Journal of Strategic Security

Volume 14 | Number 3 Article 6

Past Attacks, Future Risks: Where Are We 20-years After 9/11?

Sarah Jane Fox , Ph.D.
Staffordshire University, dr.sjfox@hotmail.com

pp. 112-157

Recommended Citation
Fox, Sarah Jane , Ph.D.. "Past Attacks, Future Risks: Where Are We 20-years After 9/11?." *Journal of Strategic Security* 14, no. 3 (2021) : 112-157.
DOI: https://doi.org/10.5038/1944-0472.14.3.1964
Available at: https://digitalcommons.usf.edu/jss/vol14/iss3/6

Past Attacks, Future Risks: Where Are We 20-years After 9/11?

Abstract

his year, 2021, marks the 20th anniversary since 9/11, recorded as the '*day that changed the world*.' Security remains an area where governments and airlines are continuously struggling to stay ahead, but since 9/11 there have been other challenges to the air transport industry – not least Covid-19.

This research primarily critically reviews the actions taken in the aftermath of 9/11 from the US and EU perspective, before consideration is given to the current/present situation, the new, and emerging challenges being faced. The research is undertaken through a legal/policy perspective.

The findings are that internationally and regionally, society is not prepared for another attack and that there remain a number of challenges that stand to impact aviation; ultimately, more collective action is needed to mitigate for such risks going forward.

Acknowledgements

This is fully my own work and research. However, as always I would like to extend my appreciation to DePaul University in Chicago - who hosted me during my Fulbright year (2015/2016).

Introduction

Written in remembrance all the victims of 9/11
and other terrorist attacks against aviation

Aviation is a great facilitator, it makes the world seem smaller, physically connecting people and society. It drives economies and brings aid and relief to disaster and war-torn areas. Air travel facilitates opportunities, whether for personal mobility or for trade and business development, allowing borders and boundaries to be crossed with relative ease.[1]

In much the same way, air travel provides the same opportunities for criminal pursuits by providing global reach. Criminal activities range from smuggling illegal and prohibited items to atrocities committed against the transport mode and the supporting infrastructure.[2] However, aviation remains a target to criminals, too, including terrorists. Aviation has often been plagued by direct and indirect events–such as directly being targeted for terrorist attacks, and indirectly being affected by global events such as wars, oil crises, and pandemics.

It could be said that two of the most significant events in the last twenty years have been September 11, 2001 (the past) and Covid-19 (the present). Particularly, the latter has reduced, if not stopped, the freedom we have taken for granted to fly across the globe. There is no denying that security breaches and terrorist attacks have been a significant challenge to the industry. Twenty years ago, the events of 9/11 clearly showed the results of what can go wrong and the devastation of what could occur. Invariably, the impact was far reaching, not just on that day but the enduring legacy it left—in term of victims, the destruction, and the changes to the aviation sector.

September 11, 2001 is recorded as the "day that changed the world"' and in essence it raised the consciousness of security, not just to the industry, but to the public.[3] Security remains an area where governments and the aviation sector are continuously struggling to stay ahead, but since 9/11 there have been other challenges to the air transport industry—not least Covid-19. This has challenged and changed the world, with a high potential to impact on security, including aviation.

Aviation as a Target

September 11, 2001 did not mark the first attack in aviation—in its relatively short history, aviation has often been plighted by attacks both directed at airports and aircrafts.[4] It was within thirty years of the Wright Brothers taking to the air that aviation was first targeted and exploited by criminals and terrorists.[5] Since this time, aviation has remained a high-profile target.

Historically, States' governments have claimed sovereignty of their skies, which influences subsequent policies, ownership rules, and other types of legislative actions and restrictions relating to airlines. These policies and legislative actions encourage the view that airlines are an extension of the State (despite subsequent deregulation and liberalization in many countries). These facts and perceptions inevitably leave airlines susceptible to attack. In most instances, an attack levied on an airline is aimed at what is perceived the *State* itself—since airlines are often a flag carrier of the country.[6]

In reality, the target is more often the State affiliated with the airline, and the political stance being taken or viewed as being adopted by the State government. Security breaches and terrorist attacks are therefore frequently political statements. This leads to an interesting debate as to who is liable for security and who should bear the cost of security measures. Security comes at a price; however, the lack of security is infinitely more expensive.

