, and Fuhrmann M (2018). Debating Drone Proliferation, International Security, Vol. 42, (3), 178–182.
19. Gettinger D (2019). The Drone Databook. The Center for the Study of the Drone: Bard College, retrieved from: https://dronecenter.bard.edu/projects/drone-proliferation/databook/, viii.
20. Ibid., ix.
21. Ibid. 1.
22. Ibid. 1.
23. Hambling D (2020). The Weird And Worrying Drone War In The Caucasus. Forbes, retrieved from: https://www.forbes.com/sites/davidhambling/2020/06/22/the-weird-and-worrying-drone-war-in-the-caucasus/#72daa6245daf.

24. Rogers J (2019). The Darkside of Our Drone Future, The Bulletin of the Atomic Scientists. retrieved from: https://thebulletin.org/2019/10/the-dark-side-of-our-drone-future/.
25. Ibid. 19, x.
26. Aldens C, et al. (2020). Wings Along the BRI Exporting Chinese UCAVs and Security? LSE IDEAS Strategic Insight, retrieved from: https://www.lse.ac.uk/ideas/Assets/Documents/updates/LSE-IDEAS-Wings-Along-the-BRI.pdf.
27. Nichols M (2019). U.N. report finds likely use of armed drone in Libya by Haftar or 'third party'. Reuters, retrieved from: https://fr.reuters.com/article/worldNews/idUSKCN1SE2RF.
28. Ibid. 26.
29. Ibid. 26.
30. Rogers J (2019). Personal Interview with US Force Protection Officers, US Military.
31. 'In Iraq we had Chinese drone with Chinese contractors helping Iraqi forces . . . We had Russian anti-air systems and Iranian drones all in one base as well. It was pretty crowded'. Rogers J (2019). Personal Interview with US Force Protection Officers, US Military.
32. See Shortell D (2019). DHS warns of 'strong concerns' that Chinese-made drones are stealing data, CNN. retrieved from: https://edition.cnn.com/2019/05/20/politics/dhs-chinese-drone-warning/index.html, and Bowler T (2020). Huawei: Why is it being banned from the UK's 5G network? BBC, retrieved from: https://www.bbc.com/news/newsbeat-47041341.
33. The term 'crucible' is inspired by Jack McDonald's chapter on the Balkans Crucible and UAS use in the 1990s. McDonald J (2017). Enemies Known and Unknown: Targeted Killings in America's Transnational War. Oxford University Press: Oxford.
34. Salame G (2019). Interview with UN Special Representative for Libya Ghassan Salamé, United Nations Political and Peacebuilding Affairs. retrieved from: https://www.youtube.com/watch?v=IB3jie4i7SI.
35. Axe D (2020). Why Is China Providing Drones to Fuel Libya's Civil War? The National Interest, retrieved from: https://nationalinterest.org/blog/buzz/why-china-providing-drones-fuel-libyas-civil-war-118111. Also see Human Rights Watch (2020). Libya: UAE Strike Kills 8 Civilians Attack Apparently Unlawful; Compensate Families of Victims. Retrieved from: https://www.hrw.org/news/2020/04/29/libya-uae-strike-kills-8-civilians.
36. The Economist (2020). Khalifa Haftar is losing ground and lashing out in Libya. The Economist, retrieved from: https://www.economist.com/middle-east-and-africa/2020/05/02/khalifa-haftar-is-losing-ground-and-lashing-out-in-libya.
37. Reuters (2020). Jets hit Libya's al-Watiya airbase where Turkey may build base, sources say. Reuters, retrieved from: https://www.reuters.com/article/us-libya-security/jets-hit-libyas-al-watiya-airbase-where-turkey-may-build-base-sources-say-idUSKBN24608H.
38. The reported specifications of the drone vary between the press, government, and manufacturer. Baykar (2020). Bayraktar TB2. retrieved from: https://baykardefence.com/uav-15.html and Presidency of Defence Industries, (2020). Bayraktar Armed Unmanned Aerial Vehicle. retrieved from: https://www.ssb.gov.tr/Website/contentList.aspx?PageID=365&LangID=2.
39. Gady FS (2019). Useful, but not decisive: UAVs in Libya's civil war, IISS. retrieved from: https://www.iiss.org/blogs/analysis/2019/11/mide-uavs-in-libyas-civil-war.
40. Ibid.
41. Rogers J (2020). Soleimani helped turn Iran into one of the most effective proponents of remote warfare; his impact lives on, UK Defence Journal. retrieved from: http://ukdefencejournal.org.uk/soleimani-helped-turn-iran-into-one-of-the-most-effective-proponents-of-remote-warfare-his-impact-lives-on/.
42. Wohlstetter A (1958). The Delicate Balance of Terror, RAND. retrieved from: www.rand.org/about/history/wohlstetter/P1472/P1472.html.
43. Brownsword S (2020). Turkey's unprecedented ascent to drone superpower status, Drone Wars. retrieved from: https://dronewars.net/2020/06/15/turkeys-unprecedented-ascent-to-drone-superpower-status/.
44. Cole C & Cole J (2020). Libyan war sees record number of drones brought down to earth. retrieved from: https://dronewars.net/2020/07/01/libyan-war-sees-record-number-of-drones-brought-down-to-earth/.

45. Imhof O (2019). Increasing foreign role risks spiralling Libya conflict out of control, Airwars, retrieved from: https://airwars.org/news-and-investigations/increasing-foreign-involvement-could-spiral-libya-conflict-out-of-control/.
46. Ibid.
47. Ibid.
48. Ibid.
49. Iddon P (2020). Turkey Is Deploying Lots of Air Defense Systems In Syria And Libya. Forbes, retrieved from: https://www.forbes.com/sites/pauliddon/2020/07/07/turkey-is-deploying-lots-of-air-defense-systems-in-syria-and-libya/#696b0dcc5555.
50. Fishman B & Hiney C (2020). What Turned the Battle for Tripoli? The Washington Institute. retrieved from: https://www.washingtoninstitute.org/policy-analysis/view/what-turned-the-battle-for-tripoli.
51. Ibid.
52. Iddon P (2020). Turkey's New Akinci Drone Is Impressive, But It's No Substitute For Modern Fighter Jets. Forbes, retrieved from: https://www.forbes.com/sites/pauliddon/2020/08/25/turkeys-new-akinci-drone-looks-impressive-but-its-no-substitute-for-modern-fighter-jets/#d88d7ba602eb.
53. Yan S (2020). China sells armed drones to Serbia amid concerns arms deal could destabilise region. The Telegraph. retrieved from: https://www.telegraph.co.uk/news/2019/09/11/china-sells-armed-drones-serbia-amid-concerns-arms-deal-could/.
54. Roblin S (2020). Missile-Armed Chinese Drones Arrive In Europe As Serbia Seeks Airpower Edge, Forbes. retrieved from: https://www.forbes.com/sites/sebastienroblin/2020/07/09/missile-armed-chinese-drones-arrive-in-europe-for-serbian-military/#74b248be79d2.
55. NATO Engages (2019). Questions and answers by NATO Secretary General Jens Stoltenberg at the "NATO Engages: Innovating the Alliance" conference. retrieved from: https://www.nato.int/cps/en/natohq/opinions_171550.htm?selectedLocale=en.
56. Ibid. 54.
57. Crawford N (2020). Growing public debt isn't the only problem with Chinese lending to the Balkans. IISS. retrieved from: https://www.iiss.org/blogs/analysis/2020/03/gstrat-bri-in-the-balkans.
58. Heath R & Gray A (2018). Beware Chinese Trojan horses in the Balkans, EU warns. Politico. retrieved from: https://www.politico.eu/article/johannes-hahn-beware-chinese-trojan-horses-in-the-balkans-eu-warns-enlargement-politico-podcast/.
59. Elabdi F & Hudson J (2020). No discussion of buying Greenland, but Pompeo underscores US interest in the Arctic during Denmark trip, The Washington Post. retrieved from: https://www.washingtonpost.com/world/europe/pompeo-greenland-arctic/2020/07/22/754947cc-cb6b-11ea-99b0-8426e26d203b_story.html.
60. Depledge D, Kennedy-Pipe C, Rogers J (2019). The UK and the Arctic: Forward defence. The Arctic Yearbook, retrieved from: https://arcticyearbook.com/arctic-yearbook/2019/2019-scholarly-papers/320-the-uk-and-the-arctic-forward-defence.
61. Rogers J (2020). Strengthen NATO relations in the Arctic [Styrk Nato-relationerne i Arktis]. Altinget, retrieved from: https://www.altinget.dk/forsvar/artikel/debat-styrk-nato-relationerne-i-arktis.
62. TASS (2014). Russian military forming drone squadron for Arctic reconnaissance. TASS, retrieved from: https://tass.com/russia/759495.
63. Rogers J (2020). 'The Arctic and US Homeland Security'. In Grice F (ed.). The Handbook of US Homeland Security (forthcoming, CRC Press, Taylor & Francis).
64. Ibid.
65. Bendett S (2019). Russia Plans More Arctic UAVs. Defence One, retrieved from: https://www.defenseone.com/ideas/2019/02/russia-plans-more-arctic-uavs/154998/.
66. Hønneland G (2015). Russia and the Arctic: Environment, Identity and Foreign Policy, London: Bloomsbury.
67. Presidential Memoranda (2020). Memorandum on Safeguarding US National Interests in the Arctic and Antarctic Regions. The White House, retrieved from: https://www.whitehouse.gov/presidential-actions/memorandum-safeguarding-u-s-national-interests-arctic-antarctic-regions/.
68. McCullough A (2020). Russian MiG-31s Allegedly Intercept Global Hawk Over Arctic Waters. Air Force Magazine, retrieved from:

https://www.airforcemag.com/russian-mig-31s-allegedly-intercept-global-hawk-over-arctic-waters/#.XzOGIE49Z2M.twitter.

