

INTEGRATED AIR & MISSILE DEFENCE CENTRE OF EXCELLENCE

Souda Air Base

73100 Chania

<https://www.iamd-coe.org>



**“With guns you can
kill terrorists, with
education you can kill
terrorism” Malala
Yousafzai**

The Evolving Asymmetric Threat of Unmanned Aircraft Systems: A Weapon of Choice for Non- State Actors, How Alliance Could Diminish Such Threat

By Antigoni Blazogiannaki (intern)

This paper reflects only the IAMDCOE policies and its authors' positions, and it is not intended to create any legal obligations, nor does it reflect NATO's policies or positions, or engage NATO in any way.

Acknowledgments

I would like to acknowledge and give my warmest thanks to the Concept Development & Experimentation Branch of IAMD COE for their support and guidance. To B. Gen. E. Panou, LtC. I. Stathakis, LtC D. Koutsoukos, LtC. K. Kirilov, Cpt. E. Mavrogiannakis, Maj. I. Kotronakis for their time, effort, useful advice, and suggestions throughout the research process.

Table of Contents

1. Introduction	1
2. Terminology	2
3. History of drone warfare	6
4. Features that make UAS attractive to non-state actors	12
5. Challenges of Countering UAS	16
6. Techniques and strategies that can diminish the impact of non-state actors use of UAS	20
6.a. Drone Forensics	21
6a.a. OSINT	21
6a.b. Radio Frequency (RF) Analysis	22
6c. Laser.....	24
6d. Urban Air Traffic Management (UATM)	26
7. Future Threats.....	27
7a. Artificial Intelligence (AI)	27
7b. Commercial off-the-shelf (COTS)	29
7c. Additive Manufacturing (3D printers)	30
7d. Other types of drones and drone swarms	31
7e. UAS used for Improvised Explosive Devices (IEDs)	34
8. Conclusion and Recommendations.....	36

1. Introduction

We live in a world where security threats are not just a local or national matter but a global one, challenging traditional defenses and demanding innovative responses. Amongst these threats, terrorism remains one of the most pervasive and complex security threats that globally affects international stability and prosperity. As NATO has stated, terrorism is perceived the most direct asymmetric threat that knows no border, nationality or religion, and it is considered one of the two main threats to the Alliance.

Terrorism has a long history, however, the form of terrorism over the years is constantly evolving. The evolution of terrorist threats is a consequence of the progressing terrorist motivations, the rise of information technology and the aforementioned ease with which information is disseminated, the accelerating urban centralization of vital components of national infrastructure along with the escalation of Weapon of Mass Destruction (WMD) technology.¹ Therefore, aerial terrorism is gradually emerging as a forceful form of terrorism capable of causing substantial damage to human life and infrastructure. Recent advancements in technology have provided non-state actors with unprecedented access to powerful tools that were once the exclusive domain of nation-states. One such tool is the Unmanned Aircraft System (UAS), commonly referred to as drones, which has rapidly evolved into a weapon of choice for non-state actors due to its accessibility, cost-effectiveness, and operational flexibility. At the time of writing, there are 113 states that have military drone programs and 65 non-state that are able to utilize drones, whereas the figure it is highly likely to go higher.² Drones are changing and developing the characteristics of nowadays' warfare, increasing the killing capacity in the hands of non-state actors, creating a potential more threaten environment for the NATO Alliance and Partners.

The present paper aims to explore why drones have become a favored weapon among non-state actors, assess the implications of this trend for NATO and its partners, and examine countermeasures that can mitigate the threat. The paper is structured to provide a comprehensive review of UAS terminology,

¹ Nikola Brzica. Understanding Contemporary Asymmetric Threats. Croatian International Relations Review, vol. 83, no. XXIV, 2018.

² Christina Schori Liang. Building Resilience Against Terrorist Attacks Involving Uncrewed Aerial Systems. Geneva Centre for Security Policy, no. 5, 2023

trace the history of drone warfare, outline the features that make UAS attractive to non-state actors, discuss the challenges in countering UAS, and propose strategies to diminish the impact of UAS misuse. Finally, it highlights emerging technological advancements, including artificial intelligence, that could escalate the complexity and lethality of future UAS threats.

2. Terminology

To effectively present this research, it is crucial to clarify the key terms used throughout. It is important to mention that for some of these terms there is no universal definition. For this paper, it is being used 'The Official NATO Terminology Database' to indicate the definition of these terms which are fundamental for the better comprehension of this paper.

Artificial Intelligence (AI): Artificial intelligence is considered “an interdisciplinary field, usually regarded as a branch of computer science, dealing with models and systems for the performance of functions generally associated with human intelligence, such as reasoning and learning.”³

There are two types of AI, the weak and the strong. Weak AI is the standard, trained to perform limited tasks such as Alexa and Siri which are applications powered by artificial intelligence, designed to perform tasks such as setting reminders, answering questions etc. Strong AI, commonly referred to as artificial general intelligence and involved a range of analytics similar to humans.

Asymmetric Threat (NATO 6844): “A threat emanating from the potential use of dissimilar means or methods to circumvent or negate an opponent’s strengths while exploiting his weaknesses to obtain a disproportionate result.”⁴

The 21st century’s main security threats are posed by hostile acts by extremists, terrorists and organized crime. Taking that into consideration, we can agree with Nikola Brzica that one of the most common manifestations of asymmetric threats with the most gathered attention, has been terrorism.⁵

³ NATO. The official NATO Terminology Database. <https://nso.nato.int/natoterm/content/nato/pages/home.html?lg=en> (Accessed 2024-03-01).

⁴ Ibid

⁵ Nikola Brzica. Understanding Contemporary Asymmetric Threats. Croatian International Relations Review, vol. 83, no. XXIV, 2018.

Counter Terrorism (NATO 25793): “All preventive, defensive and offensive measures taken to reduce the vulnerability of forces, individuals, and property against terrorist threats and /or acts to respond to terrorist acts.”⁶

COTS/ Commercial off-the-shelf (NATO 13006): “Pertaining to a commercially marketed product which is readily available for procurement and normally used without modification.”⁷

The fast-paced technological progress of the commercial area has resulted in cheap, manageable, and disposable UASs to become available to any individual⁸. Particularly, when Federal Aviation Administration (FAA) approved the commercial use of drones beyond the pilot’s line of sight in conjunction with the fact that state and non-state actors can easily acquire drones and drone technology through off-the-shelf options, it is easily understood that the future of countering weaponized drones would be significantly harder.⁹

Open Source Intelligence / OSINT (NATO 12186): “Intelligence derived from publicly available information, as well as other unclassified information that has limited public distribution or access.”¹⁰

It is important to mention here that OSINT can be both a primary and secondary function. Primary as an all-source primary resource which it acts and stands alone with a combination of human sources, open geospatial data, and public analysis. And secondary, as a secondary function to its classified counter parts.¹¹ OSINT results have the objective of supporting decision and policy making processes. Hence, OSINT can be used in a variety of fields such

⁶ NATO. The official NATO Terminology Database. <https://nso.nato.int/natoterm/content/nato/pages/home.html?lg=en> (Accessed 2024-03-01).

⁷ Ibid

⁸ NORTH ATLANTIC COUNCIL. NATO Countering Class I Unmanned Aircraft Systems (C-UAS) Handbook. NATO, vol. 2, no. 2, 2020.

⁹ Thomas G. Pledger. The role of drones in future terrorist attacks. Land Warfare Paper, vol. 137, no. 137, 2021.

¹⁰ NATO. The official NATO Terminology Database. <https://nso.nato.int/natoterm/content/nato/pages/home.html?lg=en> (Accessed 2024-03-01).

¹¹ Fordred, A (2023) Cyber Institute, ‘OSINT MINI’, <https://courses.thecyberinst.org/courses/osintworkshop>

as law enforcement, security professionals and investigators.¹² This method could be considered applicable and quite useful in terms of counter terrorism as well.

Terrorism (NATO 18957): “The unlawful use or threatened use of force or violence, instilling fear, and terror, against individuals or property in an attempt to coerce or intimidate governments or societies, or to gain control over a population, to achieve political, religious or ideological objectives.”¹³

Unmanned Aircraft Systems (UAS) (NATO 6475): “A system whose components include the unmanned aircraft, the supporting network and all equipment and personnel necessary to control the unmanned aircraft”. For the last 10 years, UAS or as often it will be referred to this paper, drones, have been experiencing healthy growth worldwide.¹⁴

¹² Jeff M, (2023), Udemy, ‘OSINT: Open Source Intelligence’, <https://www.udemy.com/course/osint-open-source-intelligence>

¹³ NATO. The official NATO Terminology Database. <https://nso.nato.int/natoterm/content/nato/pages/home.html?lg=en> (Accessed 2024-03-01).

¹⁴ Ibid

NATO UAS CLASSIFICATION						
Class	Category	Normal Employment	Normal Operating Altitude	Normal Mission Radius	Primary Supported Commander	Example Platform
Class III (> 600 kg)	Strike/Combat*	Strategic/National	Up to 65,000 ft	Unlimited (BLOS)	Theatre	Reaper
	HALE	Strategic/National	Up to 65,000 ft	Unlimited (BLOS)	Theatre	Global Hawk
	MALE	Operational/Theatre	Up to 45,000 ft MSL	Unlimited (BLOS)	JTF	Heron
Class II (150 kg - 600 kg)	Tactical	Tactical Formation	Up to 18,000 ft AGL	200 km (LOS)	Brigade	Hermes 450
Class I (< 150 kg)	Small (>15 kg)	Tactical Unit	Up to 5,000 ft AGL	50 km (LOS)	Battalion, Regiment	Scan Eagle
	Mini (<15 kg)	Tactical Subunit (manual or hand launch)	Up to 3,000 ft AGL	Up to 25 km (LOS)	Company, Platoon, Squad	Skylark
	Micro** (<66 J)	Tactical Subunit (manual or hand launch)	Up to 200 ft AGL	Up to 5 km (LOS)	Platoon, Squad	Black Widow

Table 1: NATO UAS Classification Table (NATO UNCLASSIFIED)

3. History of drone warfare

Drones have been part of warfare for a longer time than we can imagine. Over the years, the progression of drone technology has evolved significantly, reflecting the evolution of warfare practices. This evolution has led in the utilization of drones as invaluable assets within military and non-state groups.

