Journal of Transportation Security (2019) 12:83–101
https://doi.org/10.1007/s12198-019-00203-0

Civil unmanned aircraft systems and security: The European approach

Mikko Huttunen[1]

Received: 26 February 2019 / Accepted: 30 August 2019 / Published online: 23 September 2019

Abstract

Civil unmanned aircraft systems, commonly known as drones, have many useful applications but can also be used to intentionally cause harm. Additionally, drones themselves can be subject to unlawful interference. In this article, I analyze how European Union's new rules on drones affect such security threats. I argue that the rules on protecting drones from unlawful interference are promising, although the required security features can also be abused by rogue operators. The intentional misuse of drones, however, is not much deterred by the rules that seek to protect persons and property from such misuse. Rules concerning the operator and the pilot assume compliance, the mandatory technical safeguards can be circumvented, and oversight is difficult because drones are mostly operated from outside airports in a distributed manner. One way to fill the security gap is to employ anti-drone technology that detects drones and prevents them from entering sensitive airspace without permission. Although many airports have already adopted such technology, the EU should consider making it mandatory for the busiest airports. Regardless of rules enacted by the Union, though, reliable and safe means of stopping unlawful drone operations should be employed at critical locations. This applies also to areas like prisons and power plants, the protection of which falls within the ambit of national security.

Keywords Unmanned aircraft systems · Remotely piloted aircraft systems · Drones · Security · Aviation law · Air law · European law · European aviation safety agency

Introduction

The use and misuse of drones

Civil[1] unmanned aircraft systems (UAS), which are often called drones,[2] have greatly risen in popularity during the past decade. The rise in popularity is chiefly based on

[1]This article excludes discussion on state aircraft, including for instance "[a]ircraft used in military, customs and police services" (Convention on International Civil Aviation, Art. 3, para. b).

[2]Regarding the choice and meaning of the terms, see my earlier article (Huttunen 2017).

✉ Mikko Huttunen
mikko.huttunen@ulapland.fi

[1] Faculty of Law, University of Lapland, Rovaniemi, Finland

advancements in battery, motor, stabilization, navigation, camera, and sensor technology as well as the globalized economy. This has created a new industry of modern drones that can be used for many purposes, and that are relatively cheap and easy to use. Drones have become a useful tool for professional applications and a popular consumer item for recreational purposes. In fact, millions of drones are sold in Europe alone every year. The estimation is that the amount of drones will increase, and that their technological capabilities will continue to evolve. (EASA 2016a, 8–36. See in detail Desmond 2018, 182–266).

In general, the growing drone industry is viewed as benefiting the society both in terms of professional and recreational use. However, as already noted in the 1944 Convention on International Civil Aviation (Chicago Convention), civil aviation can also be misused, creating a threat to the general security (Preamble, para. 1). In manned aviation, this prophecy has been fulfilled countless times in the form of aircraft hijackings, bombings, and other unlawful acts (for an overview, see e.g. Elias 2010, 1–50; Klenka 2019; Price and Forrest 2016, 45–100; Schiavo 2008; Sweet 2008, 13–36 and 55–104). As unmanned technology improves and the number of drones increases, they too risk threatening security, whether aviation, public, national, or even international security.

Civil UAS, just like manned civil aircraft, can be dangerous to their *environment*.[3] Most notably, drones can be used for acts of terrorism, such as assassination or mass murder. They can be weaponized, piloted to target, deliver explosives, or spread chemical or biological weapons. At least since the 1990s, terrorist groups have acquired and experimented with drone technology of the time. (Rassler 2016, 13–60). For example, the Japanese Aum Shinrikyo cult purchased remote control helicopters in the 1990s for the purpose of spraying sarin gas, though ultimately they resorted to other methods (Olson 1995, 42). A more recent case involved two drones carrying explosives in Caracas, which allegedly was an attempt to attack the president of Venezuela (e.g. Waters and Fiorella 2018). Drones might also be used to bring down manned aircraft (Rassler 2016, 52–54) or trains (Shvetsov and Shvetsova 2017).

Even without terroristic intent, a drone pilot can cause harm to manned aircraft by flying the UAS at an altitude or location not allowed by air law. While the current likelihood of collision appears low (Dourado and Hammond 2016), its effects could be serious according to a study commissioned in the UK (QinetiQ and Natural Impacts 2016). Tests show that recreational drones (that often weigh about 1.5 kg) may not endanger jet engines, but professional ones (7 kg) can (Schroeder et al. 2017; Song et al. 2017). Even the former might severely damage an aircraft wing (Gregg 2018. But see DJI 2018).

At times, such airspace violations can result from pilot error or technical malfunction with the stray drone itself. Recreational and even professional operators can make mistakes, especially since drones are still an emerging and divergent field of aviation (Wild et al. 2016. See generally Wiegmann and Shappell 2003). However, since present drone technology already contains many safeguards to prevent accidental trespass (see e.g. DJI 2019), the bigger threat appear to be unprofessional rogue pilots who deliberately disregard operational limitations.

[3] Here, I use the concept of environment in its broad meaning, referring to all natural and legal persons, property, and circumstances external to the drone.

A typical case of airspace violation is indeed one where the drone is flown in a clearly illegal manner. Consider, for example, proximity reports submitted to the United Kingdom AIRPROX Board (UKAB). In the reports, we find plenty of incidents where a drone has been spotted flying at an altitude greatly above the allowed altitude. For instance, in May 2019 an A320 pilot, while ascending from Gatwick airport, reported a near miss with a drone flying at 3000 ft (UKAB 2019b). In December 2018, particular disorder was caused by a drone flying too close to Gatwick airport, which resulted in about a thousand flights being cancelled. Although the case is still under investigation, as no official report has been published, there are reasons to believe that the act was intentional. (BBC 2019).

Such near misses involving drones have been on the rise: in 2014, just six proximity reports were filed in the UK, whereas there were 125 in 2018 (UKAB 2019a). While the reports have been criticized by the AIRPROX Reality Check for, inter alia, lack of evidence and the fact that many drones have built-in altitude limits (e.g. ARC 2019), such counter-arguments are not too convincing either. It is very difficult for pilots to provide photo evidence of such incidents because they occur so suddenly, and the safety limits of many drones can be bypassed (see NLD 2019). The situation in Central Europe appears similar. For instance, the German air traffic control company Deutsche Flugsicherung (DFS) received 158 proximity reports regarding drones in 2018 (DFS 2019, 27). In the United States of America, the Federal Aviation Administration (FAA) receives over 100 such reports every *month* (FAA 2019).

Drones can also be used for other criminal activities, such as the smuggling of narcotics and other goods. For instance, in the UK in late 2018, a number of men were sentenced for a conspiracy involving drug and mobile phone deliveries into prisons. The deliveries were made using drones to which the items were tied with a fishing line. (Birmingham Crown Court 2018). Smuggling across an international border is another illicit application, of which there are plenty of cases. For example, in 2017 it was discovered that cigarettes were being trafficked across the border between Finland and Russia (Yle 2017. See in detail Finnish Border Guard 2019).