69. Allison G (2019). Israeli firm providing Maritime Patrol services to Iceland. UK Defence Journal, retrieved from: https://ukdefencejournal.org.uk/israeli-firm-providing-maritime-patrol-services-to-iceland/.
70. Danish Defence Agreement 2018–2023. Retrieved from: https://fmn.dk/temaer/forsvarsforlig/Documents/danish-defence-agreement-2018-2023-pdfa.pdf.
71. See about Russian Orlan 10s: Rogers J (2020). 'Drone Warfare: Distant Targets and Remote Killings'. In Thapa M, Marton P, and Romaniuk SN (eds.). The Palgrave Encyclopaedia of Global Security Studies. London: Palgrave. With Holland A.
72. It is important not to indulge in hyperbole when discussing the threat posed by hostile drones. To minimise this, each example presented in this final section will be grounded in empirical cases of hostile drone deployment. In addition, the technical capabilities mentioned throughout this section are currently available or have come to light during advanced vulnerabilities testing. It is from these examples that a disturbing list of current and future threats can be compiled.
73. Williams A (2020). The Drones Were Ready for This Moment. The New York Times, retrieved from: https://www.nytimes.com/2020/05/23/style/drones-coronavirus.html.
74. Preventing Emerging Threats Act of 2018. S. Rept. 115-332, Senate – Homeland Security and Governmental Affairs, retrieved from: https://www.congress.gov/bill/115th-congress/senate-bill/2836.
75. For a detailed discussion of 'virtuous drones' see: Kennedy C & Rogers JI (2015). Virtuous drones? The International Journal of Human Rights, 19: 2, 211–227, DOI: 10.1080/13642987.2014.991217.
76. Police Executive Research Forum (2020). Drones: A Report on the Use of Drones by Public Safety Agencies – and a Wake-Up Call about the Threat of Malicious Drone Attacks. Washington, DC: Office of Community Oriented Policing Services, vii
77. 'As of early 2020, the United States is extremely vulnerable to drone attacks.' Ibid.
78. PWC. Skies without limits: Drones taking the UK's economy to new heights. PWC, retrieved from: https://www.pwc.co.uk/intelligent-digital/drones/Drones-impact-on-the-UK-economy-FINAL.pdf.
79. Uber Elevate (2020). The Future of Urban Mobility, retrieved from: https://www.uber.com/us/en/elevate/.
80. Thorbecke C (2020). Small Virginia town soon to be the site of drone delivery program for Walgreens. ABC News, retrieved from: https://abcnews.go.com/Business/small-virginia-town-site-drone-delivery-program-walgreens/story?id=65799937.
81. Amazon (2020). Amazon Prime Air, Amazon. retrieved from: https://www.amazon.com/Amazon-Prime-Air/b?ie=UTF8&node=8037720011.
82. As the strategist Colin Grey has argued, 'the enemy will always move against your perceived weakness'. See Grey quoted in Mattis J (2018). Remarks by Secretary Mattis on the National Defense Strategy, US DoD, retrieved from: https://www.defense.gov/Newsroom/Transcripts/Transcript/Article/1420042/remarks-by-secretary-mattis-on-the-national-defense-strategy/. For detailed discussion of these weaknesses, see Rogers J (2019). The Darkside of Our Drone Future. The Bulletin of the Atomic Scientists, retrieved from: https://thebulletin.org/2019/10/the-dark-side-of-our-drone-future/.
83. Police Executive Research Forum (2020). Drones: A Report on the Use of Drones by Public Safety Agencies – and a Wake-Up Call about the Threat of Malicious Drone Attacks. Washington, DC: Office of Community Oriented Policing Services, vii–xi.
84. Ibid.
85. Rogers J (2019). The Edge of Drone Warfare, TEDx 2019. retrieved from: https://www.youtube.com/watch?v=_GbXictC9eU.
86. Ibid.
87. BBC News (2018). Venezuela President Maduro survives 'drone assassination attempt'. BBC, retrieved from: https://www.bbc.com/news/world-latin-america-45073385.
88. Rogers J (2019). Written Evidence submitted by Dr James Rogers (SDU/Yale University). Domestic Threat of Drones Inquiry. UK Parliament, retrieved from: data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/defence-committee/domestic-threat-of-drones/written/103710.pdf.
89. DJI (2020). Mavic 2: See the Bigger Picture. DJI, retrieved from: https://www.dji.com/dk/mavic-2.

90. DJI (2020). Phantom. DJI, retrieved from: https://www.dji.com/dk/phantom.
91. DJI (2020). Mavic 2: See the Bigger Picture. DJI, retrieved from: https://www.dji.com/dk/mavic-2.
92. Anna Jackman quoted in Drones piloted by climate-change activists target Heathrow. The Economist, retrieved from: https://www.economist.com/britain/2019/06/15/drones-piloted-by-climate-change-activists-target-heathrow.
93. For more see the work of Sale Lilly, RAND. Also see van der Zee B & Standaert M (2019). 'Not enough pork in the world' to deal with China's demand for meat. The Guardian, retrieved from: https://www.theguardian.com/business/2019/nov/23/china-pigs-african-swine-fever-pork-shortage-inflation.
94. Reuters (2019). Chinese pig farm jams drone of crooks spreading African swine fever. ABC News. retrieved from: https://www.nbcnews.com/news/china/chinese-pig-farm-jams-drone-crooks-spreading-african-swine-fever-n1105631.
95. Ibid.
96. Reuters (2019). China pig farm jams drones dropping swine fever-laced products onto its sites, but also GPS. The Japan Times, retrieved from: https://www.japantimes.co.jp/news/2019/12/23/asia-pacific/china-pig-farm-jams-drones-dropping-swine-fever-laced-products-onto-site-also-gps/#.XOJlosgzZPY.
97. Huang Y (2019). Why Did One-Quarter of the World's Pigs Die in a Year? The New York Times, retrieved from: https://www.nytimes.com/2020/01/01/opinion/china-swine-fever.html.
98. The Telegraph (2020). Chinese pig farm attempts to block criminal drones with signal jammer, accidentally disrupts planes, The Telegraph. retrieved from: https://www.telegraph.co.uk/news/2019/12/23/chinese-pig-farm-attempts-block-criminal-drones-signal-jammer/.
99. Tu AT (2014). Aum Shinrikyo's Chemical and Biological Weapons: More Than Sarin. Forensic Science Review, 2014; Vol. 26, Issue (2), 115–120. Also see Warrick J (2019). Exclusive: Iraqi scientist says he helped ISIS make chemical weapons. The Washington Post, retrieved from: https://www.washingtonpost.com/world/national-security/exclusive-iraqi-scientist-says-he-helped-isis-make-chemical-weapons/2019/01/21/617cb8f0-0d35-11e9-831f-3aa2c2be4cbd_story.html.
100. Rogers J (2019). The Darkside of Our Drone Future. The Bulletin of the Atomic Scientists, retrieved from: https://thebulletin.org/2019/10/the-dark-side-of-our-drone-future/.
101. Ibid.
102. Tucker P (2019). A Criminal Gang Used a Drone Swarm To Obstruct an FBI Hostage Raid. Defence One. retrieved from: https://www.defenseone.com/technology/2018/05/criminal-gang-used-drone-swarm-obstruct-fbi-raid/147956/.
103. Ibid.
104. Sullivan JP Bunker RJ & Kuhn DA (2018). Mexican Cartel Tactical Note #38: Armed Drone Targets the Baja California Public Safety Secretary's Residence in Tecate, Mexico. Small Wars Journal, retrieved from: https://smallwarsjournal.com/jrnl/art/mexican-cartel-tactical-note-38-armed-drone-targets-baja-california-public-safety.
105. Rogoway T & Trevithick J (2020). The Night A Mysterious Drone Swarm Descended On Palo Verde Nuclear Power Plant. The Drive, retrieved from: https://www.thedrive.com/the-war-zone/34800/the-night-a-drone-swarm-descended-on-palo-verde-nuclear-power-plant.
106. Ibid.
107. Ibid. 100. Also see Davies W (2018). The global terror network that started in Pontypridd. BBC Wales Investigates, retrieved from: https://www.bbc.com/news/uk-wales-44826806.
108. Ibid. 100.
109. Ibid. 100.
110. As one officer in the US military stated, 'We have lost tactical air superiority. We will not get air superiority in the future. We need to accept this; they will get through'. Rogers J (2019). Personal Interview, Technical Sergeant, US military.
111. Barrington L & Yaakoubi A (2019). Yemen Houthi drones, missiles defy years of Saudi air strikes. Reuters, retrieved from: https://www.reuters.com/article/us-saudi-aramco-houthis/yemen-houthi-drones-missiles-defy-years-of-saudi-air-strikes-idUSKBN1W22F4.

112. Rogers J (2019). Remote warfare increasingly strategy of choice for non-state actors, UK Defence Journal, retrieved from: https://ukdefencejournal.org.uk/remote-warfare-increasingly-strategy-of-choice-for-non-state-actors/.
113. Conflict Armament Research (2020). Evolution of UAVs employed by Houthi forces in Yemen. CAR, retrieved from: https://storymaps.arcgis.com/stories/46283842630243379f0504ece90a821f.
114. Doffman Z (2019). Russian Military Plans Swarms Of Lethal 'Jihadi-Style' Drones Carrying Explosives. Forbes, retrieved from: https://www.forbes.com/sites/zakdoffman/2019/07/08/russias-military-plans-to-copy-jihadi-terrorists-and-arm-domestic-size-drones/#6e0bd5d632e7.

Part VI

Annexes

Annex A

NATO UAS Classification Table

NATO UAS CLASSIFICATION		
Class	Category	Normal Employment
Class III (> 600 kg)	Strike/ Combat	Strategic/ National
	HALE	Strategic/ National
	MALE	Operational/ Theatre
Class II (150 kg–600 kg)	Tactical	Tactical Formation
Class I (< 150 kg)	Small (>15 kg)	Tactical Unit
	Mini (<15 kg)	Tactical Sub-unit (manual or hand launch)
	Micro (<66 J)	Tactical Sub-unit (manual or hand launch)

Figure A.1: NATO UAS Classification Table (Source: NATO ATP-3.3.8.1, Ed. B, Ver. 1).

Normal Operating Altitude	Normal Mission Radius	Primary Supported Commander	Example Platform
Up to 65,000 ft MSL	Unlimited (BLOS)	Theatre	Reaper
Up to 65,000 ft MSL	Unlimited (BLOS)	Theatre	Global Hawk
Up to 45,000 ft MSL	Unlimited (BLOS)	JTF	Heron
Up to 18,000 ft AGL	200 km (LOS)	Division, Brigade	Watchkeeper
Up to 5,000 ft AGL	50 km (LOS)	Battalion, Regiment	Scan Eagle
Up to 3,000 ft AGL	Up to 25 km (LOS)	Company, Platoon, Squad	Skylark
Up to 200 ft AGL	Up to 5 km (LOS)	Platoon, Squad	Black Widow

Annex B

Military UAS Fact Sheets

Image provided by Janes.