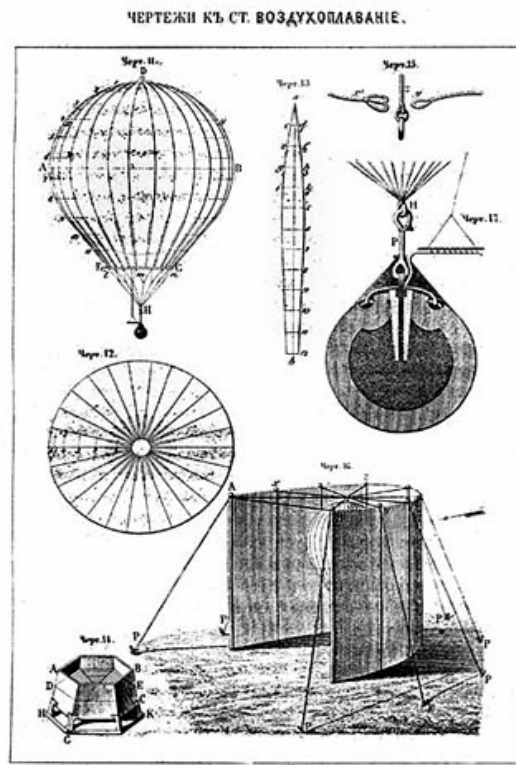


Figure 1: pilotless hot-air balloon controlled by timed fuses

There are three different perspectives regarding the first drone that has been used. From the historical perspective, it was in July 1849 when Austrians bombed Venice by using pilotless hot-air balloons armed with bombs controlled by timed fuses.¹⁵

¹⁵ Remote piloted aerial vehicles. Remote Piloted Aerial Vehicles : An Anthology. Remote piloted aerial vehicles. 2003-02-02. https://www.ctie.monash.edu/hargrave/rpav_home.html (Accessed 2024-03-).

From the aviation perspective, it was during the First World War, after Wright brothers presented powered flight when the first remote control plane was developed.¹⁶ Britain's Aerial Target, it was a small radio-controlled aircraft that was first tested in March 1917 while the American aerial torpedo known as Kettering Bug first flew in October 1918.¹⁷ However, neither were used operationally during the war.



Figure 2: Aerial Target from the First World War (IWM's collection)

From the military perspective, the first use of drone in battle was in 1973, during the Yom Kippur War, 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 defenses were degraded as a result. This success could be considered the commencement point for both Unmanned Aerial Vehicles (UAV) and Unmanned Aerial System (UAS) as the dominant feature in most modern militaries.¹⁸

¹⁶ "History of Drone Warfare", The Bureau of Investigative Journalism, 4 September 2020, <https://www.thebureauinvestigates.com/explainers/history-of-drone-warfare/>

¹⁷ Imperial War Museums. A Brief History of Drones. Imperial War Museums. <https://www.iwm.org.uk/history/a-brief-history-of-drones> (Accessed 2024-02-20).

¹⁸ Joint Air Power Competence Centre. A Comprehensive Approach to Countering Unmanned Aircraft Systems, The Joint Air Power Competence Centre, von-Seydlitz-Kaserne, Römerstraße 140, 47546 Kalkar, Germany.: Joint Air Power Competence Centre, 2020,.

The term “drone” was first used after the UK developed the Queen Bee (1947), also known as “the mother of all drones”. Queen Bee was the first full production full-sized, reusable, unmanned aircraft. The aircraft could be functioned remotely by another pilot or controller sitting in another aircraft, on a warship or from a control panel on land. It could operate from runways or be shot from catapults, to be recovered on floats. Queen Bee was certainly the first truly successful pilotless aircraft.¹⁹



Figure 3: Queen Bee, 1947 (IWMs collection)

There were some key technological developments that made drones the predominant in today’s battlefield:

- a) 1970s: Developing of aircraft with glider-like properties with incredible long, thin wings that could hold the plane aloft at altitude for hours (endurance)
- b) 1990s: Ability to loiter combined with the use of transmitters to send the footage straight back to battlefield commanders
- c) 2000s: US Air Force and CIA became the first to successfully fit drones with missiles, as part of a failed CIA attempt to kill Osama bin Laden.
- d) The rise of Lithium-ion (Li-ion) batteries which replaced Nickel Metal Hybride (NiMH) and Lithium-Polymer (LiPo) batteries gave a range of advantages to drone industry.²⁰

¹⁹ Dave O’Malley, ‘The mother of all drones’, Vintage Wings of Canada <https://www.vintagewings.ca/stories/mother-of-all-drones>

²⁰Kami Shah. The Evolution and Future of Drone Battery Technology. Drones Technology. 2024-03-08. <https://dronstechnology.com/the-evolution-and-future-of-drone-battery-technology/> (Accessed 2024-07-31).

e) The evolution on electric motor and specifically on ‘outrunner’ motor provided reliability as the number of moving parts reduced and the costs for the improved motors were significantly decreased as their utility became more widespread amongst mass-market users.²¹

It was on November 12, 2001, when USA launched its first successful drone strike in Afghanistan, two months after the terrorist attacks of September 11. Since then, remotely striking has become one of the main components of US counterterrorism strategy.²²

Regarding non-state actor use of drones, the first known attempt to weaponize a drone was in 1994 when Aum Shinrikyo, a Japanese terror group failed trials to release sarin by using a remote-control helicopter.²³ As for the first lethal UAV attack by a non-state actor, it took place in 2014 when Hezbollah killed several al – Nusra Front Fighters in Syria.

Initially, Syria civil war was considered the most-drone- dense conflict.²⁴ Nevertheless, Ukraine-Russia war is now considered the first full-scaled drone war, and at the time of writing has not been ending yet. According to Forbes’ article, Ukraine military is acquiring at least 50,000 FPVs a month, in the amount of a few hundred dollars per drone.²⁵ Hence, it can be presumed that Ukraine war might be the most drone- dense conflict.

²¹M. J. Logan, J. Chu, M. A. Motter et al. Small UAV Research and Evolution in Long Endurance Electric Powered Vehicles. NASA, 2007

²²K. A. Greico, J. W. Hutto. Can drones coerce? The effects of remote aerial coercion in counterterrorism. *International Politics*, 2021.

²³ K. Chavez, O. Swed. Off the Shelf: The Violent Nonstate Actor Drone Threat. *Air & Space Power Journal*, 2020.

²⁴ K. Chavez, O. Swed. The proliferation of drones to violent nonstate actors. *Defence Studies*, 2020.

²⁵ David Axe. In The Hottest Sector of The Ukraine War, The Ukrainians Might Deploy As Many Drones As The Russians Deploy Soldiers. *Forbes*. 24-03-10. <https://www.forbes.com/sites/davidaxe/2024/03/10/in-the-hottest-sector-of-the-ukraine-war-the-ukrainians-might-deploy-as-many-drones-as-the-russians-deploy-soldiers/> (Accessed 2024-06-20).

Table 2

Examples of UAS attacks involving non-state armed groups, planned or attempted terrorist attacks that took place using aerial drones.

<i>Year</i>	<i>Country</i>	<i>Non-State armed group</i>	<i>Deployment Type</i>
1994	Japan	Aum Shinrikyo	Planned attack to spread sarin gas using remotely controlled helicopters.
2002	Colombia	Fuerzas Armadas Revolucionarias de Colombia (FARC)	Nine model aero planes recovered by the Colombian military, believed to have been used to smuggle drugs.
2013	Pakistan	Al-Qaeda	A planned multiple drone attack was stopped by local law enforcement.
2014	Iraq and Syria	Islamic State	Commercial off-the-shelf and homemade aerial drones at scale were started being used during military operations.
2015	Japan	Environmental activist	A UAV carrying radioactive material landed on the roof of the Prime Minister’s office in a protest against government policy.
2016	Iraq	Da’esh	Between 30 September 2016 and 11 February 2018, researchers identified 338 reports of UAV use by Da’esh in Iraq and the Syrian Arab Republic, of which 262 involved offensive action. This included the use of “booby trapping” UAVs to explode on recovery, deploying them as one-way attack UAVs, and use to guide vehicle-borne IED attacks, among others.
2018	Mali	Jama’at Nusrat al-Islam wal-Muslimin (JNIM)	Commercial UAVs used to record propaganda footage. In 2019, Algerian security forces seized 11 UAVs alongside a large number of explosives and conventional mortars.
2018	Bolivarian Republic of Venezuela	Military defectors	Commercial UAVs carrying explosives used in the attempted assassination of President Nicolás Maduro
2018	Syrian Arab Republic	Hay’at Tahrir al-Sham	Multiple customized UAVs used in a rudimentary “swarm” in an attack on a military base.

2018	Syria	-	Two Russian military bases were attacked by a swarm of 13 homemade aerial drones.
2019	Saudi	Houthi	Drone attack in Two key Saudi Oil Installations.
2019	Saudi Arabia	Houthi	Abha Civilian airport attack. One person was killed and 21 wounded.
2019	Yemen	Houthi	Dozens of people have been killed on a military parade in the southern port city of Aden.
2019	China	Criminal Groups	UAVs reportedly used to drop contaminated pork products to fake outbreaks.
2022	Syrian Arab Republic	Hay'at Tahrir al-Sham	A single-use, fixed-wing UAV rigged with explosives flown into a church, killing two people.
2022	United Arab Emirates	Ansar Allah	Attack strikes three oil transport tankers, killing several workers and sparking a fire at Abu Dhabi's international airport.
2023	Arabian Peninsula	Al-Qaeda	Seven attacks were carried by using armed drones in the Shabwa governorate of southern Yemen. The target of the attacks were members of the Shabwa Defence Forces.
2024	Jordan	Islamic Resistance in Iraq (IRI)	On January 28 th 2024, three American soldiers were killed and 40 were injured when an explosive-laden drone was exploded on an American outpost in Jordan.

Sources: **a)** United Nations Office of Counter-Terrorism, Global Counter-Terrorism Programme on Autonomous and Remotely Operated Systems (AROS Programme). AROS PROGRAMME Autonomous and Remotely Operated Systems Global Report on the Acquisition, Weaponization and Deployment of Unmanned Aircraft Systems by Non-State Armed Groups for Terrorism-related Purposes. United Nations Office of Counter Terrorism, (2024), **b)** Thomas G. Pledger. The role of drones in future terrorist attacks. Land Warfare Paper, no. 137, (2021), **c)** News Wires. Yemen's Houthi rebels in deadly attack on Saudi airport. France24. 2019-06-24. <https://www.france24.com/en/20190623-yemens-houthi-rebels-launch-deadly-strike-saudi-airport> (Accessed 2024-07-01). **d)** Ben Hubbard, Palko Karasz and Stanley Reed. Two Major Saudi Oil Installations Hit by Drone Strike, and U.S. Blames Iran. The New York Times. 2019-09-14. <https://www.nytimes.com/2019/09/14/world/middleeast/saudi-arabia-refineries-drone-attack.html> (Accessed 2024-06-29). **e)** BBC. Yemen war: Houthi missile attack on military parade kills 32. BBC. 2019-08-01. <https://www.bbc.com/news/world-middle-east-49189241> (Accessed 2024-06-28). **f)** Rueben Dass. Al-Qaeda in the Arabian Peninsula's Drone Attacks Indicate a Strategic Shift. Lawfare media. 2023-08-20. <https://www.lawfaremedia.org/article/al-qaeda-in-the-arabian-peninsula-s-drone-attacks-indicate-a-strategic-shift> (Accessed 2024-08-01).