Aim & Scope of Present Research

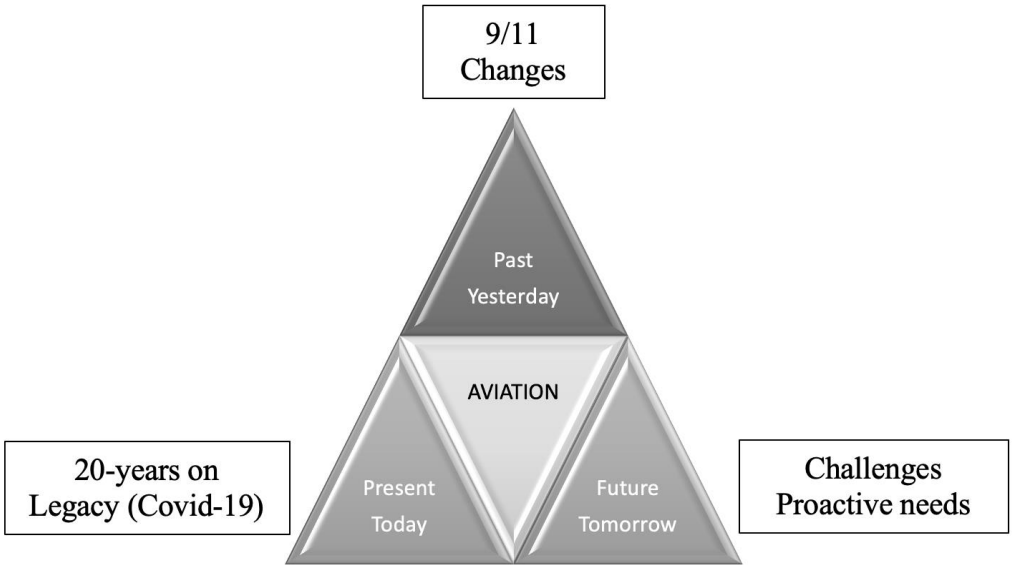
This article is written from a legal and policy perspective (through the discipline of law) and takes a triangulated approach (Figure 1: Structure of this paper).

- First, historical research is undertaken. The focus is primarily on discussing the action and mitigation put into place directly after 9/11, and because of the subsequent enquiry.
- This is undertaken by reviewing, investigating, and reflecting on the United States and the European Union approaches in the aftermath and as a consequence of 9/11.[7]

https://digitalcommons.usf.edu/jss/vol14/iss3/6
DOI: https://doi.org/10.5038/1944-0472.14.3.1964

- The primary approach is to consider this from a legislative and policy viewpoint, in terms of consistency and conformity of calls for action.
- Second, the attention is then turned to the present time—current measures and difficulties (covering factors such as sharing passenger details and the conflict between security vs. privacy);
- And, third, as part of this consideration, analysis is given to current and future risks, threats, and vulnerabilities, including with respect to Covid-19.

Figure 1: Structure of the research presented in this article



Responses to Attack

The history of aviation shows the primary approach to security to be one of reaction, and not foresight and pro-active prevention. In essence, this has, for the most part, resulted in delayed responsive mechanisms, whereby policies and practices have been put into place to mitigate the reoccurrence of attacks already experienced.

The ICAO Framework for Aviation Security

The Convention on International Civil Aviation was agreed and opened for

signatories in 1944 in Chicago (also known as the Chicago Convention).[8] The International Civil Aviation Organization (ICAO) was founded as part of the Chicago Convention requirements—with a remit, to support diplomacy and cooperation in air transport. At that time security was not written into the Convention.