Russia

Altius/Altair

Primary Function	ISR and strike UAV
NATO UAS Classification	Class III/MALE
Contractor	Sokol Aircraft Factory/ Sokol OKB RUS
Power Plant	2 x RED A03/V12 Diesel Engines
Wingspan	28.5 m
Length	11.6 m
Height	
Weight	5,000–6,000 kg
Maximum Take-Off Weight	
Endurance	Up to 48 hrs
Payload/Armament	2,000 kg
Speed	Cruise: 150–250 km/h
Range	450 km (LOS), 10,000 km (BLOS)
Ceiling	12,000 m
IOC	Estimated enter service in 2021
Remarks	

Image provided by Janes.

Russia

Grusha/Granat-1

Primary Function	ISR
NATO UAS Classification	Class I/Mini Tactical
Contractor	Izhmash
Power Plant	Electric Motor
Wingspan	0.8 m
Length	
Height	
Weight	2.5 kg
Maximum Take-Off Weight	
Endurance	1.3 h
Payload/Armament	Max 0.4 kg
Speed	120 km/h
Range	10 km
Ceiling	5,000 m
IOC	
Remarks	Start by hand or catapult, landing by parachute

Image provided by Janes.

Russia

Eleron-3

Primary Function	ISR, BDA, EW
NATO UAS Classification	Class I/Mini
Contractor	ENIKS
Power Plant	Electric Engine
Wingspan	1.47 m
Length	0.45 m
Height	
Weight	
Maximum Take-Off Weight	4.8 kg
Endurance	1 h 40 min
Payload/Armament	0.8 kg
Speed	Cruise: 70 km/h, Max: 130 km/h
Range	25 km (LOS)
Ceiling	5,000 m
IOC	FOC in RUS Army
Remarks	Hand held or elastic rubber band start, parachute landing

Image provided by Janes.

Russia

Eleron-10SV

Primary Function	ISR
NATO UAS Classification	Class I/Mini UAS, Flying Wing
Contractor	ENIKS
Power Plant	Electric Engine
Wingspan	2.2 m
Length	0.88 m
Height	0.38 m
Weight	15.5 kg
Maximum Take-Off Weight	
Endurance	2.5 h
Payload/Armament	
Speed	Cruise: 75 km/h, Max: 135 km/h
Range	> 50 km (LOS)
Ceiling	4,000 m
IOC	Operational in RUS ARMY
Remarks	Hand held or elastic rubber band start, parachute landing

Image provided by Janes.

Russia

Forpost

Primary Function	ISR, Comms Relay
NATO UAS Classification	Class II/Tactical
Contractor	Ural Works of Civil Aviation (UWCA)
Power Plant	1 × Piston Engine
Wingspan	8.55 m
Length	5.85 m
Height	1.25 m
Weight	325 kg (estimated)
Maximum Take-Off Weight	454 kg (estimated)
Endurance	17.5 h
Payload/Armament	Max. 100 kg
Speed	Max. 204 km/h, Cruising at 110 km/h
Range	250 km
Ceiling	6,000 m
IOC	FOC in RUS Navy and AF
Remarks	Take-off and landing on runway

Image provided by Janes.

Russia

Granat-4

Primary Function	ISR, EW
NATO UAS Classification	Class I/Small Short-range Tactical UAV
Contractor	Izhmash Unmanned Systems
Power Plant	
Wingspan	3.2 m
Length	2.4 m
Height	
Weight	
Maximum Take-Off Weight	30 kg
Endurance	
Payload/Armament	3 kg
Speed	Max. 145 km/h, Cruising at 90 km/h
Range	70 km–100 km
Ceiling	3,500 m
IOC	
Remarks	

Image provided by Janes.

Image provided by Janes.

Russia

Korsar

Primary Function	ISR
NATO UAS Classification	Class III/MALE UAV
Contractor	Luch Design Bureau
Power Plant	Piston Engine with a Pusher Propeller
Wingspan	6.50 m
Length	4.20 m
Height	
Weight	
Maximum Take-Off Weight	200 kg
Endurance	8 h
Payload/Armament	
Speed	Max. 150 km/h
Range	120 km
Ceiling	5,000 m
IOC	Presented at the International Military Technical Forum ARMY-2019
Remarks	

Image provided by Janes.

Image provided by Janes.

Russia

Okhotnik (Hunter)

Primary Function	Strike, Combat, Stealth
NATO UAS Classification	Class III /HALE UAV
Contractor	JSC Sukhoi Company
Power Plant	Single AL-31 Turbo-fan Engine
Wingspan	19 m
Length	11.65 m
Height	3.10 m
Weight	20,000 kg (Operating Weight, Empty)
Maximum Take-Off Weight	
Endurance	10 h
Payload/Armament	2 internal weapons bays for up to 2,000 kg of guided and unguided munitions
Speed	Max. 1,000 km/h
Range	6,000 km
Ceiling	18,000 m
IOC	First prototype observed on 23 Jan. 2019, introduction planned for 2024
Remarks	Conventional wheeled take-off and landing

Image provided by Janes.

Image provided by Janes.

Russia

Orion-E

Primary Function	ISR
NATO UAS Classification	Class III/MALE UAV
Contractor	Kronshtadt Group
Power Plant	Piston or turboprop engine that drives a two-bladed pusher propeller
Wingspan	16 m
Length	8 m
Height	3 m
Weight	
Maximum Take-Off Weight	1,000 kg
Endurance	24 h
Payload/Armament	Max 200 kg
Speed	Max. 200 km/h, Cruising at 120 km/h
Range	250 km
Ceiling	7,500 m
IOC	In test phase
Remarks	

Image provided by Janes.

Russia

Orlan-10

Primary Function	ISR, EW (Leer-3)
NATO UAS Classification	Class I/Small
Contractor	STT Spetsialny Tekhnologicheski Tsentr
Power Plant	1 Piston Engine
Wingspan	3.10 m
Length	1.80 m
Height	
Weight	
Maximum Take-Off Weight	16 kg
Endurance	16 h
Payload/Armament	Max. 6 kg
Speed	Max: 150 km/h, Cruise: 90 km/h
Range	Radius of Operation: 140 km/10 h
Ceiling	5,000 m
IOC	Delivered in 2014, currently in service with over 700 systems operational
Remarks	Rail Launched, Parachute Landing

Image provided by Janes.

Image provided by Janes.

Russia

Takhion (Tachyon)

Primary Function	Tactical Reconnaissance
NATO UAS Classification	Class I/Mini UAV, Flying Wing Design
Contractor	Kalashnikov Concern
Power Plant	Electric Engine
Wingspan	2 m
Length	0.61 m
Height	
Weight	
Maximum Take-Off Weight	25 kg
Endurance	
Payload/Armament	
Speed	Max: 120 km/h, Cruise: 54 km/h
Range	40 km
Ceiling	5,000 m
IOC	Operational in RUS ARMY
Remarks	

Image provided by Janes.

Russia

Zastava (Bird-Eye-400)

Primary Function	Tactical Reconnaissance
NATO UAS Classification	Class I/Mini UAV
Contractor	Israel Aerospace Industries (IAI), assembled by 'Ural Works of Civil Aviation' (UWCA)
Power Plant	Electric Engine
Wingspan	2.2 m
Length	0.8 m
Height	
Weight	
Maximum Take-Off Weight	4.1 kg
Endurance	80 min
Payload/Armament	1.2 kg
Speed	80 km/h
Range	15 km
Ceiling	1,000 m
IOC	FOC in RUS Army
Remarks	Elastic rubber band catapult start, parachute landing

Image provided by Janes.

Image provided by Janes.

China

BZK-005

Primary Function	ISR
NATO UAS Classification	Class III/HALE UAV
Contractor	Beijing University of Aeronautics & Astronautics
Power Plant	
Wingspan	
Length	
Height	
Weight	1,200 kg
Maximum Take-Off Weight	
Endurance	40 h
Payload/Armament	150 kg
Speed	Cruise: 150–180 km/h
Range	
Ceiling	7,800 m
IOC	Operational in PLAAF
Remarks	

Image provided by Janes.

Image provided by Janes.

China

BZK-007

Primary Function	ISR
NATO UAS Classification	Class III/MALE
Contractor	Guizhou Aircraft Industry Corporation (GAIC)
Power Plant	Single Piston Gasoline Engine
Wingspan	14.6 m
Length	7.7 m
Height	2.74 m
Weight	
Maximum Take-Off Weight	700 kg
Endurance	16 h
Payload/Armament	100 kg max
Speed	Max. 230 km/h
Range	
Ceiling	7,500 m
IOC	Operational in PLAAF
Remarks	Fixed Tricycle Landing Gear System

Image provided by Janes.

Image provided by Janes.

China

CH-4 A/CH-4 B

Primary Function	ISR (CH-4 A), ISR and strike (CH-4 B)
NATO UAS Classification	Class III/MALE UAV
Contractor	Aerospace Long-March International Trade Company Ltd. (ALIT)
Power Plant	Piston Engine
Wingspan	18 m
Length	8.5 m
Height	3.4 m
Weight	
Maximum Take-Off Weight	~ 1,300 kg
Endurance	40 h (CH-4 A), 14 h (CH-4 B)
Payload/Armament	115 kg (CH-4 A), 345 kg (CH-4 B)
Speed	Max. 235 km/h (CH-4 A) Max. 210 km/h (CH-4 B)
Range	3,500 km (CH-4 A), 1,600 km (CH-4 B)
Ceiling	~ 7,000 m
IOC	In Service
Remarks	Wheeled Take-Off and Landing

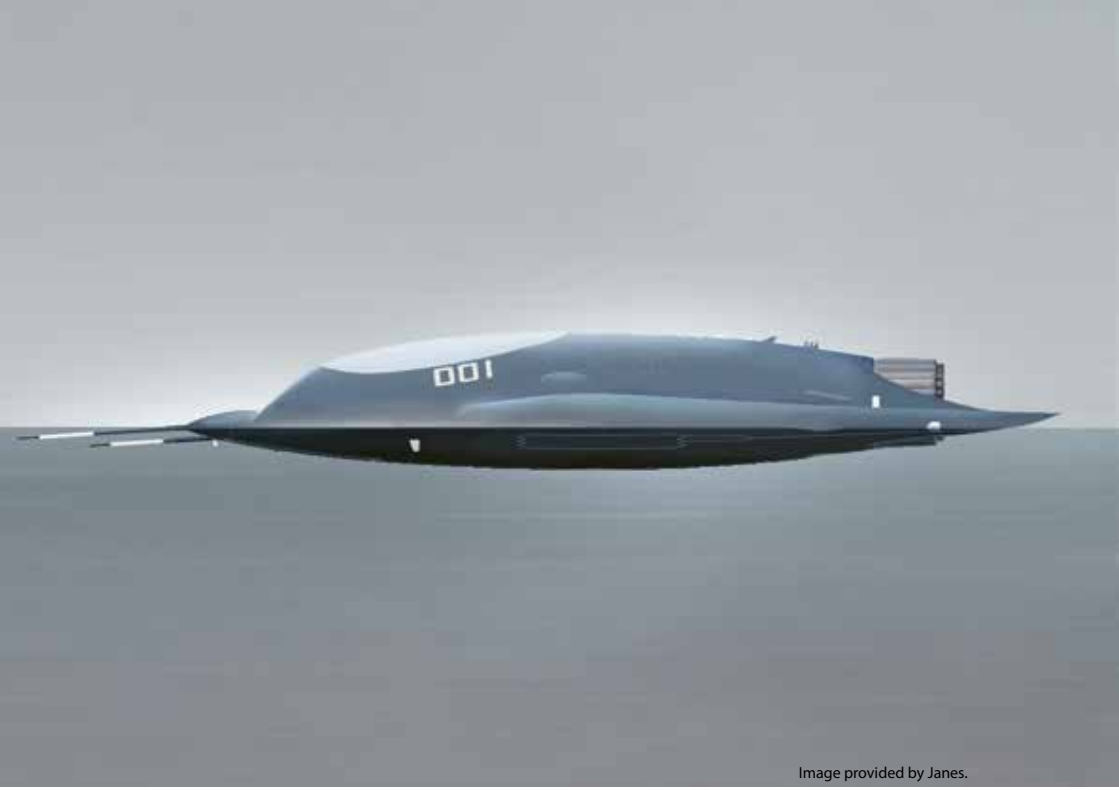


Image provided by Janes.