4.Features that make UAS attractive to non-state actors

The purpose of this chapter is to present these features that make UAS attractive to non-state actors. Over the past years, there has been a substantial increase in the use of UAS. UAS are changing how war is conducted on NATO's doorstep, 'causing destabilizing effects across regions, escalating conflicts, and putting increased killing capacity in the hands of non-state actors.'²⁶

Initially, the development of drones was to eliminate the risk of losing a pilot during reconnaissance missions. The idea was successful but in doing so, it developed and evolved in areas for which there was no intention, such as in the field of terrorism, creating negative consequences.²⁷ UAS have become the dominant tool not only in the wargame such as the Ukraine-Russia conflict which is considered the first full scale drone conflict but also in the field of terrorism.

There are certain ways that non-state actors can misuse UAS. These are the following ones:²⁸

- ✓ Biological, chemical, radiological, nuclear
- ✓ Propaganda
- ✓ Psychological
- ✓ Cyber-Attack and Electronic Warfare
- ✓ Armed Use
- ✓ Intelligence, Surveillance and Reconnaissance (ISR)
- ✓ Suicidal Drone
- ✓ Smuggle or transport material
- ✓ Disruption of air operations

²⁶ Sarah J. Lohmann. Emerging and disruptive technologies used in counterterrorism: The future of big data, drones and hypersonic weapons. In *Countering terrorism on tomorrow's battlefield: Critical infrastructure security and resiliency handbook*, 23-44. USA: Strategic Studies Institute and US Army War College Press, 2022, pp. 23-44.

²⁷ Ankit Kumar. Drone proliferation and security threats: a critical analysis. *Indian Journal of Asian Affairs*, vol. 33, no. 1/2, 2020

²⁸I Ilikjevski, Z Dimovski, K Babanoski. The weaponisation of drones - a threat from above used for terrorist purposes. *Journal of Criminal Justice and Security*, vol. 3, no. 3, 2023.

<i>Ways that terrorists can acquire UAS²⁹</i>	<i>Terrorists use of UAS is facilitated by³⁰</i>
Obtaining military-grade UAS via theft or other means	The unregulated civilian market and the ability to acquire tech in the Dark web
Purchasing a commercial UAS variant	The availability of unsecured explosives, used as payloads
Building a device from scratch (3D printers)	Easy access to explosive precursors
Converting a small plane into an inhabited system	The access to technical expertise via the internet and social media

There is no doubt that non state actors have demonstrated a preference for using cheap and easily accessible weapons and technologies. Accordingly, their interest in UAS is not a surprise.

Hence, it is of the utmost importance to demonstrate the diverse capabilities that make UAS attractive to non-state actors.

a) **Expense:** Since many countries have developed and exported drones, the technology has become more refined and more cost effective. The costs related to acquiring, maintaining, and operating unmanned aircraft systems are quite less than that of manned aircraft. Also, the costs for the training process for drone pilots are less than those for pilots of manned aircraft.³¹ It should also be acknowledged the cost effectiveness of UAS given the fact that they are multiuse, reusable, and they are cheaper than ballistic missiles and manned aircraft. Finally, it is worth noting the huge advantage for non-state actors as the expenses for deploying drones are much less than the expenses needed to combat them. As the Danish Institute for international

²⁹ Don Ressler. Remotely piloted innovation: terrorism, drones and supportive technology. Combating terrorism center. 2016-10-20. <https://ctc.westpoint.edu/remotely-piloted-innovation-terrorism-drones-and-supportive-technology/> (Accessed 2024-04-08).

³⁰ David Lewis. Preventing terrorists from using emerging technologies. Vision of Humanity. 2023-09-11. <https://www.visionofhumanity.org/preventing-terrorists-from-using-emerging-technologies/> (Accessed 2024-01-15).

³¹ John W. Rollins. Armed drones: evolution as a counterterrorism tool. Congressional Research Service. 2023-11-07. <https://crsreports.congress.gov/product/pdf/IF/IF12342> (Accessed 2024-01-22).

Studies claims “drones can cause damage and disruption hugely disproportionate to their cost”.

b) **Safety:** As the term indicates, because UAS are unmanned, automatically the risk of a killed, injured or captured pilot is considerably reduced. It is also guaranteed a high survivability prelaunch.³² UAS provide to non-state actors another concept of safety, the anonymity. Enforcement remains a challenge, as identifying and prosecuting violators can be difficult, given the anonymity that drones can provide to the operators of the drones.³³ It is important to mention here that even though the advanced technology of UAS and its features provide anonymity to their operators at the same time it can be used for propaganda videos to promote their ideology and recruit new members and supporters.

c) **Precision:** UAS can get closer to ground-based targets than pilot-controlled aircraft. Hence, this feature enables potentials for high accuracy in targeting. Furthermore, UAS can attack targets that are difficult to reach by land, giving the opportunity to non-state actors to UASs’ enabling attacks over national borders and perimeter defenses. The great chance of achieving long-range and acceptable accuracy with relatively inexpensive and increasingly available technology, make UAS even more attractive to non-state actors.³⁴

d) **Accessibility of drone technology/Commercial-off-the-shelf (COTS) drone technology:** Non-state actors can purchase civilian drones (and weaponized them) via general platforms such as Amazon, making control

³² Don Rassler. Remotely piloted innovation: terrorism, drones and supportive technology. Combating terrorism center. 2016-10-20. <https://ctc.westpoint.edu/remotely-piloted-innovation-terrorism-drones-and-supportive-technology/> (Accessed 2024-04-08).

³³ Maria-Louise Clausen. Non-state armed groups in the sky: Global regulation fails to address the security risks posed by civilian drones. Danish Institute for International Studies. 2024-04-15. <https://www.diis.dk/en/research/non-state-armed-groups-in-the-sky-global-regulation-fails-to-address-the-security-risks> (Accessed 2024-05-23).

³⁴ I Ilikjevski, Z Dimovski, K Babanoski. The weaponisation of drones - a threat from above used for terrorist purposes. Journal of Criminal Justice and Security, vol. 3, no. 3, 2023.

acquisition almost impossible.³⁵ The commercial drone industry is developing at an outstanding rate, considering the increased demand of UAS worldwide. Therefore, new technologies are emerging in electronics and artificial intelligence (AI), along with microcontrollers, processors and mobile hardware are driving the industry to new heights, creating for UAS a variety of affordable purchasing pathways. Due to the rapid popularization of drones, it has been created a market that will lead the way for technological improvements to sizes, form factors, energy storage, sensors, and the ability to utilize and integrate advanced computer capabilities. Consequently, these developments will increase the range, lifting capacity and overall capabilities of drones, making them both more lethal and more difficult to counter.³⁶

e) **Operational flexibility:** UAS offer five operational benefits that make them attractive to non-state actors. First of all, potential targets of interest to non-state actors lack barriers. However, even to the targets that are protected, a successful attack by non-state actors is feasible as UAS enables them to *attack over perimeter defenses*. Secondly, most non-state actors or other asymmetric activities are performed from close distances. The imperative for operatives to cross controlled borders and to execute their operation to a foreign country is insecure. Therefore, the UAS's ability to *attack over national borders* is inevitably attractive to non-state actors. Third, non-state actors lack the ability to perform large scale operations or cause damage to a wide area. The capability to stage *multiple simultaneous attacks* is an attractive strategy. Forth, since one of the effects of terrorist attacks is the possibility of achieving a strong psychological effect by scaring people and putting pressure to politicians, UAS *enables extended campaigns* of terrorist violence than a single terrorist attack. Finally, UAS enables *aerial attack of area targets with unconventional weapons*, a feature that could be attractive to non-

³⁵ Maria-Louise Clausen. Non-state armed groups in the sky: Global regulation fails to address the security risks posed by civilian drones. Danish Institute for International Studies. 2024-04-15. <https://www.diis.dk/en/research/non-state-armed-groups-in-the-sky-global-regulation-fails-to-address-the-security-risks> (Accessed 2024-05-23).

³⁶ Thomas G. Pledger. The role of drones in future terrorist attacks. Land Warfare Paper, no. 137, 2021.

state actors in order to achieve their objectives, especially when the preferred target is not a point target but an area.³⁷

The above features are the main reasons that make UAS quite attractive. However, there are other characteristics as well that make UAS a weapon of choice to non-state actors. First, drones can surveil targets for longer duration than manned aircraft. The invisibility feature of drones gives them the advantage of not being visible with naked eye and even the newest technological developments, cannot always detect them, giving drones the element of surprise, a feature that makes UAS even more attractive to non-state actors.

Additionally, another advantage of UAS, is that a drone can act as a force multiplier and it can help security forces with surveillance of terror camps and monitoring border security. Undeniably, non-state actors may exploit the same technology to carry out attacks.³⁸

Finally, yet importantly, regarding the difficulty in detecting and identifying drones, a significant factor that contributes to this is the small radar cross-sections (RCS). Radar systems can detect objects with a large radar cross-section such as manned aircrafts but when it comes to drones and more specifically to commercial drones, it is quite difficult to detect them as many of which have the RCS of a bird. And when a target has the RCS of a bird, it is struggling to distinguish it from an actual bird.³⁹

5. Challenges of Countering UAS

In this chapter it is demonstrated the main difficulties when it comes on countering drones.

³⁷ Brian A. Jackson et al.. Evaluating novel threats to the homeland, Unmanned aerial vehicles and cruise missiles, Santa Monica: RAND Corporation, 2008, p. 1-70.

³⁸ Ankit Kumar. Drone proliferation and security threats: a critical analysis. Indian Journal of Asian Affairs, vol. 33, no. 1/2, 2020

³⁹ Robin radar systems. Why Traditional Radar Isn't Effective at Tracking Drones. Robin radar systems. <https://www.robinradar.com/why-traditional-radar-isnt-effective-at-tracking-drones> (Accessed 2024-08-21).

Firstly, it is the defender's dilemma. As it has been mentioned in chapter four, commercial drones are reusable, therefore non-state actors can utilize the same cheap commercial drone for different purposes such as ISR, attacks etc. This multipurpose, creates an uncertainty which makes it challenging to forecast the parameters of the risk these drones can pose. Especially, do-it-yourself (DIY) drones create instability which complicates the planning of drone defenses. Due to the technological advances to the commercial sphere, non-state actors have been more flexible at weaponized drones than state actors. Consequently, national counter measures tend to fall behind to this rapid hostile adaptability.

