



Universiteit
Leiden
The Netherlands

The legality of countering potential threats posed by drones under international air law

Kurtpınar, O.; Scott, B.I.

Citation

Kurtpınar, O., & Scott, B. I. (2024). The legality of countering potential threats posed by drones under international air law. *2024 International Conference On Unmanned Aircraft Systems (Icuas)*, 347-354. doi:10.1109/ICUAS60882.2024.10556979

Version: Publisher's Version

License: [Leiden University Non-exclusive license](#)

Downloaded from: <https://hdl.handle.net/1887/4170278>

Note: To cite this publication please use the final published version (if applicable).

The Legality of Countering Potential Threats Posed by Drones Under International Air Law

Öykü Kurtpinar
Ph.D. candidate at Leiden University
Leiden, Netherlands
e.o.kurtpinar@law.leidenuniv.nl

Benjamyn I. Scott
Assistant Professor at Leiden University
Leiden, the Netherlands.
b.i.scott@law.leidenuniv.nl

The Convention of International Civil Aviation of 1944 recognises that States must refrain from using weapons against civil aircraft while they are in flight. However, the rise in non-cooperative unmanned aircraft raises the question of how can these be lawfully intercepted.

I. INTRODUCTION

Unmanned Aircraft (UA or drone) are currently being deployed across the Single European Sky for a variety of purposes and in numerous sectors. For example, they are being deployed for agriculture, construction, surveillance, healthcare and environmental purposes [1]. The use of drones is also evolving and the technology is advancing, whereby they are increasingly being used in new and innovative ways, which is only expected to continue. For example, a future use case will be passenger air taxi services (PATs) using unmanned electric vertical take-off and landing (eVTOL) aircraft. The European Union (EU) is predicting that, by 2030, with the correct framework in place, the drone service market in Europe could be worth €14.5 billion, which would be expected to grow annually by around 12.3% [1].

The swift rise in accessibility and affordability, as well as the advancements in the technology, is allowing for a greater number of people to access this airborne technology and conduct increasingly more complex operations. This is, however, posing a considerable challenge for regulators and law enforcement as the capabilities and operation portfolios are advancing more rapidly than the capacity to evaluate and address the potential threats posed by drones.¹ This involves both legitimate lawful uses of drones, as well as threats posed by non-cooperative drones. The latter may include the use of drones for criminal activities, such as to smuggle drugs across international borders and into prisons, which have been referred to as ‘narcodrones’, as well also for surveillance to support criminal activities [3].

Drones may also intentionally be operated outside of the regulatory framework [4], [5], such as near critical

infrastructure, which would be a breach of the law. A notable example is their use near airports to disrupt air traffic, such as on 28 September 2023, when a non-cooperative drone caused delays and cancelled flights at Frankfurt airport [6]. Finally, non-cooperative drones can also result from unintentional actions by the operator, such as due to ignorance or carelessness [7].

As a result of the rise in non-cooperative drones, the EU Commission included a specific flagship action in *Drone Strategy 2.0 for a Smart and Sustainable Unmanned Aircraft Eco-System in Europe* (Drone Strategy 2.0), which was to adopt a counter-drone (C-UAS) package [1]. This has resulted in the publication of Two Handbooks [7], [8] and a *Communication On Countering Potential Threats Posed By Drones* (C-UAS Communication) [9]. This paper will provide a critical overview of the Communication, which is an attempt by the EU to:

- “(i) provide a comprehensive and harmonised policy framework;
- (ii) build a common understanding of applicable procedures to face the continuously evolving threats possibly posed by drones; and
- (iii) take into account the rapid developments in technology.” [9]

The paper will provide background to the topic and offer insight into the future actions to be taken by the EU and other stakeholders, including the development of a C-UAS Policy. Further, as a response to non-cooperative drones can either be *passive* (e.g. detection, classification or identification) or *active* using countermeasures (e.g. physical destruction, neutralising, or taking control of the drone), it is necessary to look at the legality of such acts. For example, active responses may result in the shooting down of a civil aircraft, which raises a question of the legality of such an act pursuant to Article 3(bis) of the Convention on International Civil Aviation (Chicago Convention) 1944 [10]. This will require a legal analysis of the Article to understand its scope and applicability. This will then allow for it to be applied to

¹ Highlighting the prevalence of illegal drone activity, the Final Report of Riga CTR Airspace Assessment by EUROCONTROL revealed that within the selected airspace, 91% of the recorded flights exceeded the maximum

flight altitude permitted, and therefore is deemed illegal under national regulations [2].

various counter-drone activities to determine whether they would be lawful under international law.