Image provided by Janes.

China

Gongji 11 (Sharp Sword)

Primary Function	Stealth, Combat
NATO UAS Classification	Class III HALE
Contractor	Hongdu Aviation Industry Group
Power Plant	1x Turbofan
Wingspan	14 m
Length	11.65 m
Height	3.1 m
Weight	6,350 kg
Maximum Take-Off Weight	20,215 kg
Endurance	
Payload/Armament	
Speed	Cruise: 1,000 km/h
Range	4,000 km
Ceiling	12,500 m
IOC	In service in PLAAF (allegedly)*
Remarks	

* Taxi tests are believed to have occurred in May 2013. Flight tests were reported in Chinese media through 2018–2019.

Image provided by Janes.

China

Wing Loong I

Primary Function	Multi Role UAV
NATO UAS Classification	Class III MALE
Contractor	AVIC
Power Plant	1 × Piston Engine
Wingspan	14 m
Length	9 m
Height	2.8 m
Weight	
Maximum Take-Off Weight	1,150 kg
Endurance	20 h
Payload/Armament	200 kg
Speed	Max 280 km/h
Range	200 km
Ceiling	7,500 m
IOC	In service in PLAAF
Remarks	Wheeled Take-Off and Landing

Image provided by Janes.

China

Wing Loong II

Primary Function	Multirole UAV
NATO UAS Classification	Class III MALE UAV
Contractor	AVIC
Power Plant	1 × Turboprop
Wingspan	20.5 m
Length	11 m
Height	4.1 m
Weight	
Maximum Take-Off Weight	4,200 kg
Endurance	32 h
Payload/Armament	480 kg
Speed	Stall: 150 km/h, Max: 370 km/h
Range	2,000 km
Ceiling	9,000 m
IOC	In service in PLAAF
Remarks	Wheeled Take-Off and Landing

Image provided by Janes.

China

Wuzhen-8/DR-8

Primary Function	
NATO UAS Classification	Class III/HALE
Contractor	
Power Plant	Rocket Powered
Wingspan	
Length	
Height	
Weight	
Maximum Take-Off Weight	
Endurance	
Payload/Armament	
Speed	Possibly High Supersonic
Range	
Ceiling	
IOC	Showcased in the National Day parade of 2019. No reports if operational in PLAAF
Remarks	Speculated to be launched in the air via a bomber or transport aircraft

Image provided by Janes.

China

Xianglong

Primary Function	ISR
NATO UAS Classification	Class III/Multi-Role HALE UAV
Contractor	Guizhou Aviation Industry Group (GAIC)
Power Plant	1 x Turbofan
Wingspan	
Length	14 m
Height	5.40 m
Weight	
Maximum Take-Off Weight	7,500 kg
Endurance	
Payload/Armament	650 kg
Speed	Cruise: 750 km/h
Range	
Ceiling	18,000 m
IOC	
Remarks	Tricycle Type Landing Gear

Image provided by Janes.

Iran

ABABIL-3

Primary Function	ISR
NATO UAS Classification	Class I/Small
Contractor	Iran Aircraft Manufacturing Industrial Company (HESA)
Power Plant	Piston Engine
Wingspan	5 m
Length	3.5 m
Height	1 m
Weight	
Maximum Take-Off Weight	
Endurance	4 h
Payload/Armament	
Speed	200 km/h
Range	100 km
Ceiling	5,000 m
IOC	Operational in IRGC Air Force
Remarks	

Image provided by Janes.

Iran

Fotros

Primary Function	ISR and Strike
NATO UAS Classification	Class III
Contractor	
Power Plant	
Wingspan	
Length	
Height	
Weight	
Maximum Take-Off Weight	
Endurance	16 to 30 h
Payload/Armament	
Speed	
Range	2,000 km
Ceiling	7,600 m
IOC	Accepted for service
Remarks	

Image provided by Janes.

Iran

Qods Yasir (Sayed-2)

Primary Function	ISR
NATO UAS Classification	Class I/Small
Contractor	Qods Aviation Industry Company
Power Plant	2-Stroke Piston Engine
Wingspan	3.05 m
Length	1.19 m
Height	
Weight	
Maximum Take-Off Weight	
Endurance	20 h
Payload/Armament	25 kg
Speed	120 km/h
Range	450 km
Ceiling	4,600 m
IOC	Operational in IRGC and IRN Army
Remarks	Unlicensed Copy of Boeing ScanEagle

Image provided by Janes.

Iran

Saeqeh

Primary Function	
NATO UAS Classification	
Contractor	Shahed Aviation Industries
Power Plant	Turbofan/Piston
Wingspan	6–7 m
Length	
Height	
Weight	
Maximum Take-Off Weight	
Endurance	
Payload/Armament	
Speed	
Range	
Ceiling	
IOC	Operational in IRGC AF
Remarks	Based on the US-manufactured RQ-170 reconnaissance drone that crashed in Iran in December 2011

Image provided by Janes.

Iran

Shahed-129

Primary Function	ISR, Strike
NATO UAS Classification	Class III MALE
Contractor	Shahed Aviation Industries
Power Plant	Four-Cylinder, Fou-Stroke Aircraft Engine
Wingspan	16 m
Length	8 m
Height	3.1 m
Weight	
Maximum Take-Off Weight	
Endurance	24 h
Payload/Armament	400 kg
Speed	Cruise: 150 km/h
Range	2,000 km
Ceiling	7,300 m
IOC	In operational service
Remarks	Similar in size, shape and role to the US MQ-1 Predator

Annex C

Commercial Drones Fact Sheets

DJI Mavic 2 Pro

Primary Function	Private and Industrial Use
NATO UAS Classification	Class I
Manufacturer	DJI
Power Plant	Electrical Motor
Dimensions (unfolded)	322 x 242 x 84 mm
Weight	907 g
Endurance	31 min
Speed	72 km/h
Range	5 km
Max Photo resolution	20 MP
Max Video resolution	4K
Market Price	~ 1,500 Euro

Albatross

Primary Function	Private and Industrial Use
NATO UAS Classification	Class I
Manufacturer	Applied Aeronautics
Power Plant	Electrical Motor
Dimensions (unfolded)	740 x 200 x 150 mm, Wingspan 3 m
Weight	MTOW 10 kg
Endurance	1–4 h (depends on battery set up)
Speed	Cruise: 68 km/h, max: 129 km/h
Range	100 km
Max Photo resolution	Compatible with most cameras
Max Video resolution	Compatible with most cameras
Market Price	~ 3,000 Euro

Anafi

Primary Function	Private Use
NATO UAS Classification	Class I
Manufacturer	Parrot
Power Plant	Electrical Motor
Dimensions (unfolded)	175 x 240 x 65 mm
Weight	320 g
Endurance	25 min
Speed	54 km/h
Range	4 km
Max Photo resolution	21 MP
Max Video resolution	4K
Market Price	~ 650 Euro

Spreading Wings S1000+

Primary Function	Commercial and Professional Use
NATO UAS Classification	Class I
Manufacturer	DJI
Power Plant	Electrical Motor
Dimensions (unfolded)	Diagonal Wheelbase 1045 mm
Weight	MTOW 6–11 kg
Endurance	15 min
Speed	–
Range	–
Max Photo resolution	Variable Payload
Max Video resolution	Variable Payload
Market Price	~ 4,000 Euro

A15H Foldable FPV

Primary Function	Private Use
NATO UAS Classification	Class I
Manufacturer	Snaptain
Power Plant	Electrical Motor
Dimensions (unfolded)	294 x 204 x 82 mm
Weight	680 g
Endurance	7 min
Speed	–
Range	30 m
Max Photo resolution	1280 x 720 px
Max Video resolution	720 P
Market Price	~ 70 Euro

Annex D

About the Authors

(in alphabetical order)

Major Osman Aksu

Major Aksu holds a bachelor of Electronic Engineering Degree from the TURAF Academy in 2001. He had flight training and basic Weapons Controller training until 2003 in İzmir. He was assigned as a Weapons Controller at Diyarbakır CRC until 2008. After that, he was selected as AEWC Project Officer for Peace Eagle in the US. He returned to TURAF HQ Ops. Div. in 2010, and worked as PE Project Officer until 2013. He was selected as Weapons Controller at NAEW FC GK in 2013, Fighter Allocator at CRC Ankara in 2014. He was assigned as Airspace Coordination Officer in ATC Ankara between 2014 and 2019. He participated in Airspace Control-Management activities for US/Coalition OIR missions. As of November 2019, Major Aksu became the SME for CAS/JTAC in the Combat Air Branch of the JAPCC.

Dr Christian Alwardt

Dr Christian Alwardt is a senior researcher in the 'Arms Control and Emerging Technologies' project at the IFSH, where he also heads the research project 'Algorithms and Artificial Intelligence as Game Changers?'. Christian Alwardt has been conducting technology assessments since 2008, with his research focusing on topics of security and arms control policy, as well as the future of warfare. He is actively involved in expert committees, acts as a media contact and advises ministries and committees. Christian Alwardt initially studied physics, business administration and international relations at the University of Hamburg and graduated with a degree in physics. As part of his research at the CLISAP Cluster of Excellence, he received his doctorate in natural sciences.