It was not until 30-years later, in 1974, that the provisions for international aviation security were first introduced through Annex 17 to the Chicago Convention.[9] The reasoning was attributed to the growing rise of security breaches against aviation in the late 1960s.[10] In fact, this development by ICAO followed the adoption of several international conventions in relation to offences committed against an aircraft.[11] ICAO's approach to minimizing security breaches is via a method of assistance, whereby ICAO assists Member States through guidance documents such as the Security Manual Safeguarding Civil Aviation Against Acts of Unlawful Interference.[12]

Today, the initial focus of developing Standards and Recommended Practices (SARPs) has evolved to a three-pillar approach. This being

1. Policy initiatives;
2. Audits focusing on the Member States capabilities to oversee their own aviation security initiatives and activities; and,
3. Assistance to States in addressing serious security deficiencies revealed through the ICAO audits (performed under the Universal Security Audit Programme—managed by the Aviation Security Audit Section–ASA).

The security provisions cover both airports and aircraft. In the years between 1973 and 1985, airports were particularly targeted, with twenty-five attacks occurring at various airports across the globe. Consequently, this led to the Protocol for the Suppression of Unlawful Acts of Violence at Airports (signed at Montreal on 24 February 1988), which was supplementary to the earlier Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation (1971, Montreal).[13]

Undoubtedly, these attacks were also instrumental in leading to the establishment of the ICAO Aviation Security (AVSEC) Panel in the late 1980's (after Lockerbie).[14] It is the role of the experts on this Panel to

https://digitalcommons.usf.edu/jss/vol14/iss3/6
DOI: https://doi.org/10.5038/1944-0472.14.3.1964

advise and address evolving threats to civil aviation.

That said, many of the significant changes to aviation security have come as a direct result of tragedies, or near misses that have revealed fallibilities in the current security measure. Screening techniques and search methods at airports have been particularly investigated in subsequent enquiries. And of course, there remains a direct correlation between the security at the airport and the risk and exposure to the aircraft. While the focus on this article relates to security put in place after 9/11, there are lessons to be learned from the 1988 terrorist bombing of Pan Am Flight 103 over Lockerbie in Scotland, which shows the consequences of failures at an airport and the inability to coordinate information.[15]

Lockerbie 1988

The report into Lockerbie revealed several failings, plus the inability of the international community to undertake concerted action to liaise. This included bringing the perpetrators to justice via trial. While this did lead to various corrective measures and practices being introduced, it is arguable whether all lessons were learned and acted upon before 9/11.

It is questionable whether there has been consistency across the globe in terms of implementation of security practices since Lockerbie. The Pam Am 103 attack has similarities but also stark difference to 9/11. It did involve an U.S. airline—Pan-Am (flight 103)—but the circumstances of Lockerbie were also unique in terms of the international depth of this atrocity, meaning, the location of the explosion, the fact that many of the victims were U.S. citizens (who died in a U.S.-operated aircraft but within the territory of the UK, and at the hands of bombers from Libya) who were not killed in the event.

While the devastation caused by 9/11 was much higher—in terms of lives lost and the sheer destruction—it did not challenge the international community in the same way as Lockerbie. Lockerbie, in fact, led to positive changes such as preventing luggage being carried without the respective owner or passenger onboard.[16] One other significant finding of the Lockerbie investigation was the accusations levied at the airline itself and the fact that the U.S. intelligence services had alerted Pan Am that it was at risk; however, it was identified that the airline had repeatedly ignored

warnings that its security measures for interlining baggage were not sufficient.[17]

The Presidential Commission investigating the incident placed much of the blame for bombing of Pan Am Flight 103 on the "seriously flawed" aviation security system, beginning with inept and confused Pan Am security at Frankfurt and London. However, criticism was also levied at the U.S. Federal Aviation Administration (FAA) and their failure to enforce its rules. One of the subsequent recommendations of the Commission was that a new assistant secretary of transportation for security and intelligence should be created to oversee aviation safety, and that the FAA's security division should be elevated to report directly to the FAA Administrator (at that time James B. Busey). The Commission Chair stated,

> [t]he sad truth [was] that the aviation security system administered by the FAA has not provided the level of protection the traveling public demands and deserves. The system is seriously flawed and must be changed.[18]

September 11, 2001

Nearly 13-years later and 12-years after the formulation of AVSEC, 9/11 occurred. The 2001 terrorist attacks once more exposed vulnerabilities in air travel. It revealed that previous learning from Lockerbie had not been applied. The circumstances had not been foreseen or anticipated by experts and other related stakeholders—certainly, factors to mitigate attacks had not been effectively utilized.