II. BACKGROUND TO COUNTER-DRONE ACTIVITIES IN THE EU

A. Non-Cooperative Drone Activities in the EU

The term ‘non-cooperative drone’ is commonly used to describe drone activities, that demonstrate non-compliance with the applicable laws [9]. This could be the specific drone rules that govern the operation, as well as other more general rules such as privacy and criminal law. This could stem from criminal activities, illegal actions (intended regulatory breach) or amateur behaviours (ignorance or carelessness).

In 2022, a reported incident involved the use of an explosive-loaded drone to attack a football match between Barcelona and Real Madrid. The target was the Camp Nou Stadium, with a capacity of roughly 100,000. The potential loss of life could have been significant and prompted the implementation of additional counter-drone technology at the stadium. An individual was eventually sentenced to 3 years in prison for planning the attack [12], [13].

Drones are increasingly exploited for assaults on critical infrastructure and public institutions, serving as a means to transport hazardous materials. Past occurrences have also revealed drones delivering not only dangerous materials, but also mobile phones, drugs and weapons. Several such incidents have already been documented, including a case in Italy where an inmate reportedly fired at fellow prisoners with a gun allegedly smuggled in by a drone [14].

High-tech onboard cameras allow perpetrators to collect sensitive information, facilitate attacks or provide real-time updates during criminal activities. Furthermore, cyberattacks involving drone-mounted jammers can disrupt security systems, communications and even hijack sensitive data [15]. In Europe, there are already alleged cases of criminal reconnaissance activities conducted before burglaries, providing a technological leverage point for criminals [16].

Drones are also increasingly being used for attacks against individuals. Police reports detail alarming incidents, including a Dutch case where a girl was terrorised by a drone in Midden-Drenthe [17]. These instances often involve affordable light-weight drones, which can in normal circumstances be operated in the Open Category [5]. However, its operation near individuals, over crowds of people or in no-fly zones places such operation into a higher risk category (Specific Category or Certified Category) and necessitates special authorisation [5].

In the EU, there are also reported incidents of near-mid-air collisions such as the incident that took place when the radars of a Wizz Air aircraft approaching the runway at an altitude of about 1,200m failed to detect the large quadcopter near

Katowice Airport, Poland and passed over a large drone with just 50m of clearance [18].

It is important to note that not all non-cooperative drone activities are driven by malicious intent. Many incidents involve users exhibiting ignorance or carelessness, engaging in such activities without criminal or illegal intentions. However, the absence of the *mens rea* element does not necessarily absolve individuals from legal consequences, or eliminate associated risks and damages. For instance, when an Open Category drone operation is accidentally flown beyond the visual line of sight (BVLOS), it transitions from operating in the Open Category to the Specific Category, so the operator must obtain the right authorisation. Loss of control during a flight or a lack of awareness regarding aerial restrictions may result in flights occurring in prohibited zones, such as around nuclear power plants or airports.

Past incidents suggest immediate impacts of drone incidents range from potentially affecting human life through injuries or fatalities to causing economic losses through repair costs and service disruptions, and even triggering environmental problems like water contamination [7].

B. Counter-Drone Technology and Activities

Proposed solutions against the above-explained drone threats are mostly technical – which supplement the existing laws – and address the aspects of detection, tracking and identification as well as neutralisation and forensics concerning non-cooperative drones. Such drone monitoring equipment can be *passive* (simply looking or listening) or *active* (sending a signal out and analysing what comes back). Functions provided by the monitoring equipment include: detection, classification or identification, locating and tracking, and alerting [19].

The interception of the non-cooperative drone can lead to three distinct scenarios [19]:

1. Taking control of the drone;
2. Neutralising the drone; or
3. Physically destroying the drone.

These outcomes can be achieved through various technical methods. This could be done in 2 main ways [19]:

1. **Physical:** Retaining a physical approach to restrict the target drone physically, these tools can use a net-like structure or a bird to capture the drones. They can be terrestrial such as human-held-vehicle or vehicle-mounted (net guns) or aerial as in attached on defender drones [20]. A significant portion of current anti-drone systems deploy also military components capable of destruction such as missiles or weapons [21].

2. **Electronic:** Hacking or hijacking prohibits the original operator the use of the drone as the controls are usurped to retain such control by the anti-drone system.

Radio Frequency Jammers are among other electronic C-UAS tools, which are employed to disable the controller's communication and disrupt wireless networks in the vicinity. The drone's response to jamming is unpredictable (e.g. falling or returning to a 'home' point) and relies on its programmed reactions [20], [21].

High Power Microwaves may also be used that generate an electromagnetic pulse (EMP) capable of damaging or destroying the electronic components of the drone [19], [20], [21].

III. OVERVIEW OF THE C-UAS STRATEGY

A. Introduction: Drone Strategy 2.0

The Drone Strategy 2.0 presents, *inter alia*, the EU's efforts to develop counter-drone tools, which involve knowledge building, technologies, funding, research and innovation programs such as Horizon Europe [21]. A significant emphasis is given to the aimed synergy between the civil, security and defence industries, with an explicit emphasis on counter-drone technologies.