Chief Inspector Sascha Berndsen

Sascha Berndsen, Chief Inspector. He is a member of the Signal Intelligence Division of the State Police of North Rhine-Westphalia. He started his career in 1991 as a naval officer in the German Navy, including a master degree in electrical engineering. In 2003 he changed to the State Police North Rhine-Westphalia. He has been assigned to the C-UAS section in 2015, starting at the G7 summit with C-UAS jamming operations. His responsibility today is to advance the capabilities in detecting and engaging UAS with Radio Frequency sensing, Radar, electro-optical sensors and jamming.

Joel Bollö

Joel Bollö the CEO of Micro Systemation (MSAB) in 2002, Joel served as Founder/President of DLX Group AB where he assisted technology companies in coming to market by successfully developing and launching new products and capabilities. Prior to founding DLX Group, Joel played a key role in dramatically increasing the growth of Nordic Data Distribution and subsequently at Netwise. In addition to leading MSAB in its strategic direction and day to day operations, Joel travels extensively around the world to advise senior government officials, law enforcement authorities and stakeholders regarding growing trends in technology development, privacy and encryption as it relates to public safety and digital evidence.

Captain (N) Daniel D. Cochran

Captain Cochran is currently serving as the JAPCC's Maritime Air Section Head. His background includes three operational tours in F/A-18 aircraft, with his most recent tour as a squadron commanding officer. He's flown combat missions ISO four Operations, including IRAQI FREEDOM and ENDURING FREEDOM. A graduate of the United States Naval Test Pilot School (USNTPS), he has led many aircraft test projects and instructed at USNTPS. He is a distinguished graduate of the Air Force Institute of Technology with a Master's of Science in Aeronautical Engineering and member of the Society of Experimental Test Pilots. He's accumulated 3,200 flight hours in 32 aircraft and 760 carrier arrested landings.

Lieutenant Colonel (ret.) James Corum PhD

Dr Corum holds a MA from Brown University and a PhD in History (Queen's University, Canada). He is an internationally recognized academic in military history, airpower and counter-insurgency. He has authored eleven books and more than 70 major journal articles and book chapters on strategic studies, airpower and military history. Dr Corum has had a career in higher military education, serving as a professor at the USAF School of Advanced Air and Spacepower Studies (1991–2005), professor at the US Army Command and General Staff College (2005–2008), and dean of the Baltic Defence College (2009–2014). From 2014 to 2019 he served as Programme Leader for the MA Programme in Terrorism and Security Studies at Salford University, UK.

Dr iur. Ulrich Dieckert

Dr Ulrich Dieckert is a Berlin-based lawyer, who runs his own law firm (www.dieckert.de) and has specialized in his legal work – amongst other fields – on the law of drones. He also published a guide on 'Drones – Technology and Law in Commercial and Governmental Operation' (in German); additionally, he is the chair of the expert group 'Legal Questions of Drone Operations' of UAV DACH e.V. and a member of the Advisory Council on Drones headed by the German Federal Ministry of Transportation and Digital Infrastructure.

Dr Hans-Albert Eckel

Dr Eckel is Head of Program 'Impact, Protection and Materials' at the German Aerospace Center (DLR). Within this Program, DLR develops and investigates innovative solutions for the advancement of the capabilities of the German Armed Forces. This includes laser technology, research on missile systems, aircraft structures, and telemedicine. Previously Dr Eckel was head of department 'Laserstudien und Konzepte' at DLR's Institute of Technical Physics. There he developed experimental and theoretical concept and system studies of specific, mainly defence related, applications of high power laser sources. Dr Eckel holds a diploma in physics and a PhD in laser spectroscopy. He published more than 100 scientific papers and holds several patents mainly in the field of high power lasers and laser applications.

Lieutenant Colonel Heiner Grest

Lieutenant Colonel Grest is currently serving in the C4ISR+S Branch as a Space SME. In 1982 he began his military career as a conscript. In previous appointments he has been working in various command and staff positions in the area of Surface-Based Air and Missile Defence as well as in different national staff positions. He was deployed to the NATO mission in Afghanistan at ISAF HQ. Lieutenant Colonel Grest holds a diploma in business administration from the Bundeswehr University Hamburg.

Lieutenant Colonel André Haider — Editor

Lieutenant Colonel Haider is an artillery officer by trade with over fifteen years' experience in command & control and operational planning. He is the Joint Air Power Competence Centre's (JAPCC) Remotely Piloted Aircraft Systems Subject Matter Expert for almost ten years and represents the JAPCC in the NATO Joint Capability Group Unmanned Aircraft Systems (JCGUAS) and NATO Counter-UAS Working Group. He authored multiple studies and articles with regard to operational and legal issues of UAS. He initiated and led the project 'A Comprehensive Approach to Countering Unmanned Aircraft Systems' which has resulted in the publication of this book.

Dr Martin Hellmann

Since 2010, Martin Hellmann is the Coordinator of Civil Security Research and Dual-Use at the German Aerospace Center's (DLR) overall Program Coordination for Defence & Security Research. He is also a reserve officer (Major d. R.) in the German armed forces. In his current DLR position, he is coordinator for civil security research, dual-use and EU-related topics. As a strategy and security analyst for the DLR Executive Board, he is the contact person for ministries, industry, and national and European research institutions. He is DLR representative in various national and European think tanks, working groups. Mr Hellmann holds a Diploma Degree as well as a PhD Degree in Electrical Engineering.

Lieutenant Colonel Henry Heren

Lieutenant Colonel Heren is a NATO Space & Cyberspace Strategist assigned to the JAPCC. He is a Master Space Operator and a Fully Qualified Joint Staff Officer with operational and planning experience in the Pacific, Europe, Africa, and the Middle East. After more than 28 years' service in the US Air Force, he transitioned to the US Space Force in 2020. He is a graduate of the US Air Force Weapons School, with experience in assignments focusing on Space, Cyberspace, and Electronic Warfare Operations.

Heleen Huijgen LLM BSc

Heleen Huijgen has a Bachelor's degree of Science and a Master's degree in International and European Law from the University of Amsterdam and works for the department of Military Operations at TNO. She wrote the master-thesis 'The Formation of the Legal Framework Prohibiting Chemical Weapons with Regard to Non-State Actors' under supervision of Professor Terry Gill. During an internship at the Dutch Permanent Mission to the UN in Geneva at the disarmament department, Huijgen was responsible for the preparation and organization of the Meeting of State parties to the Cluster munition convention and the preparation for the First Committee of the General Assembly meeting of the UN in New York.

Liisa Janssens LLM MA

Liisa Janssens is Scientist Law and Philosophy of Law at Military Operations, TNO and PhD-researcher at Vrije Universiteit Brussels. Janssens has a Master's degree in Law at Leiden Law School and a Master's degree in Philosophy at Leiden University and is working in her PhD research on analyses that examine AI in the scope of Philosophy of Law. Janssens was assigned to the project on 'The Internet of Things' by the Dutch Cyber Security Council (National Coordinator for Security and Counterterrorism of the Dutch Ministry of Security and Justice). Janssens was the editor of 'The Art of Ethics in the Information Society – Mind You' Amsterdam University Press (2016), and co-editor of 'Being Profiled: Cogitas Ergo Sum', Amsterdam University Press (2018).

Adam Jux

Adam Jux is a retired Royal Air Force Officer who also served in the Royal Australian Air Force and the Australian Army over his 27 years of military experience. He is a qualified targeteer having worked in the discipline for the last ten years, including on operations. He has instructed in targeting, collateral damage estimation and has mentored targeting at the Joint and Component levels. He recently consulted with the United Nations Institute for Disarmament Research (UNIDIR) and contributed to a research paper for the protection of civilians in urban conflict. He is currently working as a civilian targeteer for NATO's Joint Warfare Centre in Stavanger, Norway under contract for Comprehensive Training Solutions (CTS).

Major Fotios Kanellos

Major Kanellos graduated from the Hellenic Air Force (HAF) Academy in 2003 as an Electrical Engineer with specialization in Telecommunication and Computer Science. He holds two Master degrees, one in Technical-Economic Systems from the National Technical University of Athens (NTUA) and another in Environmental Sciences from the University of Patras. Major Kanellos served as an inspection engineer for T-2 C/E aircraft and system engineer for the T-6A Flight Simulator at the Hellenic Air Training Command (HATC) in Kalamata. His previous appointment was at the HAF Support Command (HAFSC) managing IT and Cybersecurity projects. His current appointment is as a Cyberspace SME at the Joint Air Power Competence Centre.

David Kovar

David Kovar is the CEO and founder of URSA, Inc. (Unmanned & Robotics Systems Analysis), which focuses on the collection, integration, analysis, and presentation of UAV related data for fleet management, criminal investigations, failure analysis, and predictive analysis. He has worked in digital forensics and cyber security since the mid-1990's and formerly led EY's U.S. incident response program.

Senior Chief Inspector Jürgen Künstner

Jürgen Künstner, Senior Chief Inspector, Head of Department of Special Technical Forces (mobile radio surveillance, radio reconnaissance, drone flight and drone defence) in North Rhine-Westphalia (NRW). He joined the Police in 1980, via the normal patrol service and the special units. In 1996 he joined the present State Office for Central Police Services (LZPD NRW). There he headed the Central Office for the Coordination of Operational Situations, was a member of the Advisory Group of the State of NRW and took over the present office in 2008. At that time with ten officers, this department grew to 26 employees (police officers, graduate engineers, technical staff) and is currently the best-equipped police station for drone defence in Germany.

Lieutenant Colonel Paul J. MacKenzie

A Communications and Electronics Engineering (Air) Officer in the RCAF, he examines Cyberspace as it relates to NATO Joint Air Power and from a defensive perspective through to the potential in exploiting offensive effects. He holds a Master's of Science degree in Computer and Information Technology, is a graduate of the Canadian Forces Joint Command and Staff Program and has 32 years of experience in the provision of IT/CIS to operations. His senior appointments include Director of Operational Support (CIS), CANOSCOM HQ (Ottawa), Chief A6 Staff, NATO AWACS Airbase, CO CAN Contingent (Technical Element) NATO AWACS and Director, A6 Staff – 1 CAN Air Division. He was Chief OpFor (Cyberspace) for NATO's largest Joint exercises from 2016 to 2019.