Secondly, it is becoming increasingly difficult to distinguish drones from birds or objects with a similar physical signature, such as air- conditioning systems. NATO Members and Alliance need to stop drone attacks before they are in progress.

Furthermore, another challenge that emerges is the drone threat in an urban environment and it needs to be taken seriously. Indeed, there is an incomprehension to policy-making organs, regarding drones, which can lead 'to blown-up expectations considering both the gravity of the threat and the requirements of effective defense measures. Better analyses of how drones change, and challenge urban airspaces will help to correct these misperceptions and inform the debates on whether the drone threat justifies investments of scarce resources into measures that specifically counter drones.⁴⁰

Since drone proliferation is approached according to safety and security, governments should fund not only measures to mitigate drone expansion risks but also countering systems. Inevitably, 'drone traffic will escalate in civilian territories, demanding new operational and safety regulatory measures. Other issues that will occur are (new) environmental risks such as noise and visual pollution and band-width availability. Accordingly, drones will become both a threat to critical national infrastructure and vital national infrastructure themselves, as in logistics and transportation services. It would be a mistake to consider that drone threats are only a military concern. Commercial off the shelf use of drones in urban environments can involve risks, such as providing a view from above from spying on critical infrastructure (police stations,

⁴⁰ Ankit Kumar. Drone proliferation and security threats: a critical analysis. *Indian Journal of Asian Affairs*, vol. 33, no. 1/2, 2020

nuclear powerplants), carrying capacity (smuggling), disrupting law enforcement and last but not least weaponizing drones to inflict harm and distribute harmful materials such as radioactive sand, hazardous biological/chemical agents.

It is for safety and security reasons that it is mandatory to have unambiguous legal architecture in domestic urban spaces. ‘Homeland security and law enforcement agencies usually act as the first responders, working across both safety and security’. The regulatory and legal framework is a challenge that refers to all types of drones. There is an imperative need for regulation concerning drone operation, airspace restrictions, rules of engagement and privacy concerns, in order to guarantee responsible and accountable use of drones.⁴¹

At this point, it would be quite beneficial the presentation of three primary identified challenges when integrating drones, as they were indicated in a briefing by the Center for European Policy Analysis (CEPA).⁴²

a) Interoperability: The challenges in achieving interoperability among Alliance Members remain an issue. This issue complicates collaboration in terms of shared target information, intelligence of targets, command and control (C2) nodes. Also, by lacking opportunities to test the interoperability of multiple different systems, it is therefore slowing the role of Artificial Intelligence (AI) playing in the development of autonomous drones.

b) Capability Gap: It is true that a serious capability gap exists within NATO, especially in terms of aerial drone capabilities as well as in other domains. It is an urgent need for technological upgrades and enhancements.

c) Counter-UAS strategies: Undoubtedly, there is a need for effective countermeasures against hostile drones. As Federico Borsari has warned “Despite increased focus and resources, many NATO countries are not well-

⁴¹ M. Emimi, M. Khaleel and A. Alkrash. The current opportunities and challenges in drone technology. International Journal of Electrical Engineering and Sustainability (IJEES), vol. 1, no. 3, 2023

⁴² Miriam McNabb. CEPA experts highlight key challenges in drone warfare integration. Drone life. 24-05-13. <https://dronelife.com/2024/05/13/cepa-experts-highlight-key-challenges-in-drone-warfare-integration/> (Accessed 2024-06-25).

positioned to counter what is becoming a very vicious and purposeful threat coming from drones”.⁴³

At this point, it is crucial to indicate one more challenge of countering UAS and this is the absence of a universal definition of terrorism. In a utopian world, a commonly accepted definition of terrorism would be already existed, based on the reason that it is not a matter of who terrorize but the action of terrorism itself. Whether the actor is a civilian, an organization or a state.

Even though there has been a huge progress regarding countering terrorism and specifically combating the methods that non state actors are using for the achievement of their goals by the act of terrorism, an appropriate universal definition remains elusive because terrorism relates to the structure of each society and different bodies, organizations and government agencies have various definitions to suit their own particular role, purpose or bias.⁴⁴ Hence, there has not been given an adequate answer to the question of *what is terrorism*.

As Schmid argues, in order to create an efficient counter terrorism strategy, it is essential the existence of an agreement on the fundamental elements of the terrorism which inevitably requires a definition agreeable from all the involved bodies.⁴⁵

One of the reasons on why it is difficult to define terrorism is that, terrorism is a contested concept and political, legal, social signs and popular notions are often diverging. It is not feasible to combat terrorism effectively if every party has a different definition. That can best describe as ‘one man’s terrorist is another man’s freedom fighter’.

Terrorism is a cross-border phenomenon and organizations and countries have their own definition of terrorism. Someone could say that since NATO has an official definition of terrorism, it has no interest in a universal definition of terrorism. Nevertheless, NATO deals with threats outside its

⁴³ Ibid

⁴⁴ Bakker, E. (2021) Terrorism and Counterterrorism: Comparing Theory and Practice [online course]. Universiteit Leiden. <https://www.coursera.org/learn/terrorism>

⁴⁵ Marsili, M. (2023). Morals and Ethics in Counterterrorism. *Conatus - Journal of Philosophy*, [online] 8(2), pp.373–398. doi:<https://doi.org/10.12681/cjp.34495>.

Alliances, therefore, a universal definition of terrorism needs to be established, in order for NATO to be able to deal effectively with terrorist threats worldwide.

NATO needs to place importance on a universal definition of terrorism for the following reasons:

a) In order to develop a powerful and efficacious international defensive strategy, as it is mandatory the existence of an agreement of what it is that we are dealing with.

b) Without a universally accepted definition of terrorism, it is unfeasible to develop international agreements against terrorism.

c) “Although many countries have signed bilateral and multilateral agreements concerning a variety of crimes, extradition for political offences is often explicitly excluded, and the background of terrorism is always political.”⁴⁶

d) It will create adequate conditions for the legislation against those involved in or supporting terrorism. International conventions and laws will be created for the discipline of terrorists, terrorist organizations, states sponsoring terrorism and economic firms trading with them.

e) “The operational use of the definition of terrorism could motivate terrorist organizations, due to moral and utilitarian considerations, to shift from terrorist activities to alternate courses (such as guerrilla warfare) in order to attain their aims, thus reducing the scope of international terrorism.”⁴⁷

6. Techniques and strategies that can diminish the impact of non-state actors use of UAS

Future warfare will heavily rely on AI, robotics, and drones to reduce human loss and costs while optimizing battlefield strategies and intelligence. Therefore, the aim of this chapter is to outline techniques and strategies that could be beneficial for diminishing the impact of non-state actors use of UAS. There are many techniques, passive or active that can be used to counter UAS.

⁴⁶ Schmid, A. (n.d.). Terrorism - The Definitional Problem. *Case Western Reserve Journal of International Law*, 36(2).

⁴⁷ Schmid, A. (n.d.). Terrorism - The Definitional Problem. *Case Western Reserve Journal of International Law*, 36(2).

For this paper, it is going to be demonstrated the most effective ones and the most recent developments.

6.a. Drone Forensics: Because of the emergence of illicit activities, the demand for forensic analysis of the captured drones is urgent. Drone forensics can provide a great deal of information about the potential suspect of a crime according to the gathered data from on-board sensors and other electronics that assist with flight and navigation, as well as the camera and digital storage and of course this will help to prevent further crime.⁴⁸

By the term drone forensics, it is described the forensic processing and forensic analysis of UAVs. Drone forensics can be carried out whether the UAVs are in whole and intact or have been crashed and damaged and only some parts are available. Drone forensics involves the recovery in a forensically sound way of any data stored within the drone itself or held on any removable media which the drone has used. Analysis of data found on a drone will potentially be related to flights, locations, altitudes, times, dates and videos or images that the drone has captured.⁴⁹

There are many ways that a forensic analysis of a drone can be achieved. Open-Source Intelligence (OSINT) and Radio Frequency Sensors are some of them.

6a.a. OSINT: OSINT tools have substantially advanced over the years. Initially focused on traditional media analysis, OSINT tools have shifted towards the vast information resources available on the internet, in both private and public sectors. Indicative of this development is the prediction that the global open-source intelligence market will rise to \$29 billion by 2026.⁵⁰

The future of OSINT tools is expected to be driven by artificial intelligence and machine learning, offering enhanced precision and speed in data

⁴⁸ A. Hannan Azhar, T. E. Allen Barton, T. Islam. Drone Forensic Analysis Using Open Source Tools. *Journal of Digital Forensics, Security and Law*, vol. 13, no. 1, 2018

⁴⁹ qccglobal. Drone Forensics Services. qccglobal. 2024-02-08. <https://qccglobal.com/drone-forensics-services/> (Accessed 2024-07-02).

⁵⁰ Esteban Borges. Top 15 OSINT tools for expert intelligence gathering. *Recorded future*. 2024-04-29. <https://www.recordedfuture.com/threat-intelligence-101/tools-and-technologies/osint-tools> (Accessed 2024-06-26).

processing and analysis. “The integration of big data analytics with AI and machine learning enhances the accuracy and efficiency of intelligence analysis, supporting the generation of actionable intelligence.”⁵¹

There are many advantages that the advanced OSINT analytics tools can provide. Firstly, automated processes reduce the chances of human error and improve efficiency and speed for data processing. Secondly, the reported data can be easily converted into clear and concise visual presentations, enabling faster identification of emerging threats and real time monitoring.

Concerning how OSINT tools can diminish the threat of UAS, there are courses that can provide knowledge certified expertise in the field of drone open-source intelligence investigations that are available to military, law enforcement and government. These courses focusing on tools and techniques available to identify, analyze and geolocate drones and their owners. Moreover, drone users are quite likely to have online digital footprints, which can lead to more OSINT capabilities in investigations. Other capabilities that can be unlocked via OSINT tools are: assessing cyber and physical security vulnerabilities in UAS/ C-UAS systems, and a quick response to a drone incident. Also, there are tools like Maltego and Shodan that can gather information about drone model, firmware versions and potential vulnerabilities.

6a.b. Radio Frequency (RF) Analysis: Another way to detect drones is by using RF sensors. RF sensors are passively listening to the Radio Frequency spectrums in which drones communicate with their controller. The 2.4 GHz and 5.8 GHz frequency bands are the most widely used for communication and are utilized by many drones on the market, including those from DJI. An RF sensor passively monitors these frequency bands for signals. When it detects a communication protocol, it compares it to a database of known protocols to identify signals coming from a drone and its controller.⁵²

There are two types of RF sensors that can detect drones by passively monitoring RF communication protocols. The first type decodes the protocol to access all transmitted data, allowing it to provide precise information like GPS

⁵¹ Ibid

⁵² Airsight. Detect Drones using Radio Frequency (RF) Sensors. Airsight. <https://www.airsight.com/en-us/knowledge-hub/drone-detection/rf> (Accessed 2024-07-12).

coordinates, altitude, and speed. Consequently, this type of RF sensor can provide comprehensive details, such as the GPS location of both the drone and the pilot, the drone's make and model, its altitude, speed, real-time tracking, and a unique identifier for the drone.