The Commission while adopting the Drone Strategy 2.0 aimed at building a drone service market within the Union and "strengthen the Union's civil, security and defence industry capabilities and synergies". This objective required also the involvement of counter-drones and the defence sector, as a part of the drone value chain. It is connected with the broader context of EU strategies, such as the European Security Strategy [22], and the Counter-Terrorism Agenda [23]. Moreover, while pursuing to aggravate the benefits to be acquired by drone technology, the Drone Strategy 2.0 also acknowledges the growing threat posed by drones for criminal activities and attacks on public spaces, individuals and critical infrastructure. It emphasises the regulatory contradiction caused by the lack of rules and guidelines on the unauthorised or criminal use of drones while the legitimate use of drones is regulated [3].

B. C-UAS package

In response to the increasing threats posed by the proliferation of non-cooperative drones, the Commission presented the EU's policy on countering the potential threats from non-cooperative drones. It was announced as the 17th flagship in the Drone Strategy 2.0 [24].

"Flagship action 17: The Commission intends to adopt a counter-drone (C-UAS) package." [3]

The adoption of a dedicated C-UAS package would outline the future EU's policy, encompassing comprehensive guidelines, potential legislative adjustments and multifaceted support for Member States. The Strategy around which the discussion of this article evolved is the C-UAS Communication [9].

Building on the first EU counter-drone workshop in 2016 and the following initiatives introduced from the workshop, the Commission plans to keep supporting these initiatives while incorporating new strands of work to formulate a comprehensive EU counter-drone policy, comprised of six key activities [9].

- Community building and information sharing
- Testing of counter-drone systems
- Practical guidance & operational support
- Research & innovation
- Funding support
- Regulatory measures

This article is confined to analysing the last pillar which concerns the regulatory measures to be taken from the perspective of the Chicago Convention Article 3(bis).

C. The 3 Key Actions

Exploring the regulatory measures, the Commission culminates its analysis into 3 key actions.

Action 1 Mapping: While the EU regulates legitimate drone use, a common regulatory framework for counter-drone measures remains absent.

"The Commission will initiate a mapping study to identify regulatory needs and the potential for harmonising Member States' laws and procedures."

Non-binding guidelines for airport incidents were developed and welcomed by the sector [7], [10]. However, they have a limited scope so they are not sufficient against the growing number of unauthorised drone activities. Therefore, the Commission, in collaboration with Member States, will analyse the need for future legislative or non-legislative measures.

The Commission will conduct a mapping study to assess the current regulatory landscape, including ICAO framework developments, ensuring a balance between countering the threats and legitimate drone activities.

Action 2 Risk-Assessment: Detailed and comprehensive rules for airports regarding drone threats are established to a certain extent.

"In line with an evidence-based approach, the Commission will undertake an aviation security-risk assessment on drones to identify potential additional vulnerabilities of airports, which could mandate regulatory changes."

Nevertheless, the Commission together with Member States, will still conduct a security-risk assessment to identify potential airport vulnerabilities against non-cooperative drones, necessitating any necessary regulatory changes.

Action 3 Structured Dialogue: The need for a structured dialogue with industry, including drone manufacturers, is emphasised, regarding ‘security-by-design’ measures, such as “systems against spoofing, capability limitations, sharing of communication protocols, and updates for counter-drone databases” [9].

“The Commission will engage in a structured dialogue with industry on the necessity for – and nature of – potential additional specific measures relating to the security of drones.”

Industry was engaged with the Commission during the Drone Strategy 2.0 and is supporting the development of the EU rules, so this will be a continuation.

D. Wider considerations and next steps (ie international law)

The initiatives detailed in the C-UAS Communication will span until 2030. A mid-term assessment is planned to be conducted by the expert group by 2027, with a comprehensive revision of the EU’s counter-drone programme scheduled to be completed no later than 2030.

The first action point, a mapping study to identify the regulatory framework must include the international laws applicable to the EU drone activities. EU Member States, as signatories to the Chicago Convention, need to comply with the provisions of the Convention. This includes facilitating the lawful use of drones and the lawful interaction with them.

IV. THE CHICAGO CONVENTION AND ITS RELEVANCE

A. Introduction

The primary framework governing international civil aviation is the Chicago Convention, which currently has 193 State Parties (per February 2024). It was established in 1944 and sets forth principles and rules for the peaceful use of airspace and the regulation of civil aviation as highlighted in the Preamble:

*“Whereas the future development of international civil aviation can greatly help to create and preserve friendship and understanding among the nations and peoples of the world, yet its abuse can become a threat to the general security and;
Whereas it is desirable to avoid friction and to that cooperation between nations and peoples upon which the peace of the world depends;
Therefore, the undersigned Governments having agreed on certain principles and arrangements in order that international civil aviation may be developed in a safe and orderly manner and that international air transport services may be established on the basis of equality of opportunity and operated soundly and economically.”*

The text demonstrates that the aim of the Convention is to facilitate cooperation among States for the benefits of peace and security, as well as to increase aviation safety[25].