Lieutenant Colonel Roy Milke

Lieutenant Colonel Roy Milke joined the military in 1979. He completed his training as Surface-Based Air Defence Officer in 1983. This was followed by three months of special training on SA-5 (Gatschina, Soviet Union). From 1984 through 1992 he served in various SA-5 unit functions. After retraining on the Patriot weapons system (El Paso, USA), he served among others as Squadron Commander up until 2003. Then from 2003 to 2014, he worked in units dealing with maintenance and repair tasks, also the Patriot weapons system, and was deployed to Termez/Uzbekistan (2011/2012) and Kahramanmaras/Turkey (2013/2014). In 2014 Lieutenant Colonel Milke joined the Assessment, Coordination & Engagement branch at the Joint Air Power Competence Centre Kalkar, Germany.

Alex Morrow

Alex Morrow has been developing C-UAS hardware solutions since 2015 for the US Government and international partners. He works at airspace security technology company Dedrone as the Vice President of Defeat Solutions, focusing on the company's drone mitigation efforts. Prior to him joining Dedrone, Mr Morrow worked at Battelle for 18 years leading up internal research and development programs. He has expertise in electronic warfare, imaging systems, laser dazzlers, 3D camera designs, fibre optics, spectroscopy, and non-linear optics. Mr Morrow applies his vast experience in delivering cutting edge solutions by leveraging innovative solution design techniques. He lives in Ohio with his family and two cats.

Christoph Müller

Christoph Müller was recently appointed as Coordinator Defence Research at the German Aerospace Center's (DLR) overall Program Coordination for Defence & Security Research coordinating about fifty cross-cutting projects with a volume of forty-five MEUR. He previously served as the Executive Officer of the Applied Vehicle Technology Panel at the NATO Science & Technology Organization in Neuilly-sur-Seine, France, from 2017 to early 2020. He also served twelve years in the German Armed Forces implementing and commanding a specialized CBRN Explosive Ordnance Disposal platoon including one assignment to the International Security Assistant Force (ISAF) in Afghanistan. Mr Müller holds two Masters' Degrees in Mechanical Engineering and Business Administration.

Dr Thomas Neff

Dr Thomas Neff is recently the head of the department Reconnaissance and Security at the Microwaves and Radar Institute of the German Aerospace Center (DLR). Previously he was the head of the Satellite Systems Engineering group and is with DLR since 2000. He finished his PhD on Bearing Stress in Holed Polymers at the Technical University of Munich in 2001.

Wing Commander (ret.) Jez Parkinson

Wing Commander Parkinson is a RAF Regiment Officer with 33-years' regular Service; over half in the Multinational environment and in excess of 7-years on operations. He continues to work as a Reservist in the Force Protection Environment and as a civilian on Asset Protection collaborating with the military, industry and academia. He is the author of NATO FP Policy, FP Doctrine for Air Operations and the current Custodian for Joint FP Doctrine. He is responsible for the development and delivery of NATO FP Courses as well as writing several publications and articles on FP.

Phil Pitsky

Phil Pitsky is a US Navy Veteran skilled in Signals Intelligence and Electronic Warfare and has served in multiple joint, fleet, and staff positions for the Navy and Intelligence Community during his service. In the Defense Industry, he has held varying roles from Training, Operations, Program Management, and Strategic Development. In total, he brings over 20 years of industry expertise in surveillance and reconnaissance in countering emerging threats. In addition to his military service, he is a graduate of the University of North Carolina's Kenan-Flagler Business School, receiving a Master's in Business Administration in Global Business. He is currently the Vice President of US Federal Operations at airspace security technology company, Dedrone.

Lieutenant Colonel G. W. 'Berry' Pronk

Lieutenant Colonel Pronk has served for nearly 40 years in the Dutch armed forces. He served in various national Command and training positions in the realm of Ground-Based Air Defence as well as staff positions at the Royal Netherlands Air Force Command and The Royal Netherlands Army Command. Internationally he served at the former HQ Extended Air Defence Task Force (with US Army and German Airforce) and at the German Air Force Forces Command, as well as Section Chief Air Operations at J3, NATO SHAPE. Currently, the author holds the position as Subject Matter Expert for Surface-Based Air and Missile Defence at the Joint Air Power Competence Centre in Kalkar, Germany.

Dr James Rogers

Dr Rogers is DIAS Assistant Professor in War Studies, within the Centre for War Studies, at University of Southern Denmark and an Associate Fellow of LSE IDEAS within the London School of Economics. He is Special Advisor to the UK Parliament's All-Party Parliamentary Group on Drones, a UK MoD Defence Opinion Leader, and an Advisor to the United Nations. In 2020, James took up the position of NATO Country Director for the NATO SPS funded 'Vulnerabilities of the Drone Age Project'. He has previously been a Visiting Research Fellow at Stanford University, Yale University, and the University of Oxford.

Amit Samani

Amit Samani is currently serving as Vice President of Enterprise Operations for airspace security technology company, Dedrone. Amit has over 20 years of experience working within the emerging technology and security markets and has been supporting clients across critical infrastructure, aviation, and federal agencies with their strategies for taking their security from the perimeter to the lower level airspace.

Lieutenant Colonel Andreas Schmidt

Lieutenant Colonel Schmidt joined the German Air Force in 1993 and studied Computer Science at the German Armed Forces University in Munich. He built up an extensive background in Ground-Based Air Defence as Tactical Control Officer, Reconnaissance Officer, Battery Executive Officer and Battery Commander. Furthermore, he had two assignments in Fort Bliss, Texas. The main task of his first assignment was to conduct bilateral US-DEU studies for the German PATRIOT Office. During his second assignment, he was the expert on Integrated Air and Missile Defence (IAMD) at the German Luftwaffe Air Defence Centre. In between, he had an assignment in a former Air Force Division. Currently, he is the IAMD/Ballistic Missile Defence SME in the JAPCC.

Georg Schweizer

As a Swiss national, Mr Georg Schweizer received his bachelor's degree in electrical science and business economy from the University of Applied Sciences of the Canton of Zurich. In the Swiss Army, he served as a premier lieutenant in a logistics platoon. During his career in the computer, process automation and security industry, he has held international senior and management positions. He has sold, planed and realized several projects in the area of information technology, automated process control, transport and safety. On August 1, 2007, Mr Georg Schweizer joined SECURITON, a company of the Swiss Securitas Group, as Area Sales Director for perimeter protection systems.

Lieutenant Colonel (ret.) Panagiotis Stathopoulos

Lieutenant Colonel Stathopoulos graduated from the Hellenic Air Force (HAF) Academy with a BSc in Aeronautics in 1995. He holds an MSc in Human Factors and Safety Assessment in Aeronautics from Cranfield University, UK, and is a graduate of the HAF Tactical Weapons Fighter School. He is an F-16 instructor and functional check flight pilot, and he is a command pilot with more 2,000 flying hours. He has also served as director of operations and commander of the 341 Fighter Squadron from 2012 till 2016. He has served as the Electronic Warfare (EW) including SEAD Operations SME at the Joint Air Power Competence Centre from 2017 until 2020. He is now working for Airbus Defence and Space GmbH, Aircrew Publications in Manching, Germany.

Lieutenant Colonel Daniel C. Teletin — Editor

Lieutenant Colonel Teletin joined the Romanian armed forces in 1996. He graduated from the Romanian Military Technical Academy in 2001 as an aircraft maintenance officer specialized on weapons, munitions and egress systems. Hereafter he served on various positions within 95th Air Force Base, Bacau, Romania. Starting in October 2008, he undertook, for a year, his first international tour as a Military Observer within the United Nations Mission in the Democratic Republic of Congo. In July 2013 his first NATO posting materialized, serving for four years within the A4 Division at HQ Aircom, Ramstein, Germany. In August 2019 he joined the Assessment, Coordination & Engagement branch at the JAPCC in Kalkar.

Major Giuseppe Valentino

Major Valentino started his career in 1992 joining the Italian Air Force NCO School in Caserta. During his service worked in E.W. group as an Intelligence Analyst and had two tours to Sarajevo (Bosnia-Herzegovina) and was responsible for analysis and production in the Deployed Intelligence Cell. In 2005, he was engaged as a Force Protection platoon leader in Kosovo as well as supporting other key NATO operations. From 2010 to 2019 he was Section Head of COSMO-SkyMed operations in Italian Defence User Ground Segment (IDUGS). Major Valentino holds an MA with honours, in Political Science Sapienza University of Rome and an MA (level II) in Peacekeeping and Security Studies University Roma Tre, and currently serves as an ISR Subject Matter Expert at the JAPCC.

Lieutenant Colonel Dipl.-Ing. Tim Vasen

Lieutenant Colonel Vasen began his military career in July 1994 as a conscript. After his officer training he served for several years in commanding and staff positions within the artillery branch, including a deployment to KFOR as company commander of the DEU ISTAR-company. After 2005, he took over positions as an intelligence officer, responsible for IMINT planning and technical assessments, including positions in the office of military studies as a senior analyst for Space systems. From 2013 to 2017 he was part of the German Space Situational Awareness Center (GSSAC) responsible for Space intelligence. Since October 2017 he has served in the role of a Space SME at the JAPCC.

Lieutenant Colonel Daniel Wagner

Editor

Lieutenant Colonel Wagner joined the German armed forces in 1999. He completed his aviation training at Pensacola Naval Air Station in 2003 to become a Weapon Systems Officer on the TORNADO. During his time in the squadron he became a Flight Safety Officer, a Tornado Instructor, participated in several Flag exercises as well as the TLP flying course and deployed to AFG. In October 2017 he joined the Assessment, Coordination & Engagement branch at the JAPCC in Kalkar.

Lieutenant Colonel Jürgen Welsch

Lieutenant Colonel Juergen Welsch joined the German Air Force in 1984. In 1990 he gained a Bachelor Degree in Aeronautical Engineering at the Hochschule der Bundeswehr Muenchen. From 1990 on, Lieutenant Colonel Welsch worked in multiple operational- and staff positions within the field of AIRC2. In 2003, he switched to the Royal Netherlands Airforce (RNLAF). In the RNLAF, he fulfilled different operational and leadership posts, from the tactical level up to the Ministry of Defence and AIRCOM. Lieutenant Colonel Welsch participated as operator or planner in operations in Afghanistan and the Middle East. Lieutenant Colonel Juergen Welsch is working within the C4ISR+S Branch of the JAPPC as Subject Matter Expert in the field of Command and Control and Air Battle Management.

Colonel Matthew Willis — Editor

Colonel Willis graduated from the University of Cincinnati with a BSc in Aerospace Engineering and entered the US Air Force in 1990. He has been an F-16 instructor pilot, flight examiner, flight commander and assistant director of operations. He has also served as a director of operations and squadron commander of flying training and support squadrons. He is a command pilot with more than 2,400 flying hours, including more than 100 combat hours, and was a SEAD Instructor Pilot in the F-16CJ. Most recently, Colonel Willis finished two consecutive foreign affairs tours as the US Defence Attaché to Poland and as the Air Attaché to Israel. He is currently serving as the Combat Air Branch Head at the Joint Air Power Competence Centre.