Besides endangering others, drones *themselves* or their payload can also be targeted. This includes both physical and cyber interference, like hijacking, bomb attack, (data) theft, jamming the navigation system, infecting the drone with malware, or denial of service (Altawy and Youssef 2016, 8–14). Naturally, attacking an aircraft is only a security threat in cases where the aircraft or its payload is dangerous or valuable. This is the case with military and police drones (not discussed here) and heavy drones that might cause harm upon impact, as well as certain professional and commercial drone applications, like surveying and passenger transport. Because such applications are only an emerging enterprise (for a recent project, see SESAR 2018) and because the bulk of operations are recreational, involving inexpensive equipment (EASA 2016a, 17), there have been no notable incidents of drones facing unlawful interference. However, this may change in near future as drones become capable of more advanced tasks.

The purpose of this article

A tight legal framework exists to prevent safety and security risks in aviation (see generally Abeyratne 2010; Dempsey and Jakhu (eds) 2017; Havel and Sanchez 2014, 173–216; Huang 2009; Mendes de Leon 2017, 121–124 and 291–361; Milde 2012, 219–

274; Mironenko Enerstvedt 2017; Rossi Dal Pozzo 2015, 55–82). However, this framework, like air law in general, has predominantly been drafted for the purposes of manned aviation. The legal framework for unmanned aviation has only recently begun taking shape in the form of recommendations and rules issued by the International Civil Aviation Organization (ICAO), the FAA, the European Aviation Safety Agency (EASA), and national authorities all over the world (see generally Hodgkinson and Johnston 2018; Masutti and Tomasello 2018; Dulo (ed) 2016; Ravich 2018; Scott (ed) 2016).

Within the European Union (EU), in particular, the most important recent development has been the adoption of the updated EASA Basic Regulation (Regulation (EU) 2018/1139 of the European Parliament and of the Council) in July 2018. The new Basic Regulation, which brings all UAS within the regulatory scope of the Union (Art. 2, para. 1),[4] contains the most essential requirements on UAS. Specific rules are included in the Commission Implementing Regulation (EU) 2019/947 (Implementing Regulation, IR) and Commission Delegated Regulation (EU) 2019/945 (Delegated Regulation, DR), which were adopted during the spring of 2019. At the time of writing this, the three regulations are all in force. However, the IR, which deals with operational rules and procedures, will only apply from the beginning of July 2020. Together, the documents introduce an original regulatory framework that divides operations in terms of risk into three categories (open, specific, and certified) that do not directly distinguish between recreational, professional, and commercial flying.

My main objective in this article is to explore how the new EU rules on UAS address the kind of dangers presented above. To this end, I discuss three regulatory elements: rules concerning the operator and pilot, technical features, and oversight and enforcement. For each element, I outline the traditional approach, contrasting it with the new rules adopted for UAS. The benefits and shortcomings of the new rules are also assessed from the viewpoint of security. In the final chapter, I summarize my findings and consider the necessity of supplementary rules.

Traditionally, air law distinguishes between safety and security. The former refers to the reduction of the possibility of harm (ICAO 2013, ch. 2), while the latter refers to safeguarding civil aviation against acts of unlawful interference (Annex 17 to the Convention on International Civil Aviation 1944; 2011, ch. 1; Regulation (EC) No 300/2008 of the European Parliament and of the Council, Art. 3, para. 2. See in detail Mironenko Enerstvedt 2017, 117–137). Ultimately, safety is about deterring unintentional harm (accidents) and security is about deterring intentional harm (crime), though sometimes the latter has simply been viewed as part of the former (Huang 2009, 5).

This article focuses on security, assessing the new rules from the perspective of intentional rather than unintentional misuse and interference. However, this article does not only concern safeguarding civil aviation but anything that might be affected by the malicious use of drones. Hence, it deals with general security, as referred to in the Chicago Convention. To be specific, it concerns "the perceived or actual ability to prepare for, adapt to, withstand, and recover from dangers and crises caused by people's deliberate, intentional, and malicious acts" (Jore 2017) to the extent drones can pose such dangers and crises.

[4] The previous framework only applied to UAS with a maximum take-off mass of at least 150 kg (see Regulation (EC) No 216/2008 of the European Parliament and of the Council, Annex II, para. 1, subpara. í), to which standards of manned aircraft were applied (see e.g. EASA 2009). Under the new framework, these drones will mostly fall within the certified category of operations.

Since this article discusses air law, it does not analyze security measures enacted in e.g. law pertaining to policing, intelligence, and military. Additionally, since the article is concerned with EU law, I do not discuss comprehensively the developing ICAO standards and recommended practices (SARPs) or pre-existing national rules relating to drone security. However, because the EU rules on certain operations will likely follow ICAO SARPs, some references thereto will be made.

The focus of the article is on prevention rather than punishment. Thus, I will not analyze the application to UAS of aviation crime conventions, including for example the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971; see Bhatti 2016). Although such treaties often contain a provision requiring states to prevent the relevant offences, they mainly focus on ensuring that the perpetrators are duly punished. I also leave out most of the discussion on the security of unmanned air traffic management (ATM), since the exact rules on U-space (the EU's concept of managing drone traffic – see Huttunen 2019b) have not been issued at the time of writing this.

Rules on operators and pilots

Approval and licensing

In air law pertaining to manned aviation, security concerns are tackled in part through rules imposed on the operators and pilots[5] of aircraft. The purpose of such rules is to ensure that aircraft are operated only for legitimate purposes and in a legitimate way, and that aircraft are protected from interference. To this end, operations are subjected to the centralized security control exercised by authorities.

One fundamental institution in this regard is operational approval.[6] In the EU, an operator of aircraft must either acquire an air operator certificate (AOC) or declare its capability to operate safely. Broadly speaking, practicing commercial air transport requires applying for an AOC, while specialized operation (aerial work) requires declaring capability. Both give the operator the permission to conduct air operations and put them under the oversight of the authorities. Only operations that use aircraft outside the jurisdiction of EASA (e.g. certain light aircraft) and non-commercial operations using non-complex aircraft are exempted. (Basic Regulation, Art 2, para. 3, Art. 30, and Annexes I and V. See also Commission Regulation (EC) No 859/2008; Commission Regulation (EU) No 965/2012).

The requirements for UAS follow a similar but not the same approach. Drone operators, regardless of the purpose of the operation (recreational flying, aerial work, etc.), must first of all register themselves, when operating an aircraft exceeding certain thresholds. Since these thresholds are very low, including for instance any drone which presents a risk to privacy or security, virtually all operators are subject to registration. (Basic Regulation, Annex IX, para. 4.2. See also Masutti and Tomasello 2018, 73–79). Beyond registration, the necessary procedure depends on the category of operations, of which there are three: open, specific, and certified (Implementing Regulation, Art. 3).

[5] Rules concerning other crewmembers are not discussed here.

[6] Here, I use approval as an umbrella term that refers to certification, registration, operational authorization, and the declaring of capability.