Article 1 of the Chicago Convention confirms the customary international law principle that a State has sovereignty over its airspace: *“The contracting States recognize that every State has complete and exclusive sovereignty over the airspace above its territory”* [10]. This Article makes it abundantly clear that aircraft, which includes drones, have no automatic right to fly over or land in the territory of another State. This is also applicable, as affirmed in Article 3(c), to State aircraft.

As the airspace is closed, unless otherwise opened by the concerned State, the drafters of the Chicago Convention wanted to provide legal mechanisms to permit foreign aircraft. Such mechanisms can be found in:

- Article 5 Right of Non-Scheduled Flight
- Article 6 Scheduled Air Services
- Article 7 Cabotage
- Article 8 Pilotless Aircraft

If the international element is not satisfied, then the flight is domestic and outside the scope of the Chicago Convention. This will be regulated at a national level by that State or, where such responsibilities are delegated, at a regional level like in the EU[26].

Whether international or domestic, the flight will be governed by strict rules, which will apply equally to foreign and domestic carriers to ensure a high level of safety. This includes the rules on certification, licencing, rules of the air, environmental protections and registration.

B. Misuse of Civil Aviation

The first relevant clause is Article 4 of the Chicago Convention [10]:

“Each contracting State agrees not to use civil aviation for any purpose inconsistent with the aims of this Convention.”

To give clarity to what an aim inconsistent with the Convention could mean, ICAO conducted a study whereby it stated that *“an inconsistent purpose with the aims of this Convention”* means *“threats to the general security”* [11]. During the twenty-fifth (Extraordinary) Session of the ICAO Assembly, practical examples of what could be within the scope of Article 4 were discussed.

“Acts of aggression, infiltration or espionage involving discharge of harmful substances or pathogenic agents; transport of contraband or prohibited traffic using the airspace of another State, even with destination to a third State or with any

other purpose inconsistent with the aims of the Convention.” [27]

The conclusion is that such acts by States that threaten general security through the use of civil aviation would come under the scrutiny of Article 4. This could include the non-cooperative drone and C-UAS activities, such as the shooting down of civil aircraft. As this obligation is contained within the Chicago Convention, it is limited to State-to-State relations. As a result, it is not concerned with the acts of non-State actors [28].

C. Use of Weapons Against Civil Aircraft

The Chicago Convention, since its adoption, has been amended several times. Relevant to this paper is Article 3(bis), as deemed applicable to UAS by ICAO Manual on Remotely Piloted Aircraft Systems (RPAS) [29]. It covers the non-use of weapons against civil aircraft in flight.

The introduction of Article 3(bis) was provoked by the shooting down of Korean Air Lines Flight 007, which was a scheduled service from New York (US) to Seoul (South Korea) via Anchorage (US). On 1 September 1983, the Boeing 747 while *en route* from Anchorage to Seoul, entered Soviet prohibited airspace due to a navigational mistake and was shot down by a Soviet Sukhoi Su-15 aircraft. All 269 passengers and crew aboard were killed [30]. Article 3(bis) was adopted by consensus on 10 May 1984, less than one year after Flight 007 during the twenty-fifth Session (Extraordinary) of the ICAO Assembly.

Article 3(bis) (a) provides:

“The contracting States recognize that every State must refrain from resorting to the use of weapons against civil aircraft in flight and that, in case of interception, the lives of persons on board and the safety of aircraft must not be endangered. This provision shall not be interpreted as modifying in any way the rights and obligations of States set forth in the Charter of the United Nations.”

The amendment entered into force on 1 October 1998 and has 156 State Parties (per February 2024). As a result, the amendment is not binding on those contracting States that have yet to adopt Article 3(bis). Nevertheless, the Article is a codification of customary international law, so States are bound to this obligation.

Article 3(bis) uses the term ‘recognize’, so it has been argued by some commentators that this is “*not a new rule of law*”, but the recognition of “*the existence of a prior rule binding on all parties and prohibiting the use of weapons against civil aircraft in flight*” [30]. It is simply a codification of other sources of law [31]. Article 3(bis) uses the term ‘every State’, which shows that the effect of the Article is not limited to contracting States. This position is not universally held, but it

highlights the fact that Article 3(bis) may have wider application than to the 156 State Parties.