Major Andreas Wurster

Major Wurster is the Subject Matter Expert for Intelligence in the JAPCC. He joined the German Armed Forces in 1993 and started his career as Military Security NCO. In 2009 he became as a Warrant Officer an Intel Analyst and was responsible for the analysis of countries in order to assess the probability of evacuating Germans and other people by German Armed Forces. He was deployed three times on NATO missions in Afghanistan as an Intel Analyst and Intel Military Assistant, responsible for Intelligence Training for the Afghan Forces. Major Wurster graduated a two-year study in economic computer science at the Bundeswehr College for business and computer science and did several Intelligence Courses in NATO training centres.

Dr Ing. Dirk Zimper

Dr Zimper was recently appointed as Executive Board Representative Defence and Security Research at the German Aerospace Center's (DLR). He also acts as the Managing Director of the newly founded Responsive Space Cluster Competence Center. Dr Zimper previously served in various leadership positions within the DLR, NATO and the Bundeswehr. In 2020, Dr Zimper was appointed as Member to NATO's Science & Technology Board by the German MoD and works as an adviser for the Munich Security Conference. He holds a Diploma Degree as well as a Doctoral Degree in Aerospace Engineering and has published more than 35 scientific papers. Dr Zimper has been bestowed with the Bronze Cross of Honour of the Bundeswehr, the NATO Executive Service Award as well as the NATO AVT Panel Excellence Award.

Annex E

Table of Figures

Figure 1.1 Unmanned Aircraft System Components 13

Figure 1.2 Levels of Drone Autonomy.....15

Figure 1.3 Spatial Arrangement of Unmanned Aircraft System Components 17

Figure 4.1 Chinese Wing Loong (l.) and US MQ-1B Predator (r.) 57

Figure 4.2 Average Consumer Drone Audibility 59

Figure 4.3 Potential Satellite Ground Terminals at Hmeimim Airbase, Syria 67

Figure 5.1 C-UAS Methodology.....76

Figure 6.1 Intelligence Cyle and JISR process within C-UAS 88

Figure 6.2 UAS Frequency Bands.....95

Figure 7.1 Difference between Manned and Unmanned Aerial Systems.....106

Figure 7.2 The Role of SBAMD in Threat Mitigation.....109

Figure 8.1 ISIL/DAESH Drones Captured during Operation EAST MOSUL, Iraq 132

Figure 8.2 PKK Drones Captured in Hakkari, Turkey..... 133

Figure 8.3 Russian-Made Panstir S-1 Air Defence System 141

Figure 8.4 Bayraktar TB2 Armed UA 142

Figure 8.5 Air Interdiction Targets 143

Figure 9.1 Phases of the Joint Targeting Cycle 148

Figure 9.2 An example of the CARVER methodology based on UAS discussion. 153

Figure 9.3 Notional CARVER Value Rating Scale given as an example 154

Figure 10.1 Comparative RCS values of various platforms on indicative purposes 170

Figure 10.2 Commercial applications in the radio spectrum, whose waves can illuminate a LSS UAS to a passive sensor. 173

Figure 10.3 Electro-optics and Lasers Spectrum. 175

Figure 11.1 Cyber Kill Chain 186

Figure 11.2 Block Diagram of a Typical UAS 189

Figure 11.3 UAV System [sic] Cyber-Security Threat Model 192

Figure 11.4 C-UAS Vectors and C-UAS Attack Hardware/Software 201

Figure 12.1 UAS using Satellite Communications 216

Figure 12.2 Uplink Jamming..... 222

Figure 12.3 Downlink Jamming 223

Figure 15.1 layered approach to C-UAS..... 278

Figure 17.1 Critical Infrastructure Sectors. 305

Figure 19.1 Typical UAV Deployment Scenario 342

Figure 20.1 The Common Offences Using Drones..... 352

Figure 20.2 The Security Triangle 353

Figure 20.3 Drone Detection – Chances and Risks..... 356

Figure 20.4 Example of a portable, small and lightweight RF sensor..... 360

Figure 20.5 Security Cloud application using the example of a drone detection system for private or government use 366

Figure 20.6 Implementation of security cloud applications..... 367

Figure 20.7 Deployable drone defence system with high-performance sensors, effectors and built-in command and control centre..... 368

Figure 20.8 3D Drone Position Picture 369

Figure 24.1 Bridging the Valley of Death by governmentally funded research 440

Figure 24.2 Technology adoption rates measured as the percentage of households in the United States 441

Figure 24.3 Selected emerging technologies relevant for (counter) UAS technologies projected on Gartner Hype Cycle. 442

Figure 24.4 Principle function of Visual Odometry. 447

Figure 24.5 Transportable optical ground station (TOGS) and the 'Free-space Experimental Laser Terminal II' 449

Figure 24.6 RD&A and projected In-Service timespans of exemplary defence projects 455

Figure A.1 NATO UAS Classification Table 510

Annex F

List of Acronyms

A2AD	Anti-Access Area Denial
AAA	Anti-Aircraft Artillery
AAP	Allied Administrative Publication
ACCS	Air Command and Control System
ACINT	Acoustic Intelligence
ACT	Allied Command Transformation
AD	Air Defence
AEA	Airborne Electronic Attack
AI	Air Interdiction
AI	Artificial Intelligence
AirC2IS	Air Command and Control Information System
AIRCOM	Allied Air Command
AJP	Allied Joint Publication
ALIT	(CHN) Aerospace Long-March International Trade Company Ltd
AMD	Air and Missile Defence
AOD	Air Operations Directive

AOO	Area of Operations
AP	Additional Protocol (of the Geneva Conventions)
ARM	Anti-Radiation Missile
ATC	Air Traffic Control
ATO	Air Tasking Order
ATP	Allied Tactical Publication
BDA	Battle Damage Assessment
BLOS	Beyond Line of Sight
BMC3I	Battle Management, Command, Control, Communications and Intelligence
BMD	Ballistic Missile Defence
BRI	(CHN) Belt and Road Initiative
C2	Command and Control
C3	Command, Control and Communication
CA	Canada
CAOC	Combined Air Operations Centre
CARD	Coordinated Annual Review on Defence

CAS	Close Air Support
CASIC	China Aerospace Science and Industry Corporation
CBR	Chemical, Biological or Radiological
CBRN	Chemical, Biological, Radiological, and Nuclear
CCDCOE	(NATO) Cooperative Cyber Defence Centre of Excellence
CCIR	Commander's Critical Information Requirements
CCW	(UN) Convention on Certain Conventional Weapons
CDL	Common Data Link
CEP	Circular Error Probable
CESMO	Cooperative Electronic Support Measures Operations
cf.	Compare (Latin: conferatur)
CFE	(Treaty on) Conventional Armed Forces in Europe
CH	Switzerland

CHN	China
CIA	(US) Central Intelligence Agency
CIA	Confidentiality, Integrity, and Availability
CM	Cruise Missile(s)
CNAS	(US) Center for a new American Security
CoE	Centre of Excellence
COMAO	Composite Air Operation
COMINT	Communications Intelligence
COP	Common Operational Picture
COTS	Commercial-Off-The-Shelf
CPES	Cyber Physical Engineered System
CPRA	Controlled Radiation Pattern Antenna
CPU	Central Processing Unit
CR	Collection Requirement(s)
C-RAM	Counter-Rocket, Artillery, and Mortar
CRC	Control and Reporting Centre
CRS	(US) Congressional Research Service

C-SAFIRE	Counter-Surface to Air Fire
CSIS	(US) Center for Strategic & International Studies
CTL	Collection Task List
C-UAS WG	(NATO) Countering Unmanned Aircraft System Working Group
C-UAS	Counter-Unmanned Aircraft System(s)
CW	Continuous Wave
DAESH	Dawlah al-Islāmiyah Irāq wa-as Shām (cf. ISIL)
DAL	Defended Asset List
DCA	Defensive Counter-Air
DDoS	Distributed Denial of Service
DEAD	Destruction of Enemy Air Defence
DEW	Directed Energy Weapons
DFS	Deutsche Flugsicherung (German Air Traffic Control Service)
DLR	German Aerospace Center
DoD	Department of Defence

DoS	Denial of Service
DOTMLPFI	Doctrine, Organisation, Training, Materiel, Leadership, Personnel, Facilities and Interoperability
DPS	Data, Products and Services
DRAM	Dynamic Random-Access Memory
DRONEII	(GE) Drone Industry Insights
DSCA	Defence Support of Civil Authorities
DSIAC	(US) Defense Systems Information Analysis Center
E&T	Education and Training
Ed.	Editor
EDF	European Defence Fund
EDIDP	European Defence Industrial Development Programme
Eds.	Editors
EGF	European Gendarmerie Force
ELINT	Electronic Intelligence
EM	Electro Magnetic

EME	Electromagnetic Environment
EMI	Electro-Magnetic Impulse
EMO	Electromagnetic Operations
EMP	Electro-Magnetic Pulse
EMS	Electromagnetic Spectrum
EN	Estonia
EO	Electro-Optical
EOB	Electronic Order of Battle
ESM	Electronic Support Measures
EU	European Union
EW	Electronic Warfare
EWS	Electronic Warfare System
F2T2EA	Find, Fix, Track, Target, Engage, and Assess
FAA	(US) Federal Aviation Administration
FAS	(US) Federation of American Scientists
FEZ	Fighter Engagement Zone
FHM	Fault Handling Mechanism

FMV	Full Motion Video
FoA	Freedom of Action
FOC	Full Operational Capability
FOUO	For Official Use Only
FP	Force Protection
FSO	Free Space Optics
F-UA	Friendly Unmanned Aircraft
FY	Fiscal Year
GAIC	(CHN) Guizhou Aircraft Industry Corporation
GCS	Ground Control Station
GDT	Ground Data Terminal
GE	Germany
GEO	Geostationary Earth Orbit
GHz	Gigahertz
GIADS	German Improved Air Defence System
GMTI	Ground Moving Target Indicator
GNA	Government of National Accord (Interim Government for Libya)

GNSS	Global Navigation Satellite Systems
GPS	Global Positioning System
GR	Greece
GRD	Ground Resolved Distance
GSM	Global System for Mobile Communications
GWOT	Global War on Terror
HALE	High-Altitude Long-Endurance
HD	High Definition
HEL	High Energy Lasers
HEO	Highly Elliptical Orbit
HESA	Iran Aircraft Manufacturing Industrial Company
HPM	High-Power Microwaves
HtK	Hit-to-Kill
HUMINT	Human Intelligence
I&W	Indication and Warning
IAI	Israeli Aerospace Industries