This categorization and the rules that follow therefrom are based on the risks of the operation, not its purpose (see originally EASA 2015, 17–31).

The open category involves the lowest risk, thus incorporating the majority of recreational and simple professional applications, like aerial photography over non-crowded locations. In the open category, no procedure beyond registration is required. One can simply purchase a drone that meets the criteria and fly it, as long as the relevant rules are followed. For example, the category restricts the maximum take-off mass of the drone (25 kg) and only allows flying within the visual line of sight (VLOS) of the pilot. Operations are further divided into three subcategories (A1–A3). (Implementing Regulation, Arts 3–4 and 7 and Annex. See also Masutti and Tomasello 2018, 79–87).

The specific category, meanwhile, is designed for more complex operations, like inspections, surveying, and filming over crowds. Therein, one must acquire an operational authorization, based on a risk assessment, which dictates the requirements of safe flying; in the case of a standard scenario (a recognized set of operational parameters), however, the operator only needs to declare competency. Currently, the most prominent method of risk assessment is the Specific Operations Risk Assessment (SORA). Operators can also apply for a light UAS operator certificate (LUC), which entails certain benefits at the cost having to comply with more rigorous requirements. The certified category includes the most professional types of aerial work and human transportation. Accordingly, such operations are subject to air operator certification, like in manned aviation. (Implementing Regulation, Arts 3, 5–7 and Annex; JARUS 2019. See also Huttunen 2019a; ICAO 2015, sec. 6.3; Masutti and Tomasello 2018, 79–87).

With regard to pilots, the most important security measure is licensing. The objective of licensing is that only trained personnel can fly aircraft. The approach in manned aviation has been to require virtually all pilots to acquire a license and the necessary ratings to fly (Basic Regulation, Art 20–21 and Annex IV; Commission Regulation (EU) No 1178/2011). Here, too, the new drone rules mimic manned aviation. According to the Basic Regulation, any person involved in drone operations must have the knowledge and skills required by safe operation, and also demonstrate medical fitness, if it is necessary for mitigating risks (Annex IX, paras 1.1 and 2.3).

When it comes to exact qualifications, the risks of the operation are again the decisive factor. Simple operations follow a more lenient approach than with regular pilots. In the open category, the pilot is usually just required to complete an online training course and pass a theoretical examination.[7] At the higher end of the spectrum, conversely, the certified category will follow training requirements similar to manned aviation. Between these two extremes there is the specific category, where the required competence depends on a case-by-case risk assessment. (Implementing Regulation, Art. 8 and Annex. See also ICAO 2015, ch. 8; Masutti and Tomasello 2018, 97–110).

In manned aviation, operational approval and the licensing of pilots act as a deterrent to intentional misuse. While it is possible to fly without the proper paperwork, several factors make it somewhat difficult. Manned aircraft commonly require at least an airstrip to operate from and facilities for maintenance, which makes them an easy target for aviation and police authorities. The necessity of flight training, the cost of qualification, and the cost of aircraft also obstruct the use of manned aircraft for illegal

[7] As of now, some private bodies are already offering training courses (see e.g. NLR 2019).

purposes. Besides, manned aircraft can be easily identified both visually and using radar equipment. The identity of the pilot is easy to discover because (s)he is always on board the aircraft.

With civil drones, however, registration and licensing present less of an obstacle to malicious acts. Many drones are cheap and can be operated without training and covertly from anywhere. They are often difficult to identify remotely due to their small size and lack of a transponder. Therefore, approval at the organizational level will probably only be pursued by law-abiding recreational and professional operators. The same goes for the licensing of pilots. Rogue operators and pilots can easily ignore such rules without fear of punishment, which for example the aforementioned Gatwick incident demonstrates. Although criminals might play along to deceive authorities, in the end they do not care about permits. The threat of using drones in malicious acts thus remains mostly unaffected by means like registration, which assume compliance. Indeed, EASA has recognized that focusing solely on the responsibility of the remote pilot may lead to security threats, and that licensing is insufficient as the sole safety barrier (EASA 2017, 76–77 and 82). Ultimately, coercive measures are necessary to ensure the secure use of drones.

Operational rules

Besides acquiring the necessary qualifications, operators and pilots must follow a set of operational rules. These rules establish the appropriate procedures for the operation of aircraft, which is another component of secure aviation. The most fundamental of such rules are shared between manned and unmanned aviation. For instance, the rules call for pilots to maintain an appropriate separation between aircraft and obstacles, to respect limitations relating to areas and aerodromes, and to follow communication procedures. (Basic Regulation, Annex V, sec. 3, para. d and Annex IX, paras 1.1 and 2.4.1–2.4.4). In terms of detailed rules, operators and pilots of manned aircraft must comply with regulations that cover everything from flight planning to the carriage of weapons on board. Some of the rules depend on the category of operations, such as commercial air transport and specialized operations. (Commission Regulation (EU) No 965/2012; Commission Regulation (EU) No 923/2012).

The operational rules on drones are similar, although they rely on the open-specific-certified categorization. The rules of the open category, for example, limit the areas where the drone can fly, the distance of the drone from the pilot, and the payload of the drone. The rules also demand the operator to develop procedures and ensure the competence of the personnel, while the pilot is responsible for obtaining updated information about zones and observing the environment. Naturally, the duties become more stringent as we progress to the specific category, where the risk assessment determines the requirements. It is worth observing that, in the specific category, the operator must establish procedures to ensure that security requirements applicable to the area of operations are taken into consideration. At the certified level, the rules that are currently under development will be similar to those applied to manned aviation. (Implementing Regulation, Art. 7 and Annex. See also ICAO 2015, ch. 9; Masutti and Tomasello 2018, 136–152).

The aforementioned rules may discourage the willful misuse of manned aircraft, but not so much the misuse of unmanned aircraft. The reasons for this are similar to the

ones listed above regarding operational approval and the licensing of pilots. The operational environment and technology of manned aircraft provide measures to control the observance of rules pertaining to matters like separation, altitude, and equipment. Malicious drone pilots can ignore such rules, since UAS can be operated from almost anywhere and since they often cannot be remotely identified. In order to intervene with an operator or a pilot who disobeys their duties, the authorities must discover not just the drone but also the pilot who might be flying the aircraft from a great distance. This being difficult, authorities ought to be provided with means to stop drones right when it is necessary.

Securing the aircraft

Operators and pilots are also required to comply with rules that seek to protect aircraft from external threats. In the case of manned aviation, for instance, commercial operators and non-commercial operators using complex aircraft must establish security programmes. These concern e.g. the security of the flight crew compartment (cockpit), aircraft search procedures, and the protection of systems from electronic interference. (Basic Regulation, Annex V, para. 8.4). Operators must also establish procedures (like training and instructions) to secure potentially disruptive passengers and especially maintain a sterile cockpit, preventing unnecessary and unauthorized admission. (Commission Regulation (EU) No 965/2012, Annex I, para. 109a and ORO.GEN.110, para. f. See also Regulation (EC) No 300/2008, Annex, ch. 10).