V. BREAKDOWN OF ARTICLE 3(BIS)

In order for Article 3(bis) to apply, three criteria must be satisfied.

A. Weapon

First, there must be the use of a ‘weapon’. The Chicago Convention does not provide a definition of this term, so clarifications must be sought elsewhere.

It has been argued that the lack of a definition does not raise problems when the ordinary meaning of the word is used.

“The term ‘weapons’ has not been defined but its interpretation in practice should not cause any difficulties when the ordinary meaning of the word is considered; it would include guns, machine guns, cannons, missiles or targeted drones or any other object or substance that can damage or destroy an aircraft in flight.” [32]

However, in the context of counter-drone technology, this is less clear. While physical tools, such as missiles and nets, can be seen as weapons, it is less clear for non-physical such as jamming, hijacking or spoofing. It is even less clear for passive activities.

Considering the ‘cyber’ element, these systems, such as hijacking, are often referred to as ‘cyber weapons’, which also lacks a legally binding definition under international law. Protocol IV on Blinding Laser Weapons [32], while not offering an explicit definition, holds an interpretative value as it acknowledges that electromagnetic radiation, such as lasers, qualifies as weapons despite their non-physical nature [34].

For something to be a ‘weapon’, it must possess the capability to cause death, damage or destruction [34]. This requires analysis of the practice (*de facto*) more than from legal definitions (*de jure*). Consequently, when determining whether a counter-drone system constitutes a weapon, the specific technicalities and capabilities of the employed system become decisive.

Applying this framework, counter-drone systems employing physical destructive methods such as missiles readily fall under the category of weapons. Similarly, systems using radio frequencies to disrupt drone components such as HPM, though intangible, inflict damage on the drone by inducing malfunction and crashing, meet the criteria to be categorised as weapons.

Hijacking, however, introduces a different scenario. Successful hijacking does not inherently cause damage, injury or death. It should be noted that the underlying rationale of Article 3(bis) prohibits the use of weapons but explicitly allows interception (paragraph (b)). Hijacking of spoofing

which involves the takeover of a non-cooperative drone, presents parallels to paragraph b, which permits state interception such as constricting the aircraft to land at an airport, under the condition of ensuring safety.

B. Civil Aircraft

Second, the weapon must be used ‘against civil aircraft’. This should be contrasted with ‘State aircraft’. Article 3(a) of the Chicago Convention creates a legal distinction between ‘State aircraft’ and ‘civil aircraft’.

“This Convention shall be applicable only to civil aircraft, and shall not be applicable to state aircraft.”

The Convention does not define ‘civil aircraft’, however, a partial definition can be obtained from Article 3(b).

“Aircraft used in military, customs and police services shall be deemed to be state aircraft.”

As the Convention uses the term ‘deemed’, military, customs and police activities shall be *prima facie* considered State aircraft until proven otherwise [35]. However, this list is non-exhaustive, whereby border control, fire-fighting, search and rescue, disaster relief, government transport, humanitarian flights, and carriage of prisoners may also be deemed as State aircraft [36].

A non-cooperative drone may be either a civil or a State aircraft, whereby the specifics of the situation must be assessed. This will depend on the specific case, but the obligation to refrain from the use of weapons lies with the States.

C. In Flight

Third, the aircraft must be ‘in flight’. Again, this term is not defined. It could be understood to include only the time when the drone is achieving aerodynamic lift (i.e. the flight phase) or also other parts of the operation such as ground movements (e.g. taxing) or while parked. This criterion is unlikely to cause many issues for active C-UAS tools, as they are primarily focused on drones while in flight.

Article 3(bis) does, however, not require the flight to be international, despite the scope of the Chicago Convention being *international* civil aviation. Thus, it would cover domestic flights.

D. Outcome

If these three criteria are satisfied, then States have an obligation to *refrain* from the use of weapons. This is not an outright ban as States have rights and obligations under the Charter of the United Nations. This is a reference to a State’s

right to self-defence under Article 51 of the Charter of the United Nations (UN Charter) 1945 [37], which states that:

“Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations [...]”

When there is an immediate and significant threat to a nation’s sovereignty, then the state can legally use weapons against civilian aircraft. This extends to the use of C-UAS tools categorised as *weapons* against civilian drones. Nonetheless, the threshold justifying such use of weapons is very high.

Article 51 restricts the justified use of weapons to instances of armed attacks. What constitutes an armed attack has been interpreted by the Court of Justice in the *Nicaragua* case [37] and affirmed by its advisory opinion in *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory* [39]. Accordingly, an armed attack within the context of Article 51 involves state actors and it is:

“the sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to’ (inter alia) an actual armed attack conducted by regular forces, ‘or its substantial involvement therein.” [37]

It must be concluded that the right to self-defence applies only in cases of *armed attack* performed by one State against another State. The use of civil non-cooperative drones, such as for the delivery of contraband to prisons or disruption of aviation activities around airports, does not reach such a threshold.