The 9/11 attacks struck at the heart of the United States and were aimed at high-profile physical targets, represented by the Twin Towers in New York and the Pentagon—the Department of Defense Headquarters.[19] The effects were significant. Many lives were lost not only on 9/11, but for a considerable period afterwards, which included emergency service workers that attended the scenes.

The fallout and consequences extended beyond the United States to global economic markets, while also exposing vulnerabilities and heightened awareness of the threats posed by terrorism. These attacks were directed

https://digitalcommons.usf.edu/jss/vol14/iss3/6
DOI: https://doi.org/10.5038/1944-0472.14.3.1964

at a democratic government, whereby they were invariably designed to undermine and challenge confidence in States to ensure the protection and preservation of society. Not since Pearl Harbor had the United States been exposed to such a high intensity of attack on its home soil. The method of delivery was perpetrated using airplanes as weapons of mass destruction; however, the opportunity arose due to fallibilities in various systems related to aviation security.

Debatably, lessons had not been sufficiently learned from Lockerbie. There was an obvious indicator of a repetitive trend and propensity not to sufficiently or adequately inspect luggage—in this instance, in respect to carry-on items. The information given to the subsequent 9/11 Commission inquiry highlighted aspects relating to the travel documents (passports) and within the visa process for (multiple) entries by the perpetrators into the United States. This included non-compliance with immigration law. Considered collectively, the 9/11 hijackers:

- Were known al-Qaida operatives who should have been on watchlists;
- Had presented passports "manipulated in a fraudulent manner;"
- Had presented passports with "suspicious indicators" of extremism;
- Made detectable false statements on their visa applications;
- Had been pulled out of the travel stream and given greater scrutiny by border officials.
- Made false statements to border officials to gain entry to the United States; and
- Violated immigration laws while inside the United States.

September 11, 2001 caused resounding shock to resonate internationally regarding the attack and the vulnerability to aviation. Despite widespread condemnation of the attack and "post-9/11 posturing" to be proactive from an international and unified perspective, in many instances this diminished over a relatively short period of time.[20] This is illustrated by the fact that one of the most pressing issues in the aftermath of the attack related to recovery schemes—in the form of insurance payouts and compensation or protection systems.[21] The ICAO "Global Scheme on Aviation War Risk Insurance" was advocated as a coordinated solution to providing assistance in the field of aviation.[22] However, as so often been

the case with international discussions, attaining final agreement proved impossible, for while recognizing the need to achieve stability and reassurance during such crisis events, nations could simply not agree on the diversification of approaches. In essence, there was not the political will nor the mechanism at an international level to successfully implement the plan.

The reality remains that international law is comprised of international treaties under the principle of international customs, which Member States governments decide whether to enter in, or not as the case may be. The consequences of this translates to disparity of approaches and variable solutions across the globe in terms of aviation security protection. In respect to legal approaches across states, in some instances, bilateral agreements between countries ensure some consistencies or recognition as to accepted practices and procedures operated by the respective nations. However, it can also translate to differing levels of security being provided and difficulties for passengers in terms of understanding national and regional variances and requirements. This means that different physical solutions are applied at airports, and there remain different levels of effectiveness in terms of information sharing and coordination internally (with a country) and between nations.