The open category of drone operations does not require the operator to secure the UAS itself. In the specific category, meanwhile, the operator must establish measures to protect against unlawful interference and unauthorized access (Implementing Regulation, Annex, UAS.SPEC.050). Since the required measures must correspond with the intended operation and risk, it seems likely that they will only be required in operations where the drone or its payload is either dangerous or valuable. Carrying passengers will fall within the certified category, where the requirements concerning UAS security will mainly be set forth in Commission Regulation (EU) No 965/2012 (Implementing Regulation, Art. 7, para. 3).

The exact nature of compulsory security measures in specific operations sadly remains unknown, as they will depend on the operation. The SORA, which is to be used for specific category risk assessment, does not cover security aspects (JARUS 2019, 12). The rules on the certified category will likely follow the SARPs being developed within ICAO. In practice, protection will probably entail guaranteeing the security of the system (cybersecurity), the crew, the aircraft, and the remote pilot station (physical security), as these components provide the access spot for interference. For example, the operator may be required to ensure that the drone is stored in a secure location and that the number of people who can access the system is limited. This is crucially important in cargo transport and even more so in passenger transport, where standards should be no lower than in manned aviation. (See ICAO 2015, para. 9.11; Masutti and Tomasello 2018, 168–174).

In securing the UAS itself, compliance can be assumed, since it is in the interest of legitimate operators (both recreational and professional) to protect their equipment and payload. Requirements should therefore stem from a public interest to secure the drone. This is the case when there is a risk that somebody wants to interfere with the drone in

order to steal it or its payload, or cause harm by bringing it down. From this perspective, it is acceptable that the operator has no obligation to take special measures to secure the UAS in the open category, since the category limits the mass and payload of the drone. Sufficient security from interference like jamming can be achieved through the operator's own volition and technical features. In the other two categories, which involve e.g. heavier equipment, flying over crowds, and transportation, it is appropriate that the rules require the operator to ensure protection from interference. It reduces the risk of passengers and outsiders being harmed. At this stage, though, it is difficult to assess what degree of management will be sufficient in ensuring security.

Technical features

Airworthiness, identification, and geo-awareness

In addition to operational requirements, air law ensures security through technical features. In comparison with centralized means of control, like pilot licensing, technical features are decentralized. Manufacturers are responsible for installing the required equipment into each aircraft. Technical security features rely less on the compliance of the operator and the pilot. While malicious pilots may purposefully ignore provisions of air law, the restrictions embedded into the aircraft can still deter them from causing harm. This goes particularly for recreational pilots who lack the expertise of professionals. This is partly why EASA has stressed the importance of technical standards in the regulation of drones (EASA 2017, 37–39).

As a general requirement, every aircraft used in aviation must be airworthy. This means that their design must be certified (type certification), and that the airworthiness of every individual aircraft is initially approved and continuously maintained. As an example of airworthiness, the aircraft must have structural integrity and functioning navigation equipment. (Basic Regulation, Arts 9–14 and Annex II; Commission Regulation (EU) No 748/2012; Commission Regulation (EU) No 1321/2014. Of airworthiness in detail, see Florio 2011). For identification, many types of aircraft must be equipped with a transponder (Commission Regulation (EU) No 965/2012), and the EU also aims to equip a sizeable portion of all aircraft with automatic dependent surveillance-broadcast (ADS-B) technology (Commission Implementing Regulation (EU) No 1207/2011).

Like manned aircraft, drones must be provided with product integrity, including proper materials and components, and manufactured so that they do not put persons at risk in any anticipated conditions. If necessary to mitigate risks, including security risks, the aircraft is required to have the corresponding features and functionalities. The rules on specific and certified drone operations mimic pre-existing air law, necessitating airworthiness certification for drones exceeding particular thresholds. The actual airworthiness criteria for certified drones are only under development, however. It is worth noting that certified UAS that operate on protected aviation frequencies must not disturb the communications equipment of other airspace users. For drones that need not be certified, the specific category establishes airworthiness standards on a case-by-case basis through the risk assessment procedure, or a standard scenario. Drones in the open category follow a different approach, since they are treated as products. They are

segregated into five classes (C0–C4), each with its own level of standards. (Basic Regulation, Annex IX, paras. 1.2, 1.3, and 2.1.1–2.1.8; Delegated Regulation, Arts 4–6 and 40, and Annex. See also ICAO 2015, ch. 4; Masutti and Tomasello 2018, 111–135).

With identification, the EU drone rules take a distinct approach. Instead of a transponder, every drone in the open category, excluding class C0, must be equipped with a remote identification and geo-awareness system. The former must broadcast data from the drone, using an open and documented transmission protocol. It enables authorities to identify the operator and the drone, as well as the position and heading thereof. The user must not be able to modify the data concerning the serial number, position, and route of the drone and the position of the pilot. The geo-awareness system must warn the pilot when the drone is vertically or horizontally heading toward any segment of airspace where the drone is not allowed to fly. (Basic Regulation, Arts 55–57 and Annex IX, para. 4.3; Delegated Regulation, Annex, Parts 2–6. Of geo-awareness in detail, see EASA 2016b).

Whether remote identification, geo-awareness, or similar features are required in the specific category, depends on the risk assessment. In many cases there is likely a need for such measures, given the inherently higher risk of specific operations. Similar features would also provide a common basis for e.g. dynamic airspace information, electronic flight planning and tracking, and automatic detect and avoid (DAA) functionalities (see Huttunen 2019b, 80–87). The same goes for certified operations, although such will probably also incorporate equipment, like a transponder, that interfaces with the pre-existing systems of manned aviation. (See ICAO 2015, ch. 14; Masutti and Tomasello 2018, 136–152). As the risks of the operation increase, more stringent safeguards are needed.

From the perspective of intentional misuse, both remote identification and geo-awareness are problematic. The former depends on the operator entering their registration number into the UAS, since there is no requirement to bind the drone to the user at the moment of purchase. Although the drone may broadcast the required data, its operator might be unknown. The problem with geo-awareness is that is does not automatically prevent a drone from violating airspace. A pilot may deliberately ignore the warning and fly on. This shifts the responsibility again on the operator and the pilot, reducing the perceived likelihood of punishment for wrongdoings conducted using the drone. The features prescribed in the rules, regardless of the category they are employed in, are rather ineffectual in preventing security threats.

To be sure, neither remote identification nor geo-awareness are new features. Such systems, and other innovations like automatic return upon loss of control, are already employed in many consumer-grade drones. In fact, many drones employ not only geo-awareness but geofencing, which prevents the drone from entering the airspace near e.g. airports and prisons. The maximum altitude is also limited. DJI, the world's leading drone manufacturer (Skylogic Research 2019), has announced that from January 2020 it will also install ADS-B positioning technology in all new drones whose weight exceeds 250 grams. This will enable their drones to interface with manned aircraft and ATM equipped with the same technology. (DJI 2019). The security features of many drones are thus already much more advanced than the rules require.