The second type of RF sensor recognizes the communication protocol's pattern. It relies on an extensive database, typically created through testing, that includes RF signatures of various drone makes and models. This sensor's main advantage is its ability to identify any drone brand or model, as long as it's listed in the database, making it versatile and not limited to a single brand. Accordingly, the second type of RF sensor can provide the following information: drone make and model, directional detection (angle and distance from sensor), real time directional tracking (angle and distance update as drone is flying in real time) and unique MAC address for Wi-Fi drones.⁵³

Concerning this field of RF, the United Kingdom revealed that on May 2024 started the development of a Radio Frequency Directed Energy Weapon (RFDEW) capable of neutralizing drone swarms at just 10 pence (13 cents) a shot.⁵⁴ According to the UK Ministry of Defense statement, RFDEW 'beams radio waves to disrupt or damage the critical electronic components of enemy vehicles causing them to stop in their tracks or fall out of the sky'.⁵⁵ Moreover, it is also indicated that the RFDEW 'is a significant cost-effective alternative to traditional missile-based, air defense systems, capable of downing dangerous drone swarms with instant effect'. Last but not least, the high level of automation allows the system to be operated by a single person.

⁵³ Ibid

⁵⁴ Tim Martin. <https://breakingdefense.com> Uk reveals development of low-cost radio frequency directed energy weapon. Breaking Defense. 2024-05-16. <https://breakingdefense.com/2024/05/uk-reveals-development-of-low-cost-radio-frequency-directed-energy-weapon/> (Accessed 2024-06-10).

⁵⁵ Ministry of Defence, Defence Science and Technology Laboratory, James Cartlidge. Cutting-edge drone killer radio wave weapon developing at pace. Gov.uk. 2024-05-16. <https://www.gov.uk/government/news/cutting-edge-drone-killer-radio-wave-weapon-developing-at-pace> (Accessed 2024-06-20).



Figure 4: UK's Radio Frequency Directed Energy Weapon (RFDEW)

6c. Laser

There are two categories considering countering-UAS system (CUS): ground based and sky-based lasers. In the field of ground-based are the most publications regarding countering UAS. LADAR (laser detection and ranging), which is based on laser, with a peak power of 700kW, which allows for the increase of the operating range up to 2 km.⁵⁶

Generally, lasers can be categorized into low-power and high-power lasers. The low-power lasers can be used to neutralize some sensitive sensors of the drone (ex: electron-optical sensors) and the high-power lasers can be a real weapon, able to burn part of the drone and destroy it.⁵⁷

Regarding latest activities in the field of laser (for the time of writing this study), US Army on April 2024 has deployed high-energy lasers overseas to blast incoming enemy drones out of the sky. The Palletized High Energy Laser (P-HEL), developed by BlueHalo in support of the U.S Army Rapid Capabilities and Critical Technologies Office (RCCTO), is a 20-kilowatt which supports US Army's mission.⁵⁸ According to the BlueHalo's press release, the foundation of P-HEL, LOCUST Laser Weapon System (LWS) combines precision optical and

⁵⁶V.U. Castillo, A. Manco, D. Pascarella, G. Girante. A review of counter-UAS technologies for cooperative defensive teams of drones. *Drones*, vol. 6, no. 65, 2022

⁵⁷ Ibid

⁵⁸ Jared Keller. The Army Has Officially Deployed Laser Weapons Overseas to Combat Enemy Drones. *Military.com*. 24-04-24. <https://www.military.com/daily-news/2024/04/24/army-has-officially-deployed-laser-weapons-overseas-combat-enemy-drones.html> (Accessed 2024-06-15).

laser hardware with advanced software, artificial intelligence (AI), and processing to enable and enhance the directed energy “kill chain”. LOCUST LWS addresses the inherent need for mobility and quick deployment-tracking, identifying, and engaging of a wide variety of targets with its hard-kill energy laser.⁵⁹



Figure 5: US Army's Palletized High Energy Laser (P-HEL)

Also, according to an article of CNN, South Korea has started the production of the Block-I, a low-cost laser weapon that has successfully shot down small drones during testing.⁶⁰ This laser weapon can accurately target drones and multicopters at short distances. It is said that each hit would cost about 1.50 dollars. As reported by the Defense Acquisition Program Administration (DAPA) the unit measures 9 meters by 3 meters by 3 meters, and fires laser rays that are difficult if not impossible to detect before impact. It is undetectable and soundless, needs no additional ammunition, and operates solely when connected to an electrical power source.⁶¹

⁵⁹ BlueHalo. BlueHalo to Provide U.S. Army with Full-Cycle Support for High Energy Laser Systems. BlueHalo. 2024-04-08. <https://bluehalo.com/bluehalo-to-provide-u-s-army-with-full-cycle-support-for-high-energy-laser-systems/> (Accessed 2024-06-24).

⁶⁰ Y. Seo, B. Lendon. South Korea to mass produce lasers that can take out drones at \$1.50 a hit. CNN. 2024-07-11. <https://edition.cnn.com/2024/07/11/asia/south-korea-antidrone-lasers-intl-hnk-ml/index.html> (Accessed 2024-07-18).

⁶¹ Ibid



Figure 6: The Block-I laser system from South Korea's Defense Acquisition Program Administration

6d. Urban Air Traffic Management (UATM)

Urban Air Traffic Management is the collection of systems and services to support the consolidation of all Urban Air Mobility (UAM) operations including Regulations, Organizations, Airspace Structures and Procedures, Technologies and the Environment.⁶² UATM services will guarantee that the safety, flight efficiency, capacity, access and equity along with flexibility and predictability of the UAM environment are assured and maximized.⁶³ The purpose of UATM is to support UAM operations and optimize the performance of UAM and low-level airspace.

⁶²Airspace World. The Urban Air Traffic Management Concept. Airspace World. <https://airspaceworld.com/news/the-urban-air-traffic-management-concept/> (Accessed 2024-08-24).

⁶³Airservices Australia and Embraer Business Innovation Center. URBAN AIR TRAFFIC MANAGEMENT CONCEPT OF OPERATIONS. URBAN AIR TRAFFIC MANAGEMENT CONCEPT OF OPERATIONS, vol. 1, 2020

7. Future Threats

Unmanned Aircraft Systems have been a weapon of choice both for state and non-state actors. Nowadays technology, whilst it has been remarkable and rapidly progressing, is creating the tactics and techniques of future terrorist attacks and contemporary terrorist threats. Advances in range, payload, information transmission, drone-swarms, and precision-strike coerce a reframe of ‘asymmetric warfare’.⁶⁴ What is worrisome is not simply the use of technologies in isolation, but the combination of these technologies coupled in real-time with an actual kinetic attack that could prove overwhelming for law enforcement, intelligence services and security forces.⁶⁵

This chapter explores potential future threats identified in the literature review. It is outlined into the following sections: Artificial Intelligence (AI), Commercial off-the shelf (COTS), Additive Manufacturing (3D printers), drone swarms and different types of UAS, UAS used as Improvised Explosive Devices (IEDs).

7a. Artificial Intelligence (AI)

It may seem that Artificial Intelligence (AI) is a subject area that concerns society only in the latest years, but this is not true. There are many reports from the 70s and 80s that demonstrate not only what artificial intelligence is but also how it could be beneficial for the Army. Irrefutable proof is a report of the Army Science Board in 1982 about artificial intelligence and robotics. Even since then, army realized the importance of AI and how it could assist military operations and make them feasible due to the absence of human risk. It is also indicated the importance of remote control by human operators regarding robots, something that we are already witnessing nowadays with UAS.⁶⁶

⁶⁴ J. Rogers, D. Kunertova. The vulnerabilities of the drone age: established threats and emerging issues out to 2035. Centre for war studies, 2022

⁶⁵ Intel Brief. Terrorists' use of drones and other emerging technologies. The cipher brief. 18-10-03. https://www.thecipherbrief.com/column_article/terrorists-use-of-drones-and-other-emerging-technologies (Accessed 2024-02-27).

⁶⁶ I C. Peden, J V. Braddock, W Brown. Artificial Intelligence and Robotics. Army Science Board, Office Assistant Secretary of the Army, 1982

As technology evolves and proliferates, so does AI. The more drones are developed and exported, the more sophisticated and less expensive the technology becomes. Advances in AI have caused an additional headache to NATO and Alliance, considering that it is easily affordable and accessible, low cost, commercial off-the-shelf AI, therefore non-state actors can easily acquire AI technology. Non-state actors can use AI not only for cyberattacks but also to deploy AI-empowered drones, giving them asymmetric advantages over states. In addition to this, AI is mostly developed in the private sector and universities, hence it could quickly increase among non-state actors.

This raises the question of what specific dangers might emerge from combining AI technology with UAS.

AI can be used to automate specific tasks such as drone strikes and sniping, targeting both minority and high-value individuals. Higher levels of autonomy will advance functionality of drones, hence will enable greater precision of observation and strikes. Non-state actors will stage attacks regardless of geography and borders and it will be easier for them to obtain classified information about opposing forces through AI-supported hacking operations.⁶⁷ Secondly, AI can be applied to maximize the impact of cyberattacks, in order to 'hit' vulnerable individuals financially and psychologically. Third, AI can be utilized in order to manipulate public opinion by employing algorithms to generate deepfakes or synthetic text.⁶⁸

Last but not least, a forthcoming threat of AI is the feature of surveillance and facial recognition technology. "Drones with facial recognition technology will end anonymity, everywhere", giving the "advantage" of recognizing people at a distance and crowds.⁶⁹ On the contrary, the combination of UAS and AI technology could prove a formidable threat in the hands of non-state actors. One only needs to consider what will happen if non-state actors utilize off-the-shelf drones and AI technology via black markets. This combination will allow non-state groups to develop lethal autonomous weapons which will increase their capacity to automate killing on a massive scale. These autonomous

⁶⁷ Aleksander Olech. Unmanned Aerial Vehicle- a Lethal Weapon of Tomorrow for Terrorists. *Nowa Polityka Wschodnia*, vol. 1, no. 32, 2022

⁶⁸ Ibid

⁶⁹ Charles J. Dunlap. The Hyper-Personalization of War, Cyber, Big Data and the Changing Face of Conflict. *Georgetown Journal of International Affairs*, 2014

weapons or ‘killer robots’ with the AI technology, “will decide who lives and who dies”.⁷⁰

Advances in artificial intelligence and global technology proliferation are creating economic, social and military disruption.