The 9/11 Commission were informed that the circumstances relating to missed opportunities in relation to the visa process, passports, and suspicions had offered opportunities to intelligence and law enforcement officials, but that the U.S. government did not fully exploit al-Qaida's travel vulnerabilities—which had become detectable prior to 9/11.[23] One of the reasons cited was neither the State Department's consular officers nor the United States Immigration and Naturalization Service (INS) inspectors and agents were ever considered full partners in the national counterterrorism effort. This is exemplified by the Bureau of Consular Affairs' statement that before 9/11 they were not informed by anyone in the State Department or elsewhere that certain nationals, as in this case Saudi citizens, could pose security risks. Fifteen of the nineteen hijackers were Saudi nationals. Additionally, there were significant security weaknesses in the Saudi government's issuance of Saudi passports in the period when the visas to the hijackers were issued.

https://digitalcommons.usf.edu/jss/vol14/iss3/6
DOI: https://doi.org/10.5038/1944-0472.14.3.1964

In other words, there was a failing with respect to sharing information. The border inspection services should have had a proactive role in counterterrorism as their mission was in hindsight integral to the U.S. national security strategy and, given this, they should have been given commensurate resources.

Another significant factor identified in the aftermath of 9/11 was the disconnect between policymakers and terrorist mobility specialists. It was identified that:

> [m]uch remains to be done, within the United States and internationally, on travel and identity document security, penalties and enforcement policy with respect to document fraud, and travel document screening efforts at the borders. If we have one conclusion…it is that disrupting terrorist mobility globally is at least as important as disrupting terrorist finance as an integral part of counterterrorism. [24]

September 11, 2001—The impact to the European Union: Harmonization?

September 11, 2001 was significant to aviation in terms of security amendments and revisions across the globe. It caused nations to revisit their own security, including policies, laws, and physical measures. This reinforces the fact regarding national variants and the element of security in general laying with the competence of a nation and the willingness to legislate.

Today, one of the most coordinated and unified approaches to aviation security amongst countries globally is recognized to occur within the European Union (EU). However, this only developed as a direct result of 9/11; prior to then, the European Union had no legislative competence in this area, and it was left to each Member State to determine its own security measures and apply its own rules and standards to aviation.[25] This means that there were inherent differences between the States—as is so often the case globally. Notwithstanding this achievement, it should also be noted that the standard is based on harmonization or commonality rather than equal practice being entirely the same regardless of country.

The European Union common rules in the field of civil aviation security are aimed at protecting persons and goods from unlawful interference and minimizing breaches that compromise safety. The development over the years has included Regulation (EC) 300/2008, which replaces the initial framework Regulation 2320/2002.[26] The principle behind this is that the E.U. Commission work together with the Member States and other stakeholders in determining an efficient E.U. aviation security policy. However, there is a division across two policy areas—aviation, falling within the Mobility and Transport directorate, and security which lies within the now entitled Migration and Home Affairs. This plays a significant factor in terms of competence and what level the European Union can act.

In respect to aviation, common basic standards relate to:

- The screening of passengers, cabin baggage and hold baggage;
- Airport security—access control and surveillance;
- Aircraft security checks and searches;
- The screening of cargo and mail;
- The screening of airport supplies;
- Staff recruitment and training.

This means that some nations stay at a basic level, while others seek to go above this.

However, there remains several challenges to security, not just in the European Union but worldwide, for example the cost of systems and processes, and the acceptance—not least of ensuring the proper balance between security measures against privacy rights and protection of personal data. From a European Union perspective, this has played a significant factor in the implementation of certain measures, and has caused disagreement with the United States in terms of data sharing that that latter has insisted upon as a consequence of 9/11.

Other factors to consider also relate to travel convenience against operational factors—such as time and financial considerations and implications. This is significant in terms of cost also and who should bear such—for airlines, there is an associated consideration in terms of lost revenue for any time when aircraft are on the ground; and for airports,

https://digitalcommons.usf.edu/jss/vol14/iss3/6
DOI: https://doi.org/10.5038/1944-0472.14.3.1964

there are staffing costs and who financially should pay for physical security measures and trained staff. In effect, there are national variants in this respect between who employs security agents and who bears financial responsibility and where this places them legally in terms liability.