The remaining issue is, however, that even geofencing and other compulsory restrictions are never completely secure. Drones, as an emerging and digital technology,

are very susceptible to tampering. Although the rules require the manufacturer to ensure that key identification data is not falsified by the user, the latter might find a way to circumvent the feature, making discovery impossible. The same goes for geofencing. Indeed, there already exists a website for removing built-in restrictions on drones (see NLD 2019), which may tempt casual pilots and even professionals to go rogue. We must also consider the fact that there are probably millions of drones out there, including outdated and self-assembled ones, whose security mechanisms are rudimentary at best. Hence, to guarantee security, decentralized technical measures should be supplemented with centralized means of enforcement, which can halt drones that are being used harmfully.

Protection from interference

Air law imposes on manned aircraft many technical features that shield them from external harm. Again, the rules focus on protection from hijacking, emphasizing the security of the cockpit. Pursuant to the general rule, the cockpit must be lockable and the crew must be able to notify the pilots of suspicious activity (Commission Regulation (EU) No 965/2012, ORO.SEC.100). To give a more specific example, the flight deck of large aircraft, when required by operating rules, must especially be protected against forcible intrusion and arms penetration. With certain aircraft, especially large aircraft, airworthiness requires for example smoke protection, fire suppression, and systems that withstand distress. (EASA 2018, CS 25.795).

The technical provisions on drones also consider the threat of interference. In the open category, the command and control functions of the data link of Class C2 and C3 drones must be protected against unauthorized access (Delegated Regulation, Annex, Parts 3 and 4). Because specific operations represent a higher risk, operations falling within that category will likely also have to incorporate similar protection. For certified operations, the existing airworthiness policy for drones already calls for protecting the link from electromagnetic interference, though security aspects per se were not viewed as falling within EASA's competence (EASA 2009, paras 7.2 and 8.6. See also Boccardo 2016, 139–142; Masutti and Tomasello 2018, 119–120). Obviously, however, new standards going beyond such policy are being drafted. In this, the EU rules will likely follow ICAO's SARPs (see ICAO 2015, para. 13.4.5; Jeyakodi 2016, 70–74; Masutti and Tomasello 2018, 169–174).

The particular technical features required in specific and certified operations, apart from the aforementioned, are yet undefined and thus difficult to appraise. The starting point is, of course, that the features must correspond with operational rules, as discussed above. It is also safe to assume that not only the datalink but the whole system has to be protected both physically and in terms of hardware and software (see Jeyakodi 2016, 75–77). Particularly in human transport, the functioning of the features must be guaranteed. Some exemplary features include access authentication, cross checking observables, intrusion detection, data link and telemetric channel encryption, firewalls, and hardware and software authentication. Features like digital signature and logging, similar to flight recording used in large manned aircraft, would provide accountability. (Altawy and Youssef 2016, 14–16).

On one hand, the rules prescribing protective features for drones enhance the ability of legitimate operators to secure their equipment. This is in line with the interests of

operators (particularly professional ones) as well as the general public, at least in cases where there is a risk of interference. The regulatory effort to protect drones is thus laudable, especially since drones are an easy target for interference (Altawy and Youssef 2016, 1–2). On the other hand, security features also protect malicious operators. While features like control encryption are aimed at safeguarding authorized flying, they can equally be abused to prevent authorities from using anti-drone equipment. This prospect is particularly alarming when it comes to acts of terrorism. Securing the drone is thus a double-edged sword. The only counter to this would be to provide the authorities with tools that bypass the drone's security features when the aircraft is used maliciously. This would retain the protection of legal operators but enable interfering with illegal ones.

Oversight and enforcement

Joint responsibility

In the European Union, overseeing and enforcing air law is under the joint responsibility of the European Commission, EASA, and national competent authorities (NCAs) designated by each EU Member State (MS).[8] The Commission has the obligation to inspect certain aspects of airport and operator security (Regulation (EC) No 300/2008, Art. 15), but otherwise the Agency and NCAs hold a more prominent role. Oversight is thus quite centralized, albeit EU law allows the latter two bodies to delegate certain tasks to other parties by accrediting them as qualified entities (Basic Regulation, Art. 69).

According to the Basic Regulation, the Agency and NCAs must exercise oversight over all manned and unmanned operators and pilots, aircraft and related equipment, and other matters subject to the Regulation. In cases of airspace violation, for example, they are obliged to conduct an investigation and inspections, also taking all necessary enforcement measures to end such violations. (Arts 62–93). This capacity of oversight and inquiry commonly extends to the specific requirements enacted in other regulations based on the Basic one. In manned aviation, organisations having their principle place of business in an EU MS are generally under the oversight of the NCA designated by the MS, while EASA is responsible for EU level oversight and operators based in non-member states (e.g. Commission Regulation (EU) No 748/2012, Annex I, para. 21.1).

In unmanned aviation, the competence of each NCA comprises operations within the respective MS. NCAs have the authority to issue, suspend, and revoke operational authorizations, declarations, and LUCs (specific category), operator certificates (certified category), as well as documents concerning pilot competence. In the specific category, the NCA is responsible for validating the operator's risk assessment. Besides that, they have to keep records of operations and pilots; develop an oversight system for operators outside the open category; establish audit planning; inspect operators and their drones; and implement a system for violations. To provide assistance, the NCAs must also make available information on local conditions and geographical zones, and provide operators with safety guidance. (Implementing Regulation, Art. 18).

[8] Most commonly, NCAs include the national aviation authority (NAA) and the authority in charge of investigating air incidents.

In the open category of operations, the security of drones relies also on authorities and bodies responsible for product conformity assessment, as described in the Delegated Regulation. The obligation for the assessment of class C0 drones lies solely on the manufacturer itself. Meanwhile, for class C1–3 the manufacturer must choose between an EU-type examination or a full quality assurance procedure. These procedures involve not only the manufacturer but also an EU-notified conformity assessment body, who must examine the documentation and test the product specimen. (Art. 6, para. 2 and Art 13, para. 2. See in detail Annex, Parts 7–9.).

In manned aviation, oversight and enforcement is facilitated by several factors. As explained in more detail above, manned aircraft are generally identifiable and bound to take off from at least an airfield, which puts them under the scrutiny of other operators and authorities. It is thus easier to prevent illegal operation, although of course hazards cannot be completely avoided. Meanwhile, overseeing unmanned aviation is difficult because of its distributed mode of operation. Finding the pilot behind an unlawful drone operation is extremely hard, as it often requires scouring large areas of land. Hence, in cases where only the drone can be located, stopping it forcefully is the only way to enforce the law.

Airport security

The described discrepancy is widened by the fact that many EU rules on security, based on Annex 17 to the Chicago Convention (2011), focus on aircraft that operate from an airport (see Masutti and Tomasello 2018, 162). According to these rules, airports operate partly as security restricted areas, access to which is limited and controlled with security checks. This is to prevent unauthorized people and vehicles from entering vulnerable locations, like aircraft themselves or taxiways. Most noticeably, airports only allow departing passengers, crewmembers, airport staff, or personnel with other valid authorisation to enter the airside. Surveillance or patrols must be undertaken, among other things, to monitor the boundaries of restricted areas. (Regulation (EC) No 300/2008, Annex, sec. 1.1, 1.2, and 1.5; Commission Implementing Regulation (EU) 2015/1998, Annex, sec. 1.1.2–1.1.3, 1.2.2, and 1.5. See also Rossi Dal Pozzo 2015, 71–76). These restrictions apply to unmanned aviation in principle, but they do not improve drone security much, since most drones operate from outside airports.