7b. Commercial off-the-shelf (COTS)

The proliferation of UAS is inevitable, considering the global interest in drone acquisition. Admittedly, both state and non-state actors can obtain and operate commercial off-the-shelf UAS and drone technology.

The danger that arises due to this global interest is the fact that the global markets of UAS remains unregulated.⁷¹ Undeniably, commercial drone technologies are attractive to non-state groups because of the features that were mentioned in chapter four. However, it is the way that non-state actors utilize drones. It is the tactical, technical and operational proficiency that threatens NATO’s and Alliance’s security.⁷² Commercial off-the-shelf drone technology is not a new feature. What makes it though a future threat are the constant technological advances along with the aspect that non-state actors demonstrate impressive innovation in their tactics and means of attack. Non-state actors after successfully employed drones, acquired more and better drones. They have also dedicated their attention to observe and learn from their counterparts. Thereby, they have displayed ‘a capability to adapt to changes in defensive postures and responded through new technical and tactical actions’.⁷³

⁷⁰ Jacob Ware. Terrorist groups, artificial intelligence and killer drones. War on the rocks. 2019-09-24. <https://warontherocks.com/2019/09/terrorist-groups-artificial-intelligence-and-killer-drones/> (Accessed 2024-05-28).

⁷¹ Ankit Kumar. Drone proliferation and security threats: a critical analysis. Indian Journal of Asian Affairs, vol. 33, no. 1/2, 2020

⁷² E. Archambault and Y. Veilleux-Lepage. Tower 22: Innovations in Drone Attacks by Non-State Actors. International Centre for Counter-Terrorism. 24-02-01. <https://www.icct.nl/publication/tower-22-innovations-drone-attacks-non-state-actors> (Accessed 2024-08-24).

⁷³ Ibid

Off-the-shelf drone technology and UAS can become a more serious threat for national security. Imagine a non-state actor who purchased an off-the-shelf drone and has access to the internet. Nowadays the internet is like an open school. You can learn and develop skills. Hence, the internet provides a variety of 'do-it-yourself' videos for mastering drones and an array of commercial-off-the-shelf technologies.⁷⁴ And the malleability of civilian drones along with the advantages that the internet provides, allowing non-state actors various, multiple and creative uses of drones.⁷⁵

Another feature that makes commercial drones an upcoming threat is the difficulty of differentiating them from military drones. The purchasing platforms for civilian drones are various, where the control acquisition is nearly unfeasible and quite difficult to track drone components.⁷⁶

7c. Additive Manufacturing (3D printers)

Additive Manufacturing (AM), more well-known as 3D printing, offers a big advantage to non-state actors, as they can sidestep law enforcement. By using 3D printers, non-state actors reduce their identifiable actions during the acquisition phase and of course, they reduce the cost of production for various types of weapons or essential elements used to carry out attacks.

The ongoing development of consumer AM services along with the technological advances, provide more sophisticated equipment and capabilities than commercial off-the-shelf printers, giving the opportunity to non-state actors to print components for use in the creation of weapons while minimizing their logistical footprints.⁷⁷

⁷⁴ Intel Brief. Terrorists' use of drones and other emerging technologies. The cipher brief. 18-10-03. https://www.thecipherbrief.com/column_article/terrorists-use-of-drones-and-other-emerging-technologies (Accessed 2024-02-27).

⁷⁵ K. Chavez, O. Swed. Off the Shelf: The Violent Nonstate Actor Drone Threat. Air & Space Power Journal, 2020

⁷⁶ Maria-Louise Clausen. Non-state armed groups in the sky: Global regulation fails to address the security risks posed by civilian drones. Danish Institute for International Studies. 2024-04-15. <https://www.diis.dk/en/research/non-state-armed-groups-in-the-sky-global-regulation-fails-to-address-the-security-risks> (Accessed 2024-05-23).

⁷⁷ Homeland Security. Addressing risks from non-state actors' use of commercially available technologies. Public-Private Analytic Exchange Program, 2023

Especially, when 3D printers are combined with open-source communities, 3D printable parts can be designed by individuals and quickly and easily distributed for production.⁷⁸



Figure 7: "Kamikaze" drone built by Mohamad Al Bared, using a 3D printer⁷⁹

7d. Other types of drones and drone swarms

Regarding future threats of drones, another concerning development could be considered the new types of drones, such as unmanned underwater drones (UUVs).

UUVs are not completely considered a new type of drones, however UUVs have revolutionized sea operations. An irrefutable proof of the continual interests to the UUVs is reports that suggested that China back to 2010 tested

⁷⁸ Larry Friese. Emerging Unmanned Threats: the use of commercially available UAVs by armed non-state actors. Armament Research Services, vol. 2, 2016

⁷⁹ Jessica Murray and agencies. Birmingham PhD student guilty of using 3D printer to build 'kamikaze' drone. The Guardian. 2023-09-28. <https://www.theguardian.com/uk-news/2023/sep/28/birmingham-phd-student-mohamad-al-bared-guilty-using-3d-printer-to-build-kamikaze-drone> (Accessed 2024-08-24).

a torpedo-armed underwater drone able to detect, track and attack enemy submarines. The warning feature of this, is the use of artificial intelligence (AI) for better results in reconnaissance and track submerged targets than human sonar operators.⁸⁰

Some of the advantages of UUVs are the following ones. They can perform many tasks compared to manned underwater vehicles (MUVs). Equivalent to the advantages of UAVs, UUVs also provide the advantage of safety and long duration, as they can operate very deep in the oceans, without risking the crew. Moreover, the initial and maintenance cost of UUVs is considerably lower in contrast with MUVs.

At the time of writing, future features of UUVs that can make them a significant threat, could be higher positioning accuracy, transferring real-time underwater data, ability to communicate with nearby UUVs creating a network similar to swarms and the ability to operate underwater and overwater. Some of the challenges regarding malicious UUVs could be the threat of unauthorized surveillance, smuggling and the threat of undersea infrastructure.⁸¹ A recent example that show the emergence of UUVs is the Houthis's use of UUVs in the Red Sea. Houthis's drones although are not as sophisticated as the military submarines, they constitute a major problem to naval defence strategies and tactics that have being employed in the Red Sea.⁸²

Another evolving threat of drones is drone swarming. Drone swarming utilizes large numbers of coordinated aircraft, making decisions as a unit based on shared information.⁸³

⁸⁰ Thomas Newdick. China Tested An AI-Controlled Submarine-Hunting Underwater Drone A Decade Ago: Report. The warzone. 2021-07-09. <https://www.twz.com/41478/china-tested-an-ai-controlled-submarine-hunting-underwater-drone-a-decade-ago-report> (Accessed 2024-06-04).

⁸¹ W. Khawaja et al. Threats from and Countermeasures for Unmanned Aerial and Underwater Vehicles. *Sensors*, vol. 22, no. 3896, 2022

⁸²Amila Prasanga. Escalation Beneath the Waves: The Looming Threat of Houthi UUVs in the Red Sea. CIMSEC. 2024-05-08. <https://cimsec.org/escalation-beneath-the-waves-the-looming-threat-of-houthi-uuv-in-the-red-sea/> (Accessed 2024-08-16).

⁸³ Susan Becker. Drone swarms: scaling up for a new level of efficiency. *elsight*. 2022-08-22. <https://www.elsight.com/blog/drone-swarms-scaling-up-for-a-new-level-of-efficiency/> (Accessed 2024-02-18).



Source: Andy Dean/stock.adobe.com.

Figure 8: Drone Swarms

Drone swarms became mostly known to the public through light shows such as the performing by Intel at the Opening Ceremony of the Tokyo Olympic Games and since then, there are numerous drone light shows such as the Lantern Festival 2024 by High Great in Longgang.⁸⁴

The advantages of drone swarms are the decrease of operators, time and labor. Drone swarming along with beyond visual line of sight (BVLOS) and autonomy, could be another pillar that unlocks enhanced efficiency for the drone industry and boosts economic potential.⁸⁵

In terms of the challenges of drone swarms, undoubtedly it is highly complex, and full autonomy requires extremely advanced levels of artificial intelligence (AI), computer vision and sensor fusion to accomplish as well as sophisticated algorithms.

⁸⁴ Shayan Hassan. Presenting a Drone Lighting Show to the People at the Delightful Lantern Festival. Vents Magazine. 2024-05-25. <https://ventsmagazine.uk/2024/05/25/presenting-a-drone-lighting-show-to-the-people-at-the-delightful-lantern-festival/> (Accessed 2024-06-14).

⁸⁵ Susan Becker. Drone swarms: scaling up for a new level of efficiency. elsight. 2022-08-22. <https://www.elsight.com/blog/drone-swarms-scaling-up-for-a-new-level-of-efficiency/> (Accessed 2024-02-18).

Drone swarms in the hands of non-state actors could overwhelm defensive capabilities. Especially, drone swarms could be a significant threat with the feature of Bluetooth networks. The Bluetooth networks are low-power, local networks that self-organize and share information in real-time.⁸⁶ Drone swarm technology is going to proliferate globally, potentially even faster than some high-end exquisite weapons and platforms.⁸⁷

7e. UAS used for Improvised Explosive Devices (IEDs)

Another way that UAS can be misused by terrorists is to be used either as Improvised Explosive Devices (IEDs) or to carry over IEDs.

The accelerated development of the technology along with the continuous development of UAS, have converted UAS into improvised explosive devices (IEDs), making them a weapon of choice for non-state actors, leading the way to a new type of asymmetric threat.⁸⁸

It is known that in terms of technical trends, terrorists are using UAS as IEDs or as a mean of transfer IEDs. They are using weaponized UAS in order to achieve their goals. Evidence of this can be found in the Syria/Iraq conflict zone.

Also, taking into account the purchases of materials that could be used in the production of IEDs, it is indicating a big red flag to NATO and Alliance.

⁸⁶ Thomas G. Pledger. The role of drones in future terrorist attacks. Land Warfare Paper, no. 137, 2021.

⁸⁷ Zachary Kallenborn. Swarm clouds on the Horizon? Exploring the Future of Drone Swarm Proliferation. Modern War Institute at West Point. 2024-03-20. <https://mwi.westpoint.edu/swarm-clouds-on-the-horizon-exploring-the-future-of-drone-swarm-proliferation/> (Accessed 2024-06-14).

⁸⁸ I Ilikjevski, Z Dimovski, K Babanoski. The weaponisation of drones - a threat from above used for terrorist purposes. Journal of Criminal Justice and Security, vol. 3, no. 3, 2023.