Since the majority of situations involving non-cooperative drones do not constitute an armed attack, especially those envisaged by the Commission within the context of the C-UAS strategy, it would suggest active C-UAS measures would be illegal. Moreover, even in justified incidents, deploying weaponised counter-drone systems against civil drones should be compliant with the use of force principles, namely proportionality and necessity, a part of the customary international law as expressed in the Carolina doctrine [40].

Using weapons against civil aircraft is not the only option at hand. States can also take interceptive measures against the UAS, as affirmed by the ICAO Manual on RPAS [29]. In such situations, the UAS pilot must adhere to the instructions communicated by the State via electronic or visual means, and be prepared to redirect to the designated airport at the State’s request [29]² However, ICAO notes that the interception of civil aircraft as ‘in all cases, potentially hazardous’ requiring

² The manual emphasises that the requirement to respond to visual instructions could impose substantial demands on the certification of RPAS detect and avoid systems for international operations.

it to pass the legal test of an acceptable interception [41]. Therefore, besides the use of weapons, interception should be conducted as a last resort. During interception, which might involve visual signals, radio communications, or instructions to the intercepted aircraft, states are obliged to refrain from endangering the lives of persons on board and the safety of the aircraft.

VI. FINAL REMARKS

The rapid development and increasingly widespread use of drones, while offering many benefits, also present potential security risks. The EU by introducing C-UAS Communication, aims to proactively address these risks before they escalate, ensuring that the growing number of drones does not translate into an uncontrolled increase in threats.³ The C-UAS Communication is an important step towards enhancing Member States' detection and identification capabilities, supporting the development of reliable counter-drone technologies, harmonising regulations across states, and promoting international collaboration to create a secure and responsible drone ecosystem in the EU and globally.

On the other hand, the EU's aviation sector not only operates under its own internal regulations and policies, but also exists within a wider framework of international obligations. Foremost among them is the Chicago Convention, aimed at fostering peace, security, and heightened aviation safety. Addressing non-cooperative drones, particularly through *active* tools, poses potential conflicts with international and national law. While acknowledging the broader landscape of other relevant international regulations, this paper kept its analysis focused on Article 3(*bis*), which prohibits the use of weapons against civil aircraft.⁴

Although not all C-UAS tools qualify as *weapons*, those that can inflict damage, death or destruction, such as lasers, killer drones, HPM or anti-aircraft missiles, fall under the category of *weapons*. Consequently, deploying them against civilian aircraft would constitute a violation of Article 3(*bis*). Moreover, unless used against an *armed attack* by a *State actor*, such actions cannot be justified under the right to self-defence.

For instance, where the application of States' right to self-defence is justified, it should be noted that the historical context of the Chicago Convention, Article 3(*bis*) was originally conceived with traditionally manned aircraft in mind. The initial condition, addressing the "*lives of the persons on board*" presently does not apply to non-

cooperative drones, unless eVTOL aircraft capable of transporting people can and will be used for illegitimate purposes, such as human smuggling or terrorist activities.

When employing counter-drone systems that do not fall within the classification of *weapons* and, thus, lie outside the scope of Article 3(*bis*), but have the potential for interception purposes (e.g. hacking), it is imperative to implement all necessary measures to guarantee the safety. This implies prioritising techniques that minimise damage and preserve the structural integrity of the drone, thereby mitigating potential hazards to property and persons on the ground.

This paper does not advocate for the blanket rejection of all C-UAS tools based on Article 3(*bis*); rather, it underscores the nuanced nature of their selection as the potential for certain tools to violate Article 3(*bis*) depends on the context of their use, technical specifications and the actor operating the non-cooperative drone.

VII. DECLARATION STATEMENTS

A. Funding (information that explains whether and by whom the research was supported)

The authors declare that no funds, grants, or other support were received during the preparation of this manuscript.

Conflicts of interest/Competing interests:

The authors have no relevant financial or non-financial interests to disclose.

B. Code or data availability

Not applicable.

C. Authors' Contributions

The following authors contributed equally to all aspects of the study:

Öykü Kurtpınar LL.M (Adv.), *Ph.D. candidate at Leiden University*. E-mail e.o.kurtpinar@law.leidenuniv.nl.

Benjamyn Scott Ph.D., LL.M. (Adv.) is *Assistant Professor at Leiden University*, Leiden, the Netherlands.

Email: benjamyn.scott@gmail.com.

D. Ethics approval

Not applicable – No animals, including humans, were studied in any way during the writing of this paper.

E. Consent to participate

This study did not involve any 3rd party participation. All authors consent to participation.