The same goes for rules on screening. Airport security uses metal detectors, x-ray machines and other means to scan for prohibited items like weapons, explosives, and drugs. This screening targets all passengers, their cabin baggage, everyone's hold baggage, vehicles, mail, and cargo that enter a security restricted area. Meanwhile, crewmembers of aircraft are subject to a background check before they are issued any identification that authorizes their access. Aircraft themselves are searched in certain cases, and there are procedures to protect them against unauthorized access. Such include e.g. proper checking of persons seeking access, keeping external doors closed, and having electronic means to detect access. (Regulation (EC) No 300/2008, Art. 3, para. 15 and Annex, sec. 1.2–1.4 and ch. 3–6; Commission Implementing Regulation (EU) 2015/1998, Annex, sec. 1.4 and ch. 3–6; Commission Regulation (EC) No 272/2009, Annex. See also Leloudas 2017, 170–177; Rossi Dal Pozzo 2015, 77–81). Most drones, including their payload and crewmembers, fall outside the scope of such means.

The overall effects of this should not be overestimated, since oversight and enforcement do not wholly depend on measures taken at airports. Potential terrorists and criminals, like drug traffickers, are already monitored by intelligence agencies and the police before they enter any airport (see e.g. Sweet 2008, 105–144; Mironenko Enerstvedt 2017, 205–305). Drone operators are not immune to such oversight. Furthermore, airport security measures are themselves far from perfect (see Thomas 2003). Still, missing out on the procedures means that drones are left out of the "the last line of defense" (Sweet 2008, 145) in aviation security, which increases the risk of them being used for malicious purposes.

This issue cannot really be solved by subjecting all UAS to airport security. Most drones do not have the equipment to operate in controlled airspace surrounding airports, and not allowing drones to take off from any suitable location would deal a death blow to the industry. Flexibility is a key characteristic of drones, enabling them to be used immediately at remote locations without transiting first from an airport. It makes drones a convenient choice for legitimate professional and commercial missions, such as inspecting power lines, as well as recreational flying. If the benefits of drones are to be retained, alternative mechanisms of oversight and enforcement are necessary to deal with intentional misuse.

Conclusions

From the perspective of security, European Union's new legal framework on UAS relies on both innovation and tradition. The main difference with the rules on manned aviation is the categorization of operations into open, specific, and certified. The open category, which comprises mainly recreational and simple professional operations, employs less stringent security measures than the latter two categories, which include more complex cases. In the specific category, measures depend on a case-by-case risk assessment, while rules for certified operations aim to match the security level of manned aviation. Despite this novelty, many rules are notably inspired by pre-existing regulations. Operators must register themselves and pilots acquire a licence before beginning operation, and in some cases take measures to protect the UAS against physical and electronic interference. Manufacturers must equip drones with technical features that protect both outsiders as well as the drone itself. In oversight and enforcement, the rules rely mainly on national authorities and product conformity bodies.

The rules pertaining to the security of the UAS itself are generally appropriate and beneficial. The protection of legitimate drone operators and the people who use their services must be ensured, especially in air carriage. The only inevitable problem lies with protective features, which can be abused by rogue operators. Furthermore, as of now it is unclear what exact protective means will have to be employed in the specific and certified category.

The other new rules, however, are not very useful in preventing the intentional misuse of UAS, since they assume the compliance of the end user. Due to the distributed nature of unmanned flying, it is often virtually impossible to apprehend covert operators and verify the legitimacy of their operation. Therefore, the obligation to register or acquire a license does not hinder rogue operators or pilots from breaking the law. The same problem persists with the technical features required by the rules.

Remote identification and geo-awareness, in particular, have little deterring effect because they rely on the operator to input data and take corrective action. Both features actually lag behind, since manufacturers are already installing more rigorous systems on their drones. However, it is questionable whether even geofencing and ADS-B are immune to hacking, and there are already millions of low security drones flying around.

A peculiar problem with overseeing UAS is that many aviation security measures are targeted at aircraft and people that operate from airports. This includes both general oversight as well as measures specifically designed to prevent threats like hijacking and the use of explosives. Because drones are operated mostly from outside airports, they almost always fall outside the scope of such measures. Since intelligence agencies and police authorities still monitor dangerous individuals, the issue should not be exaggerated. Yet, incidents like the Gatwick one clearly call for measures that work independently of compliance, the features of the drone, and regular airport security.

Perhaps the most appropriate solution to filling the security gap in the rules is anti-drone technology that detects drones and prevents them from entering sensitive airspace without permission. The advantage of such technology is that it can be employed almost anywhere and that it also deters operators who willfully fly against the rules and have managed to bypass the protective features of the drone. Anti-drone technology is already available and employed as radars, which use optical and thermal sensors to detect drones, and jammers that disrupt the data link between the drone and its controller. There are also portable blasters that can disable or alter the course of unwanted drones. (See Simmons 2018). In the past two years, many airports have indeed invested in anti-drone systems (Berti 2019), and so have some prisons (Bannister 2018).

As of now, there are no plans to issue rules requiring EU Member States to adopt anti-drone technology. When it comes to airspace above places like prisons, proving grounds, official residences, and power plants, EU lacks jurisdiction. The same goes for situational protection, such as that required during state visits. Establishing prohibited and restricted airspace falls within the ambit of national security (see Chicago Convention, Art. 9), which according to the Treaty on European Union (2016) is the sole responsibility of the MSs (Art. 4, para. 2). This is hinted at in the Basic Regulation, according to which nothing prejudices the competence of Member States to enact national rules that subject the operation of UAS to certain conditions for reasons of e.g. public security, which fall outside the scope of the Regulation (Art. 56, para. 8). Hence, it is up to domestic authorities to determine which locations and cases require anti-drone equipment.

In the case of airports, too, it has been argued that protecting national security from UAS is mainly a task for (national) police and military authorities rather than aviation authorities (Masutti and Tomasello 2018, 168). However, Regulation (EC) No 300/2008 already shows that the EU has the competence to create Union-wide rules on airport security. Restricting access, conducting screenings, and protecting aircraft from unauthorized access are of vital importance to security, both European and national. Since anti-drone solutions are hardly a more extensive measure than those already in place at airports, it seems unfounded to argue that the Union has no mandate to legislate security problems caused by UAS. Nonetheless, the legislative procedure would have to address the restrictions many countries have on the use of radio frequency jammers (e.g. UK Wireless Telegraphy Act 2006, Part 3, sec. 68).