IAMD	Integrated Air and Missile Defence
ICAO	International Civil Aviation Organization
ICBM	Inter Continental Ballistic Missile
ICDS	(EN) International Centre for Defence and Security
ICRC	International Committee of the Red Cross
ICUAS	International Conference on Unmanned Aircraft Systems
IDA	(US) Institute for Defense Analyses
IDF	Indirect Fire
IED	Improvised Explosive Device(s)
IEEE	Institute of Electrical and Electronics Engineers
IFF	Identification, Friend or Foe
IGO	Intergovernmental Organization
IHL	International Humanitarian Law
IISS	(UK) International Institute for Strategic Studies
IMINT	Imagery Intelligence

INF	Intermediate-Range Nuclear Forces (Treaty)
INS	Inertial Navigation System
IoD	Internet of Drones
IOSB	(GE) Fraunhofer Institute of Optronics, System Technologies and Image Exploitation
IoT	Internet of Things
IP	Internet Protocol
IR	Infrared
IRGC	(Iranian) Islamic Revolutionary Guard Corps
IRNSS	Indian Regional Navigation Satellite System
ISAR	Inverse Synthetic Aperture Radar
ISIL	Islamic State of Iraq and the Levant
ISIS	The Islamic State of Iraq and Syria
ISR	Intelligence, Surveillance & Reconnaissance
IT	Information Technology
IT	Italy
JFAC	Joint Force Air Component

JFC	Joint Force Command(er)
JIPOE	Joint Intelligence Preparation of the Operational Environment
JISR	Joint Intelligence, Surveillance, and Reconnaissance
JOA	Joint Operation Area
LAWS	Lethal Autonomous Weapon System(s)
LEO	Low Earth Orbit
LiDAR	Light Detection and Ranging
LM	(US) Lockheed Martin
LNA	Libyan National Army
LOAC	Laws of Armed Conflict
LoC	Line(s) of Communication
LOS	Line of Sight
LR	Long-Range
LRE	Launch and Recovery Element
LRFD	Laser Range Finder Designator
LRU	Launch and Recovery Unit

LSE	(UK) London School of Economics
LSS	Low, Slow and Small
LTE	Long-Term Evolution
MAC	Media Access Control
MACA	Military Aid to the Civil Authorities
MACP	Military Aid to the Civil Power
MALE	Medium-Altitude Long-Endurance
MANPADS	Man Portable Air Defence System
MARA	Multidimensional Autonomy Risk Assessment
MASINT	Measurement and Signature Intelligence
MCE	Mission Control Element
MDO	Multi-Domain Operation
MEO	Medium Earth Orbit
METOC	Meteorology and Oceanography
MEZ	Missile Engagement Zone
MGCS	Mobile Ground Control Station
MJO	Major Joint Operation

MoE	Measures of Effectiveness
MR	Medium-Range
MSAB	(SWE) Micro Systemation AB
MTCR	Missile Technology Control Regime
MTS	Multi-spectral Targeting System
NAS	National Airspace System
NASA	(US) National Aeronautics and Space Administration
NATINAMDS	NATO Integrated Air and Missile Defence System
NATO	North Atlantic Treaty Organization
NAVIC	Navigation Indian Constellation
NBC	Nuclear, Biological, and Chemical
NDPP	NATO Defence Planning Process
NE	The Netherlands
NET	NATO European Territory
NGO	Non-governmental Organisation
NIAG	NATO Industrial Advisory Group

NO	Norway
NOAA	(US) National Oceanic and Atmospheric Administration
NSAA	Non-State Armed Actors
NSO	NATO Standardization Office
NSR	(RUS) Northern Sea Route
NU	NATO Unclassified
NVRAM	Non-Volatile Random-Access Memory
OCA	Offensive Counter-Air
OIR	Operation Inherent Resolve
OP	Observation Post
OSINT	Open Source Intelligence
O-UA	Opposing Unmanned Aircraft
PAC	Preventive Arms Control
PCI DSS	Payment Card Industry Data Security Standard
PCL	Passive Coherent Location
PED	Processing, Exploitation and Dissemination

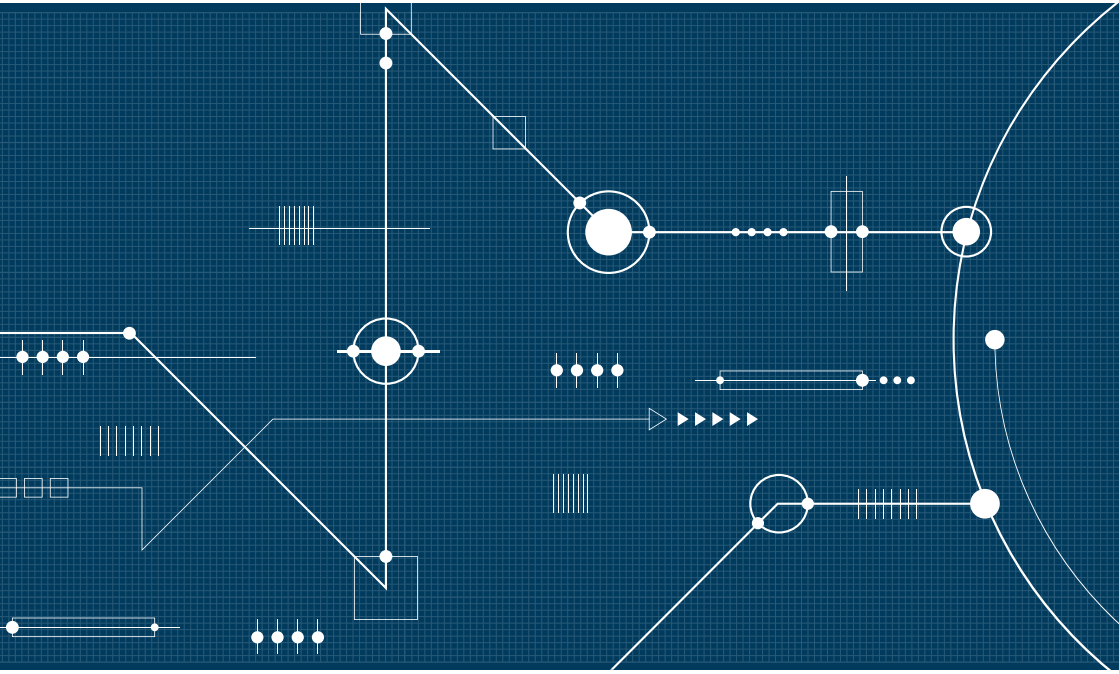
PESCO	Permanent Structured Cooperation
PGM	Precision-Guided Munitions
PNT	Position, Navigation, and Timing
PRIO	(NO) Peace Research Institute Oslo
PTZ	Pan-Tilt-Zoom
QRA	Quick Reaction Alert
QZSS	Quasi-Zenith Satellite System
R&D	Research and Development
RAM	Random Access Memory
RAP	Recognized Air Picture
RCE	Remote Code Execution
RCS	Radar Cross Section
RD&A	Research, Development and Acquisition
ret.	Retired
RF	Radio Frequency
RID	Remote Identification
RNSS	Regional Navigation Satellite System

RO	Romania
ROE	Rules of Engagement
ROSCOSMOS	(RUS) State Corporation for Space Activities
RPA	Remotely Piloted Aircraft
RUS	Russia
RUSI	(UK) Royal United Services Institute for Defence and Security Studies
SA	Situational Awareness
SACEUR	Supreme Allied Commander Europe
SACT	Supreme Allied Command(er) Transformation
SAM-PRAS	Surface to Air Missile – Precision Rating and Analysis Software
SAR	Synthetic Aperture Radar
SATCOM	Satellite Communications
SBAD	Surface-Based Air Defence
SBAMD	Surface-Based Air and Missile Defence
SEAD	Suppression of Enemy Air Defence
SEW	Shared Early Warning

SHORAD	Short-Range Air Defence
SHORADEZ	Short-Range Air Defence Engagement Zone
SIGINT	Signals Intelligence
SIPRI	(SWE) Stockholm International Peace Research Institute
SME	Subject Matter Expert
SOF	Special Operations Forces
SRAM	Static Random-Access Memory
SRL	System Readiness Level
SSA	Space Situational Awareness
START	Strategic Arms Reduction Treaty
STI	Scientific and Technical Intelligence
STO	(NATO) Science & Technology Organization
STRATCOM	Strategic Communications
sUAS	Small Unmanned Aircraft System(s)
SWaP	Size, Weight, and Power
SWE	Sweden

TAOR	Tactical Area of Responsibility
TBIJ	(UK) The Bureau of Investigative Journalism
TBMF	Tactical Battle Management Functions
TCDL	Tactical Common Data Link
TCPED	Tasking, Collection, Processing, Exploitation and Dissemination
TECHINT	Technical Intelligence
TNO	The Netherlands Organisation for Applied Scientific Research
TRL	Technology Readiness Level
TSA	Target Systems Analysis
TST	Time-Sensitive Targeting
TTP	Tactics, Techniques and Procedures
TU	Turkey
U	Unclassified
UA	Unmanned Aircraft
UAS	Unmanned Aircraft System(s)
UAV	Unmanned Aerial Vehicle

UK	United Kingdom
UN	United Nations
UNIDIR	United Nations Institute for Disarmament Research
URL	Uniform Resource Locator
URSA	(US) Unmanned & Robotics Systems Analysis
US	Unites States (of America)
USNI	United States Naval Institute
USV	Unmanned Surface Vessel
UV	Ultraviolet
UWCA	(RUS) Ural Works of Civil Aviation
UWS	Unmanned Weapons System(s)
VCP	Vehicle Check Point
VDL	Video Data Link
vet.	Veteran
VO	Visual Odometry
VPN	Virtual Private Network



Countering UAS and drones is a challenge in both the military and civil domains. Therefore, it is important to incorporate all available means and to exploit any vulnerabilities to achieve this task. It is also important to note that countering UAS and drones is already a security mission in peacetime, whereas most military defence applications are intrinsically designed for a conflict scenario. To stimulate thought on a more comprehensive approach when having to counter UAS and drones, this book provides the reader with a broad assortment of the different military, civil, and legal perspectives on the subject matter.

Joint Air Power Competence Centre

von-Seydlitz-Kaserne
Römerstraße 140 | 47546 Kalkar (Germany) | www.japcc.org

Follow us on Social Media