Figure 9: Explosive mounted drone by the PKK/KCK terrorist organization⁸⁹

It has been revealed in a past study that Da'esh forces have teams on technicians and engineers that modify commercial UAS to drop IEDs. There is also evidence that indicates that the same group has weaponized commercial UAS.⁹⁰

⁸⁹ Centre of Excellence Defence against Terrorism. Terrorist Use of Unmanned Aerial Vehicles: Turkey's Example. Defence against terrorism review, vol. 13, 2020

⁹⁰ United Nations Office of Counter-Terrorism, Global Counter-Terrorism Programme on Autonomous and Remotely Operated Systems (AROS Programme). AROS PROGRAMME Autonomous and Remotely Operated Systems Global Report on the Acquisition, Weaponization and Deployment of Unmanned Aircraft Systems by Non-State Armed Groups for Terrorism-related Purposes. United Nations Office of Counter Terrorism, 2024

8. Conclusion and Recommendations

Terrorism poses a significant challenge to NATO's security framework, and it will exist indefinitely because there will always be individuals and groups that get reassurance and motivation from this type of self-justification. Hence, it is crucial to be well-informed on the challenges that new technological developments pose to the security of the Alliances and worldwide.

The availability and approachability of drone technology is posing a great threat to global security, escalating the asymmetric threat. The evolution of UAS is leading the way to the 'dehumanization' of warfare, and drones have become a weapon of choice not only for state actors but also for terrorists. Even though, the development of drones was initially to forestall the risk of losing a pilot, non-state actors took the advantage of UAS and misused UAS in order to accomplish their objectives. These actors—once limited by access to advanced military technologies—now exploit commercially available drones to disrupt, coerce, and inflict damage across borders with minimal cost and high impact. For NATO and its allies, the weaponization of drones by non-state actors is a serious and evolving challenge, one that threatens not only military assets but also civilian infrastructures and public safety on a global scale.

Through this study, it has been identified specific ways in which drones are being misused- from serving as improvised explosive devices to conducting intelligence, surveillance and reconnaissance (ISR) operations. On the other hand, it has been also examined the core features that make UAS a go-to weapon, including low acquisition costs, anonymity, safety, precision and operational flexibility. Undeniably, non-state actors prefer the civilian/commercial off the shelf UAS because they are cheap, user-friendly and largely unregulated, making them quite easy for terrorists to purchase them and make them a weapon of choice. Proof of this rapid development is the prediction that the Global Drone Market growth will reach above USD 160 billion by 2031.⁹¹

In terms of counter terrorism measures in the field of UAS, it has been successful concerning the fighting of terrorism regarding the tactics and

⁹¹ The global security market. Global market for UAVs predicted to reach \$163 billion by 2030. securityworldmarket.com. 2024-05-16. <https://www.securityworldmarket.com/int/News/Business-News/global-market-for-uavs-predicted-to-reach-163-billion-by-2030> (Accessed 2024-05-17).

methods used by non-state actors. Nevertheless, it still needs to improve its strategies about preventing terrorism as an instrument for several groups to achieve certain goals by spreading fear and anxiety through violent acts. This implies that measures in countering drones should concentrate mainly on capturing the human operator and diminishing the commercial off the shelf base and secondly focus on stopping the drones. As it has been stated, ‘the good guys need to be on guard always, the bad ones need only to succeed once’.⁹²

Indicative of this concerning risk of misused drones by terrorists, is the introduction of a bill by the Senators Mitt Romney and Jacky Rosen of the Combating Foreign Terrorist Drones Act of 2024 on 11th of June 2024. Its objective is to prevent foreign terrorists from obtaining UAS, conduct attacks, deliver weapons and collect intelligence. Therefore, the Secretary of Defense shall submit to the congressional defense committees an intelligence assessment which includes: methods that foreign terrorist organizations use to obtain drones, identifications of suppliers, networks and other main points to facilitate the acquisitions of drones by non-state actors, evaluation of the cooperation and intelligence sharing with U.S allies and patterns in preventing terrorists from obtaining drones as well as suggestions for legislative or administrative action in order to combat terrorist organizations from acquiring drones.⁹³

Additionally, OSINT will have a crucial role in the near future as a practice in combating terrorists’ drones. Drone forensics by using OSINT tools can be very beneficial as it can provide information such as geolocation of the human operators. Geolocating the human operators is a feature that is absent in nowadays countering measures of UAS and there is an increasing demand for concentrate more to the human operator than the drone itself.

The inevitable truth of the new age of drones is the fact that the drones will always get through. Developments in technology provide to non-state actors advances that makes their detection particularly difficult. Artificial

⁹² J. Rogers, D. Kunertova. The vulnerabilities of the drone age: established threats and emerging issues out to 2035. Centre for war studies, 2022

⁹³ Congress.gov. S.4515 - Combating Foreign Terrorist Drones Act of 2024. Congress.gov. 202-06-11. <https://www.congress.gov/bill/118th-congress/senate-bill/4515/text> (Accessed 2024-08-24).

Intelligence is by far more dangerous as it is a technology that provides more sophisticated features to non-state actors, therefore making them almost impossible to tackle them. The most worrisome feature of AI in drone technology is the facial recognition which will end anonymity as every individual and especially high-value one could be considered a potential target for non-state actors. In the foreseeable future, the main tool on the battlefield would be UAS controlled by Artificial Intelligence. Subsequently, a scenario of lethal autonomous weapons powered by AI in the hands of malicious actors, is not far away from us.

Drone's technology developments have allowed infiltrating terrorists to achieve their goals much easier. Although NATO and its members have successfully introduced countering measures of misused UAS, non-state actors have proved to be resourceful and one step ahead in exploiting each and every technological advance. In the future warfare, it will be hard to distinguish a state drone strike from a terrorist drone strike. Therefore, it is of crucial need to emphasize in non-state actors' detection even before they start assembling a new "weapon", ideally during the planning procedure.

While no solution is perfect, a robust, multi-layered response offers the best path forward. Through a combination of regulatory oversight, advanced countermeasures, and international collaboration, NATO and its allies can address the security challenges posed by UAS. By continuously evolving our understanding and response to these threats, we can prepare for an increasingly complex and asymmetric battlefield, preserving peace and security in an era where unmanned technologies have reshaped the contours of warfare.

Bibliography

-A. Hannan Azhar, T. E. Allen Barton, T. Islam. Drone Forensic Analysis Using Open Source Tools. *Journal of Digital Forensics, Security and Law*, vol. 13, no. 1, 2018

-Airservices Australia and Embraer Business Innovation Center. URBAN AIR TRAFFIC MANAGEMENT CONCEPT OF OPERATIONS. *URBAN AIR TRAFFIC MANAGEMENT CONCEPT OF OPERATIONS*, vol. 1, 2020

-Airsight. Detect Drones using Radio Frequency (RF) Sensors. Airsight. <https://www.airsight.com/en-us/knowledge-hub/drone-detection/rf> (Accessed 2024-07-12).

-Airspace World. The Urban Air Traffic Management Concept. *Airspace World*. <https://airspaceworld.com/news/the-urban-air-traffic-management-concept/> (Accessed 2024-08-24).

-Aleksander Olech. Unmanned Aerial Vehicle- a Lethal Weapon of Tomorrow for Terrorists. *Nowa Polityka Wschodnia*, vol. 1, no. 32, 2022

-Amila Prasanga. Escalation Beneath the Waves: The Looming Threat of Houthi UUVs in the Red Sea. *CIMSEC*. 2024-05-08. <https://cimsec.org/escalation-beneath-the-waves-the-looming-threat-of-houthi-uuv-in-the-red-sea/> (Accessed 2024-08-16).

-Ankit Kumar. Drone proliferation and security threats: a critical analysis. *Indian Journal of Asian Affairs*, vol. 33, no. 1/2, 2020

- BBC. Yemen war: Houthi missile attack on military parade kills 32. *BBC*. 2019-08-01. <https://www.bbc.com/news/world-middle-east-49189241> (Accessed 2024-06-28).

- Bakker, E. (2021) *Terrorism and Counterterrorism: Comparing Theory and Practice* [online course]. Universiteit Leiden. <https://www.coursera.org/learn/terrorism>

- Ben Hubbard, Palko Karasz and Stanley Reed. Two Major Saudi Oil Installations Hit by Drone Strike, and U.S. Blames Iran. The New York Times. 2019-09-14. <https://www.nytimes.com/2019/09/14/world/middleeast/saudi-arabia-refineries-drone-attack.html> (Accessed 2024-06-29).
- BlueHalo. BlueHalo to Provide U.S. Army with Full-Cycle Support for High Energy Laser Systems. BlueHalo. 2024-04-08. <https://bluehalo.com/bluehalo-to-provide-u-s-army-with-full-cycle-support-for-high-energy-laser-systems/> (Accessed 2024-06-24).
- Brian A. Jackson et al. Evaluating novel threats to the homeland, Unmanned aerial vehicles and cruise missiles, Santa Monica: RAND Corporation, 2008, p. 1-70.
- Centre of Excellence Defence against Terrorism. Terrorist Use of Unmanned Aerial Vehicles: Turkey’s Example. Defence against terrorism review, vol. 13, 2020
- Christina Schori Liang. Building Resilience Against Terrorist Attacks Involving Uncrewed Aerial Systems. Geneva Centre for Security Policy, no. 5, 2023
- Congress.gov. S.4515 - Combating Foreign Terrorist Drones Act of 2024. congress.gov. 2024-06-11. <https://www.congress.gov/bill/118th-congress/senate-bill/4515/text> (Accessed 2024-08-29).
- Critical infrastructure security and resiliency handbook, 23-44. USA: Strategic Studies Institute and US Army War College Press, 2022, pp. 23-44.
- Charles J. Dunlap. The Hyper-Personalization of War, Cyber, Big Data and the Changing Face of Conflict. Georgetown Journal of International Affairs, 2014
- Dave O’Malley, ‘The mother of all drones’, Vintage Wings of Canada <https://www.vintagewings.ca/stories/mother-of-all-drones>
- David Lewis. Preventing terrorists from using emerging technologies. Vision of Humanity. 2023-09-11. <https://www.visionofhumanity.org/preventing-terrorists-from-using-emerging-technologies/> (Accessed 2024-01-15).
- David Axe. In The Hottest Sector of The Ukraine War, The Ukrainians Might Deploy As Many Drones As The Russians Deploy Soldiers. Forbes. 24-03-10.

<https://www.forbes.com/sites/davidaxe/2024/03/10/in-the-hottest-sector-of-the-ukraine-war-the-ukrainians-might-deploy-as-many-drones-as-the-russians-deploy-soldiers/> (Accessed 2024-06-20).