³ In parallel with the European Union's efforts, other jurisdictions, including the United States, are actively engaged in the development of C-UAS capabilities. Notably, the Federal Aviation Administration (FAA) was tasked with formulating a comprehensive action plan to facilitate the operational deployment of detection and mitigation systems to address the growing threat posed by unauthorized drone activity. This mandate was enshrined within the most recent FAA Reauthorization Act, enacted in 2018. Moreover, the legal implications surrounding C-UAS technologies remain a topic of ongoing discourse in the US. *See*, [42].

⁴ This analysis recognises the presence of other additional legal complexities in addressing counter-drones. For instance, taking the control of non-cooperative UAS, or CUAS technologies using radio frequency jamming or spoofing, requires the consideration of electronic communication sector regulations at the EU and national level. However, a detailed analysis of these intricacies falls outside the purview of this paper due to its restricted scope.

F. Consent for publication

This study did not involve any 3rd party participation. All authors consent to publication.

REFERENCES

- [1] European Commission, 'A Drone Strategy 2.0 for a Smart and Sustainable Unmanned Aircraft Eco-System in Europe' 29 November 2022, COM(2022) 652.
- [2] EUROCONTROL, Final Report of Riga CTR Airspace Assessment, [2019].
- [3] 'Eastern District of California | Four Indicted in Scheme to Deliver Drugs into State Prisons by Drone | United States Department of Justice'. Accessed: Feb. 09, 2024. [Online]. Available: <https://www.justice.gov/usao-edca/pr/four-indicted-scheme-deliver-drugs-state-prisons-drone>.
- [4] Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on Unmanned Aircraft Systems and on Third-Country Operators of Unmanned Aircraft Systems, OJ L 152, 11 July 2019, p. 1–40.
- [5] Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the Rules and Procedures for the Operation of Unmanned Aircraft, OJ L 152, 11 June 2019, p. 45–71.
- [6] 'Frankfurt Airport Halts Flights Over Unidentified Drone'. Accessed: Feb. 09, 2024. [Online]. Available: <https://simpleflying.com/frankfurt-airport-halts-flights-unidentified-drone/>.
- [7] Paul Hansen and Ricardo Pinto Faria, 'Protection against Unmanned Aircraft Systems: Handbook on UAS protection of Critical Infrastructure and Public Space: A five Phase approach for C-UAS stakeholders, JRC Technical Report (2023).
- [8] V. Karlos and M. Larcher, 'Protection against unmanned aircraft systems: handbook on UAS risk assessment and principles for physical hardening of buildings and sites' Publications Office of the European Union, 2023. Accessed: Feb. 09, 2024. [Online]. Available: <https://data.europa.eu/doi/10.2760/969680>.
- [9] European Commission, Communication from the Commission to the Council and the European Parliament on Countering Potential Threats Posed by Drones', 18 October 2023, COM(2023) 659 final, 1.
- [10] Convention on International Civil Aviation 1944, 7 December 1944, 15 U.N.T.S. 295 (1944). (Chicago Convention).
- [11] ICAO Council, "'Misuse' of Civil Aviation", 117th Session, C-WP/8217, 18 March 1986.
- [12] '3-year sentence for plotting drone terror attack in Camp Nou during Barçaccedil; a v Real Madrid game'. Accessed: Jan. 17, 2024. [Online]. Available: <https://www.catalannews.com/society-science/item/3-year-sentence-for-plotting-drone-terror-attack-in-camp-nou-during-barca-v-real-madrid-game>.
- [13] 'FC Barcelona's Camp Nou stadium joins Catalan police's anti-drone security system'. Accessed: Jan. 17, 2024. [Online]. Available: "https://www.catalannews.com/society-science/item/fc-barcelonas-camp-nou-stadium-joins-polices-anti-drone-security-system
- [14] A. France-Presse, 'Italian prisoner shoots at rivals with gun "smuggled in by drone"', *The Guardian*, Sep. 20, 2021. Accessed: Feb. 09, 2024. [Online]. Available: <https://www.theguardian.com/world/2021/sep/20/italian-prisoner-shoots-at-rivals-with-gun-smuggled-in-by-drone>.
- [15] A. Shelley, 'A Counter-Drone Strategy for New Zealand', *NSJ*, vol. 4, May 2022, doi: [10.36878/nsj20220518.02](https://doi.org/10.36878/nsj20220518.02).