A possible safety issue with anti-drone systems, as pointed out by EASA, is that they might disturb the aeronautical communications and data systems used by manned aircraft. This concern is obviously shared by the aviation industry. Due to the risk of impairing aviation safety, the Agency noted in 2017 that careful consideration is necessary before any steps are taken. (EASA 2017, 35). There is value in being careful, since we still lack profound experience of using the technology. Pursuant to current experience with multiple systems across the world, though, anti-drone equipment presents no threat to the safety of manned aviation. Still, the safe use of the equipment necessitates training.

Of course, airports might also oppose an obligation to invest in anti-drone equipment. It seems, however, that the investment in the technology is quite less expensive than the human, financial, and reputational costs of mass delays, let alone an accident (see Berti 2019). The crucial task in this regard, though, would be determining the criteria that would trigger the obligation to acquire a system. The most obvious threshold that comes to mind is the amount of air traffic handled by the airport, but pinpointing the exact figure would necessitate careful consideration. Enacting the provision might also require determining which type of a system would be sufficient for an airport that handles a particular amount of traffic. Possibly, the technical standards of the equipment would also have to be certified.

Whether it is necessary or useful to require airports to acquire an anti-drone system, is a worthwhile debate. It would appear that airports are smart and prudent enough to protect aviation without any legal obligation to do so. Still, given the looming threat of mass delays and mid-air collision, it might be appropriate to make anti-drone equipment a mandatory feature at the busiest airports within the EU. After all, security is not only about managing real threats, but also social perceptions (Leloudas 2017, 163). No matter what the Union decides to do, though, public and private stakeholders should continue developing solutions to address the security risks of drones. This includes particularly aviation, police, and military authorities as well as the management of airports, prisons, and power plants. Reliable and safe means of detecting and stopping unlawful drone operations should be employed at critical locations. To this end, MSs could engage in cooperation both operationally and in terms of funding, research, and training.

Funding Information Open access funding provided by University of Lapland.

References

Abeyratne RIR (2010) Aviation security law. Springer, Heidelberg

Altawy R, Youssef AM (2016) Security, privacy, and safety aspects of civilian drones: a survey. ACM Transactions on Cyber-Physical Systems 1(2):7

Annex 17 to the Convention on International Civil Aviation: Security – Safeguarding International Civil Aviation against Acts of Unlawful Interference, 9th edition, Montreal, March 2011

ARC (2019) June 2019. https://www.airproxrealitycheck.org/june-2019/. Accessed 5 August 2019

Bannister A (2018) Pioneering anti-drone system installed at Guernsey prison. https://www.ifsecglobal.com/global/pioneering-anti-drone-system-installed-guernsey-prison/. Accessed 21 August 2019
BBC (2019) Gatwick drone attack possible inside job, say police. https://www.bbc.com/news/uk-47919680 . Accessed 21 August 2019
Berti A (2019) Gatwick drone crisis: what can we learn from December's fiasco? https://www.airport-technology.com/features/gatwick-drone-impact/ . Accessed 21 August 2019
Bhatti Y (2016) Criminal liability. In: Scott BI (ed) The law of unmanned aircraft systems. Kluwer Law International, Alphen aan den Rijn, pp 79–88
Birmingham Crown Court (2018) Case T20187209
Boccardo G (2016) European aviation safety agency. In: Scott BI (ed) The law of unmanned aircraft systems. Kluwer Law International, Alphen aan den Rijn, pp 135–152
Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems
Commission Implementing Regulation (EU) 2015/1998 of 5 November 2015 laying down detailed measures for the implementation of the common basic standards on aviation security
Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft
Commission Implementing Regulation (EU) No 1207/2011 of 22 November 2011 laying down requirements for the performance and the interoperability of surveillance for the single European sky
Commission Regulation (EC) No 272/2009 of 2 April 2009 supplementing the common basic standards on civil aviation security laid down in the Annex to Regulation (EC) No 300/2008 of the European Parliament and of the Council
Commission Regulation (EC) No 859/2008 of 20 August 2008 amending Council Regulation (EEC) No 3922/91 as regards common technical requirements and administrative procedures applicable to commercial transportation by aeroplane
Commission Regulation (EU) No 1178/2011 of 3 November 2011 laying down technical requirements and administrative procedures related to civil aviation aircrew pursuant to Regulation (EC) No 216/2008 of the European Parliament and of the Council
Commission Regulation (EU) No 1321/2014 of 26 November 2014 on the continuing airworthiness of aircraft and aeronautical products, parts and appliances, and on the approval of organisations and personnel involved in these tasks
Commission Regulation (EU) No 748/2012 of 3 August 2012 laying down implementing rules for the airworthiness and environmental certification of aircraft and related products, parts and appliances, as well as for the certification of design and production organisations
Commission Regulation (EU) No 923/2012 of 26 September 2012 laying down the common rules of the air and operational provisions regarding services and procedures in air navigation and amending Implementing Regulation (EU) No 1035/2011 and Regulations (EC) No 1265/2007, (EC) No 1794/2006, (EC) No 730/2006, (EC) No 1033/2006 and (EU) No 255/2010
Commission Regulation (EU) No 965/2012 of 5 October 2012 laying down technical requirements and administrative procedures related to air operations pursuant to Regulation (EC) No 216/2008 of the European Parliament and of the Council
Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (Montreal Convention). Adopted 23 September 1971, 974 UNTS 177
Convention on International Civil Aviation (Chicago Convention). Adopted 7 December 1944, 15 UNTS 295
Dempsey PS, Jakhu RS (eds) (2017) Routledge handbook of public aviation law. Routledge, Abingdon
Desmond K (2018) Electric airplanes and drones: A history. McFarland & Company, Jefferson, North Carolina
DFS (2019) Geschäftsbericht 2018
DJI (2018) DJI Demands Withdrawal of Misleading Drone Collision Video. https://www.dji.com/fi/newsroom/news/dji-demands-withdrawal-of-misleading-drone-collision-video . Accessed 5 August 2019
DJI (2019) Elevating safety: Protecting the skies in the drone era
Dourado E, Hammond S (2016) Do consumer drones endanger the national airspace? Evidence from wildlife strike data. Mercatus Center, George Mason University, Arlington and Fairfax, Virginia
Dulo DA (ed) (2016) Unmanned aircraft in the national airspace: Critical issues, technology, and the law. American Bar Association, Chicago, Illinois
EASA (2009) Policy statement E.Y01301: Airworthiness certification of unmanned aircraft systems (UAS)
EASA (2015) Advance notice of proposed amendment 2015–10: Introduction of a regulatory framework for the operation of drones