-Don Ressler. Remotely piloted innovation: terrorism, drones and supportive technology. Combating terrorism center. 2016-10-20. <https://ctc.westpoint.edu/remotely-piloted-innovation-terrorism-drones-and-supportive-technology/> (Accessed 2024-04-08).

-E. Archambault and Y. Veilleux-Lepage. Tower 22: Innovations in Drone Attacks by Non-State Actors. International Centre for Counter-Terrorism. 24-02-01. <https://www.icct.nl/publication/tower-22-innovations-drone-attacks-non-state-actors> (Accessed 2024-08-24).

-Esteban Borges. Top 15 OSINT tools for expert intelligence gathering. Recorded future. 2024-04-29. <https://www.recordedfuture.com/threat-intelligence-101/tools-and-technologies/osint-tools> (Accessed 2024-06-26).

-Fordred, A (2023) Cyber Institute, 'OSINT MINI', <https://courses.thecyberinst.org/courses/osintworkshop>

-qccglobal. Drone Forensics Services. qccglobal. 2024-02-08. <https://qccglobal.com/drone-forensics-services/> (Accessed 2024-07-02).

-Gov.uk. 2024-05-16. <https://www.gov.uk/government/news/cutting-edge-drone-killer-radio-wave-weapon-developing-at-pace> (Accessed 2024-06-20).

-“History of Drone Warfare”, The Bureau of Investigative Journalism, 4 September 2020, <https://www.thebureauinvestigates.com/explainers/history-of-drone-warfare/>

-Homeland Security. Addressing risks from non-state actors' use of commercially available technologies. Public-Private Analytic Exchange Program, 2023

-I. Ilikjevski, Z Dimovski, K Babanoski. The weaponisation of drones - a threat from above used for terrorist purposes. Journal of Criminal Justice and Security, vol. 3, no. 3, 2023.

-I C. Peden, J V. Braddock, W Brown. Artificial Intelligence and Robotics. Army Science Board, Office Assistant Secretary of the Army, 1982

-Imperial War Museums. A Brief History of Drones. Imperial War Museums. <https://www.iwm.org.uk/history/a-brief-history-of-drones> (Accessed 2024-02-20).

-Intel Brief. Terrorists' use of drones and other emerging technologies. The Cipher Brief 18-10-03. https://www.thecipherbrief.com/column_article/terrorists-use-of-drones-and-other-emerging-technologies (Accessed 2024-02-27).

- J.Rogers, D. Kunertova. The vulnerabilities of the drone age: established threats and emerging issues out to 2035. Centre for war studies, 2022

-Jacob Ware. Terrorist groups, artificial intelligence and killer drones. War on the Rocks. 2019-09-24. <https://warontherocks.com/2019/09/terrorist-groups-artificial-intelligence-and-killer-drones/> (Accessed 2024-05-28).

-Jeff M, (2023), Udemy, 'OSINT: Open Source Intelligence', <https://www.udemy.com/course/osint-open-source-intelligence>

-Jared Keller. The Army Has Officially Deployed Laser Weapons Overseas to Combat Enemy Drones. Military.com. 24-04-24. <https://www.military.com/daily-news/2024/04/24/army-has-officially-deployed-laser-weapons-overseas-combat-enemy-drones.html> (Accessed 2024-06-15).

- Jessica Murray and agencies. Birmingham PhD student guilty of using 3D printer to build 'kamikaze' drone. The Guardian. 2023-09-28. <https://www.theguardian.com/uk-news/2023/sep/28/birmingham-phd-student-mohamad-al-bared-guilty-using-3d-printer-to-build-kamikaze-drone> (Accessed 2024-08-24).

-John W. Rollins. Armed drones: evolution as a counterterrorism tool. Congressional Research Service. 2023-11-07. <https://crsreports.congress.gov/product/pdf/IF/IF12342> (Accessed 2024-01-22).

-Joint Air Power Competence Centre. A Comprehensive Approach to Countering Unmanned Aircraft Systems, The Joint Air Power Competence Centre, von-Seydlitz-Kaserne, Römerstraße 140, 47546 Kalkar, Germany.: Joint Air Power Competence Centre, 2020

-Kami Shah. The Evolution and Future of Drone Battery Technology. Drones Technology. 2024-03-08. <https://dronstechnology.com/the-evolution-and-future-of-drone-battery-technology/> (Accessed 2024-07-31).

-K.A.Greico, J. W. Hutto. Can drones coerce? The effects of remote aerial coercion in counterterrorism. International Politics, 2021.

-K. Chavez, O. Swed. Off the Shelf: The Violent Nonstate Actor Drone Threat. Air & Space Power Journal, 2020.

-Larry Friese. Emerging Unmanned Threats: the use of commercially available UAVs by armed non-state actors. Armament Research Services, vol. 2, 2016

-M. Emimi, M. Khaleel and A. Alkrash. The current opportunities and challenges in drone technology. International Journal of Electrical Engineering and Sustainability (IJEES), vol. 1, no. 3, 2023

-M. J. Logan, J. Chu, M. A. Motter et al. Small UAV Research and Evolution in Long Endurance Electric Powered Vehicles. NASA, 2007

-Maria-Louise Clausen. Non-state armed groups in the sky: Global regulation fails to address the security risks posed by civilian drones. Danish Institute for International Studies. 2024-04-15. <https://www.diis.dk/en/research/non-state-armed-groups-in-the-sky-global-regulation-fails-to-address-the-security-risks> (Accessed 2024-05-23).

-Marsili, M. (2023). Morals and Ethics in Counterterrorism. Conatus - Journal of Philosophy, [online] 8(2), pp.373–398. doi:<https://doi.org/10.12681/cjp.34495> Ministry of Defence, Defence Science and Technology Laboratory, James Cartlidge. Cutting-edge drone killer radio wave weapon developing at pace.

-Miriam McNabb. CEPA experts highlight key challenges in drone warfare integration. Drone life. 24-05-13. <https://dronelife.com/2024/05/13/cepa->

experts-highlight-key-challenges-in-drone-warfare-integration/ (Accessed 2024-06-25).

-NATO. The official NATO Terminology Database. The official NATO Terminology Database. <https://nso.nato.int/natoterm/content/nato/pages/home.html?lg=en> (Accessed 2024-03-01).

- News Wires. Yemen's Houthi rebels in deadly attack on Saudi airport. France24. 2019-06-24. <https://www.france24.com/en/20190623-yemens-houthi-rebels-launch-deadly-strike-saudi-airport> (Accessed 2024-07-31).

-Nikola Brzica. Understanding Contemporary Asymmetric Threats. Croatian International Relations Review, vol. 83, no. XXIV, 2018.

-NORTH ATLANTIC COUNCIL. NATO Countering Class I Unmanned Aircraft Systems (C-UAS) Handbook. NATO, vol. 2, no. 2, 2020.

-Presenting a Drone Lighting Show to the People at the Delightful Lantern Festival. Vents Magazine. 2024-05-25. <https://ventsmagazine.uk/2024/05/25/presenting-a-drone-lighting-show-to-the-people-at-the-delightful-lantern-festival/> (Accessed 2024-06-14).

- Remote piloted aerial vehicles. Remote Piloted Aerial Vehicles : An Anthology. Remote piloted aerial vehicles. 2003-02-02. https://www.ctie.monash.edu/hargrave/rpav_home.html (Accessed 2024-03-).

-Robin radar systems. Why Traditional Radar Isn't Effective at Tracking Drones. Robin radar systems. <https://www.robinradar.com/why-traditional-radar-isnt-effective-at-tracking-drones> (Accessed 2024-08-21).

-Rueben Dass. Al-Qaeda in the Arabian Peninsula's Drone Attacks Indicate a Strategic Shift. Lawfare media. 2023-08-20. <https://www.lawfaremedia.org/article/al-qaeda-in-the-arabian-peninsula-s-drone-attacks-indicate-a-strategic-shift> (Accessed 2024-08-01).

- Schmid, A. (n.d.). Terrorism - The Definitional Problem. Case Western Reserve Journal of International Law, 36(2).

- Susan Becker. Drone swarms: scaling up for a new level of efficiency. elsight. 2022-08-22. <https://www.elsight.com/blog/drone-swarms-scaling-up-for-a-new-level-of-efficiency/> (Accessed 2024-02-18).
- The global security market. Global market for UAVs predicted to reach \$163 billion by 2030. securityworldmarket.com. 2024-05-16. <https://www.securityworldmarket.com/int/News/Business-News/global-market-for-uavs-predicted-to-reach-163-billion-by-2030> (Accessed 2024-05-17).
- Thomas G. Pledger. The role of drones in future terrorist attacks. ASSOCIATION OF THE UNITED STATES ARMY, vol. 136, 2021
- Thomas Newdick. China Tested An AI-Controlled Submarine-Hunting Underwater Drone A Decade Ago: Report. The warzone. 2021-07-09. <https://www.twz.com/41478/china-tested-an-ai-controlled-submarine-hunting-underwater-drone-a-decade-ago-report> (Accessed 2024-06-04).
- Tim Martin. <https://breakingdefense.com> Uk reveals development of low-cost radio frequency directed energy weapon. Breaking Defense. 2024-05-16. <https://breakingdefense.com/2024/05/uk-reveals-development-of-low-cost-radio-frequency-directed-energy-weapon/> (Accessed 2024-06-10).
- United Nations Office of Counter-Terrorism, Global Counter-Terrorism Programme on Autonomous and Remotely Operated Systems (AROS Programme). AROS PROGRAMME Autonomous and Remotely Operated Systems Global Report on the Acquisition, Weaponization and Deployment of Unmanned Aircraft Systems by Non-State Armed Groups for Terrorism-related Purposes. United Nations Office of Counter Terrorism, (2024)
- V.U. Castillo, A. Manco, D. Pascarella, G. Girante. A review of counter-UAS technologies for cooperative defensive teams of drones. Drones, vol. 6, no. 65, 2022
- W. Khawaja et al. Threats from and Countermeasures for Unmanned Aerial and Underwater Vehicles. Sensors, vol. 22, no. 3896, 2022

-Y. Seo, B. Lendon. South Korea to mass produce lasers that can take out drones at \$1.50 a hit. CNN. 2024-07-11. <https://edition.cnn.com/2024/07/11/asia/south-korea-antidrone-lasers-intl-hnk-ml/index.html> (Accessed 2024-08-24).

-Zachary Kallenborn. Swarm clouds on the Horizon? Exploring the Future of Drone Swarm Proliferation. Modern War Institute at West Point. 2024-03-20. <https://mwi.westpoint.edu/swarm-clouds-on-the-horizon-exploring-the-future-of-drone-swarm-proliferation/> (Accessed 2024-06-14)