- [16] P. Paganini, 'Thieves are using commercial drones for burglaries', *Security Affairs*. Accessed: Jan. 17, 2024. [Online]. Available: <https://securityaffairs.com/37050/cyber-crime/thieves-using-commercial-drones.html>.
- [17] 'Girl Chased By Drone While On Her Way Home At Night'. Accessed: Jan. 17, 2024. [Online]. Available: <https://dronexl.co/2020/12/22/girl-chased-by-drone-night/>.
- [18] 'UAV in near miss with passenger plane'. Accessed: Jan. 17, 2024. [Online]. Available: <https://www.thefirstnews.com/article/uav-in-near-miss-with-passenger-plane-38464>.
- [19] '10 Types of Counter Drone Technology to Detect and Stop Drones Today'. Accessed: Jan. 19, 2024. [Online]. Available: <https://www.robinradar.com/press/blog/10-counter-drone-technologies-to-detect-and-stop-drones-today>.
- [20] S. Park, H. T. Kim, S. Lee, H. Joo, and H. Kim, 'Survey on Anti-Drone Systems: Components, Designs, and Challenges', *IEEE Access*, vol. 9, pp. 42635–42659, 2021, doi: [10.1109/ACCESS.2021.3065926](https://doi.org/10.1109/ACCESS.2021.3065926).
- [21] G. Lykou, D. Moustakas, and D. Gritzalis, 'Defending Airports from UAS: A Survey on Cyber-Attacks and Counter-Drone Sensing Technologies', *Sensors*, vol. 20, no. 12, p. 3537, Jun. 2020, doi: [10.3390/s20123537](https://doi.org/10.3390/s20123537).
- [22] European Commission, Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy, 24 July 2020, COM/2020/605.
- [23] European Commission, Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond, 9 December 2020, COM/2020/795.
- [24] B. Scott and K. Andritsos, 'A Drone Strategy 2.0 for a Smart and Sustainable Unmanned Aircraft Eco-System in Europe', *Air and Space Law*, vol. 48, pp. 273–296, Jul. 2023.
- [25] B. I. Scott and A. Trimarchi, *Fundamentals of international aviation law and policy*. in *Aviation fundamentals*. Abingdon New York, NY: Routledge, 2020.
- [26] Regulation (EC) No. 1008/2008 of the European Parliament and of the Council of 24 September 2008 on Common Rules for the Operation of Air Services in the Community, OJ L 293 of 31 October 2008.
- [27] ICAO, 'Minutes', 25th Session of the Assembly Executive Committee, EX/6 (1984).
- [28] Draft Articles on Responsibility of States for Internationally Wrongful Acts (November 2001), Supplement No. 10 (A/56/10), Ch. IV.E.1, Ch. 2.
- [29] ICAO, 'Manual on Remotely Piloted Aircraft Systems (RPAS)' Doc 10019 AN/507, (2015), 11.3.2.
- [30] G. Guillaume, 'The Destruction on 1 September 1983 of the Korean Airlines Boeing (Flight KE 007)', *ITA Magazine* No. 0–18 (1984), 34, in Huang, *Aviation Safety Through the Rule of Law: ICAO's Mechanisms and Practices* (2009), 88 fn. 13.
- [31] ICAO, 'Administrative Package for Ratification of the Protocol on Article 3 Bis', https://www.icao.int/secretariat/legal/Administrative%20Packages/3bis_en.pdf.
- [32] M. Milde, *International Air Law and ICAO*. Eleven International Publishing, 2016.
- [33] Protocol on Blinding Laser Weapons (Protocol IV), Vienna, 13 October 1995, Art. 1.
- [34] B. I. Scott, *Aviation Cybersecurity: Regulatory Approach in the European Union*. Eleven, 2019, 140–147.
- [35] A. S. Williams, 'The Interception of Civil Aircraft over the High Seas in the Global War on Terror', *A.F. L. Rev.*, vol. 59, p. 73, 2007, 73–151.
- [36] R. De Oliveira, 'The Distinction Between Civil and State Aircraft: Does the Current Legal Framework Provide Sufficient Clarity of Law with Regard to Civil and State Aircraft in Relation to Aviation Practicalities?', *AILA*, vol. 41, no. Issue 4/5, pp. 329–343, Sep. 2016, doi: [10.54648/AILA2016025](https://doi.org/10.54648/AILA2016025).
- [37] United Nations, *Charter of the United Nations*, 1 UNTS XVI, 24 October 1945.
- [38] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment [1986] ICJ Reports 14.
- [39] Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, [2004] ICJ Reports 136 para. 139.
- [40] C. H. M. Waldock, *The Regulation of the Use of Force by Individual States in International Law*. Recueil Sirey, 1953, 461.
- [41] ICAO, Chicago Convention, Annex 2, 'Rules of the Air' Appendix 2, Interception of the Civil Aircraft, July 2005, 711.
- [42] Rupprecht J, 'Big Problems With Counter Drone Technology (Anti Drone Guns, Drone Jammers, Etc.)' (*Drone Law and Drone Attorney Assistance*, 10 July 2023) <<https://rupprechtlaw.com/drone-jammer-gun-defender-legal-problems/>> accessed 9 April 2024.