EASA (2016a) European drones outlook study: Unlocking the value for Europe
EASA (2016b) Study and Recommendations regarding Unmanned Aircraft System Geo-Limitations
EASA (2017) Notice of proposed amendment 2017–05 (B): Introduction of a regulatory framework for the operation of drones
EASA (2018) Certification specifications and acceptable means of compliance for large aeroplanes (CS-25), Amendment 22
Elias B (2010) Airport and aviation security: U.S. policy and strategy in the age of global terrorism. Taylor & Francis, Boca Raton, Florida
FAA (2019) UAS sightings report. https://www.faa.gov/uas/resources/public_records/uas_sightings_report/. Accessed 8 August 2019
Finnish Border Guard (2019) Pretrial Protocol 9182/R/1892/17
Florio, F De (2011) Airworthiness: An Introduction to Aircraft Certification, 2nd edition. Elsevier, Oxford
Gregg P (2018) Risk in the sky? https://udayton.edu/blogs/udri/18-09-13-risk-in-the-sky.php. Accessed 5 August 2019
Havel BF, Sanchez GS (2014) The Principles and Practice of International Aviation Law. Cambridge University Press, Cambridge
Hodgkinson D, Johnston R (2018) Aviation law and drones: Unmanned aircraft and the future of aviation. Routledge, Abingdon
Huang J (2009) Aviation safety through the rule of law: ICAO's mechanisms and practices. Kluwer Law International, Alphen aan den Rijn
Huttunen M (2017) Unmanned, remotely piloted, or something else? Analyzing the terminological dogfight. Air & Space L 42(3):349–368
Huttunen M (2019a) Drone operations in the specific category: A unique approach to aviation safety. The Aviation & Space Journal 13(2):2–21
Huttunen M (2019b) The u-space concept. Air & Space L 44(1):69–89
ICAO (2013) Doc 9859: Safety management manual (SMM), 3rd edition
ICAO (2015) Doc 10,019: Manual on remotely piloted aircraft systems (RPAS)
JARUS (2019) Guidelines on specific operations risk assessment (SORA), 2nd edn
Jeyakodi D (2016) Cyber security. In: Scott BI (ed) The law of unmanned aircraft systems: an introduction to the current and future regulation under national, regional and international law. Kluwer Law International, Alphen aan den Rijn, pp 67–77
Jore SH (2017) The conceptual and scientific demarcation of security in contrast to safety. Eur J Secur Res 4(1):157–174
Klenka M (2019) Major incidents that shaped aviation security. J Transp Secur 12(1–2):39–56
Leloudas G (2017) In: Dempsey PS, Jakhu RS (eds) Domestic regulation of security: The example of the European Union. Routledge Handbook of Public Aviation Law, Routledge, Abingdon, pp 162–179
Masutti A, Tomasello F (2018) International regulation of non-military drones. Edward Elgar, Cheltenham
Mendes de Leon P (2017) Introduction to air law, 10th edn. Kluwer Law International, Alphen aan den Rijn
Milde M (2012) International air law and ICAO, 2nd edn. Eleven International Publishing, The Hague
Mironenko Enerstvedt O (2017) Aviation security, privacy, data protection and other human rights: Technologies and legal principles. Springer, Cham
NLD (2019) NLD MOD client. https://nolimitdronez.com/ . Accessed 5 August 2019
NLR (2019) RPAS-pilot theory training. https://www.nlr.org/capabilities/professional-rpas-drone-operations/rpas-pilot-theory-training/ . Accessed 5 August 2019
Olson KB (1995) Overview: Recent incidents and responder implications. In: Proceedings of the Seminar on Responding to the Consequences of Chemical and Biological Terrorism, Chapter 2, pp 36–93
Price JC, Forrest JS (2016) Practical aviation security: Predicting and preventing future threats, 3rd edn. Elsevier, Oxford
QinetiQ, Natural Impacts (2016) Small remotely piloted aircraft systems (drones): Mid-air collision study. The UK Department for Transport. In: Military Aviation Authority, and British Airline Pilots' Association
Rassler D (2016) Remotely piloted innovation: Terrorism, drones and supportive technology. Combating Terrorism Center, West Point, New York
Ravich TM (2018) Commercial drone law: Digest of U.S. and global UAS rules, polices, and practices. American Bar Association, Lanham, Maryland
Regulation (EC) No 216/2008 of the European Parliament and of the Council of 20 February 2008 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and

repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91

Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002

Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91

Rossi Dal Pozzo F (2015) EU legal framework for safeguarding air passenger rights. Springer, Cham

Schiavo MF (2008) A chronology of attacks against civil aviation. In: Thomas A (ed) Aviation security management, vol 1. Greenwood. Westport, Connecticut, pp 142–260

Schroeder K, Song Y, Horton B, Bayandor J (2017) Investigation of UAS ingestion into high-bypass engines, Part II: Drone parametric study. 58th AIAA/ASCE/AHS/ASC Structures, Structural Dynamics, and Materials Conference

Scott BI (ed) (2016) The law of unmanned aircraft systems. Kluwer Law International, Alphen aan den Rijn

SESAR (2018) Full speed ahead for drone traffic integration: SESAR establishes U-space demonstrators across Europe. https://www.sesarju.eu/news/uspacedemonstrators. Accessed 5 August 2019

Shvetsov AV, Shvetsova SV (2017) Protection of high-speed trains against bomb-carrying unmanned aerial vehicles. J Transp Secur 10(3):115–126

Simmons, C (2018) DRONES: protecting airports and aircraft. Aviation Security International. https://www.asi-mag.com/drones-protecting-airports-and-aircraft/. Accessed 5 August 2019

Skylogic Research (2019) 2018 Drone market sector report. http://droneanalyst.com/research/research-studies/2018-drone-market-sector-report-purchase. Accessed 21 August 2019

Song Y, Horton B, Bayandor J (2017) Investigation of UAS Ingestion into High-Bypass Engines, Part I: Bird vs. Drone. 58th AIAA/ASCE/AHS/ASC Structures, Structural Dynamics, and Materials Conference

Sweet KM (2008) Aviation and airport security: Terrorism and safety concerns, 2nd edn. CRC Press, Boca Raton, Florida

Thomas AR (2003) Aviation insecurity: The new challenges of air travel. Prometheus Books, Amherst, New York

Treaty on European Union (consolidated version 2016). Official Journal of the European Union, Vol. 59, C 202, 13–388

UK Wireless Telegraphy Act 2006

UKAB (2019a) Current drone AIRPROX Count and Information. https://www.airproxboard.org.uk/Topical-issues-and-themes/Drones/. Accessed 5 August 2019

UKAB (2019b) Consolidated drone/balloon/model/unknown object report sheet for UKAB meeting on 19 Jun 2019. https://www.airproxboard.org.uk/Reports-and-analysis/Monthly-summaries/2019/Monthly-Meeting-June-2019/. Accessed 21 August 2019

Waters N, Fiorella G (2018) Did drones attack maduro in caracas? https://www.bellingcat.com/news/americas/2018/08/07/drones-attack-maduro-caracas/. Accessed 7 August 2019

Wiegmann DA, Shappell SA (2003) A human error approach to aviation accident analysis: The human factors analysis and classification system. Ashgate, Aldershot

Wild G, Murray J, Baxter G (2016) Exploring civil drone accidents and incidents to help prevent potential air disasters. Aerospace 3(3):22–32

Yle (2017) Border guards find drone with smuggled smokes on Finland-Russia frontier. https://yle.fi/uutiset/osasto/news/border_guards_find_drone_with_smuggled_smokes_on_finland-russia_frontier/9951828. Accessed 7 August 2019