Constantly, across the globe, there is the need to reevaluate technology measures and procedures in line with threats, intelligence reports and risk assessments at regular intervals or when new challenges become known. Though, many of the experiences across the world have resulted in each country taking its own response to a shared problem.

While the European approach, among the now 27 Member States of the Union, has seen more commonality of practices and procedures than occurs elsewhere across the world. [27] This said, as Gladwell observed, any responsive physical measures applied lead to the situations whereby, "[a]irport-security measures have simply chased out the amateurs and left the clever and the audacious."[28] In most cases, these responses stay one step ahead of the last attack or attempted attack.

Since 9/11 there have been a number of actual or attempted attacks toward aviation globally. In Europe, in 2006, there was an attempted terrorist attack out of London-Heathrow airport, whereby the intention was to blow-up several aircrafts in flight utilizing homemade explosives.[29] This led to the EU Commission adopting additional rules for passengers in relation to carrying on board liquids, aerosols, and gels (LAG). The ban was however only envisaged as a temporary restriction, which would be revisited when new technology became available. While this approach is replicated across the globe, there are variances with regards to volumes of the LAGs permissible.

However, in January 2014, a mandatory requirement was made throughout the European Union for all airports to screen with special liquid explosive detection equipment (which extended, at that time, to purchased LAGs at the airport). Today, many of these provisions exist, some seven years after, although there has been a relaxation of purchases made at airports.

Then, because of the attempted terrorist attack on December, 25, 2009 involving explosives concealed on a passenger, a subsequent EU legal

framework on security scanners was adopted.[30] However, it was stated that the use of security scanners at EU airports remained optional for the Member State or airport(s) and hence this remains subject to regulation at a national level. The Regulation therefore relates to the minimum operational standards and conditions for the scanners whereby a harmonized approach is adopted (but only when scanners are used). This translates to creating common rules and common basic whereby Member States can deviate and apply more stringent measures than those laid down, or not to apply them at all in some instances.

Therefore, this would seem to run contrary to the principal goal of the European Union which relates to a one-stop security approach applied to all flights with the Union. In essence, such deviation and diversity stand to create not only uncertainty for passengers but inconsistency of standards leading to potential vulnerabilities. Currently, it is identified that emphasis needs to be given to work across the following key areas:

- The general use of the security scanners at EU airports
- Working on replacing the ban on liquids, aerosols, and gels by a more improved and secure screening procedure
- Improving the security of the EU bound cargo and mail, which departs from airports located outside the European Union
- Improving the transparency and ensuring cost-related and non-discrimination when levying charges at the airports.

From a European Union perspective as to who should pay for security, the European Union again explains that while this is subject to the relevant rules of Community law, it translates through to the fact that the protection of civil aviation lies with each "State, the airport, entities, air carriers and other responsible agencies, or users."[31] This, therefore, identifies a shared approach to security, but one that remains subject to coordination and indeed cooperation, not only within a State but across States, and not just in respect to aviation but the sharing of other information and security data.

The USA: Action(s) After 9/11

The investigation into 9/11 revealed numerous failings relating to structuring of agencies and coordination amongst them. As was discussed,

https://digitalcommons.usf.edu/jss/vol14/iss3/6
DOI: https://doi.org/10.5038/1944-0472.14.3.1964

this related also to the remit of agencies. As of March 1, 2003, INS ceased to exist, with its functions being transferred to new entities–US Citizenship and Immigration Services (USCIS), US Immigration and Customs Enforcement (ICE), and US Customs and Border Protection (CBP)— within the newly created Department of Homeland Security (DHS).

The Aviation and Transportation Security Act established the Transportation Security Administration (TSA) within the Department of Transportation (DoT).[32] This Act applied many responses appertaining to lessons learnt from the 9/11 attacks (as well as later threats that year) and included measures such as fortification of aircraft cockpit doors.[33] Prior to 9/11, the FAA had been working with ICAO to strengthen international security standards by adopting a harmonized approach across the world. However, the United States responsive measure surpassed this somewhat slower mechanism. This again reveals some of the issues of trying to ensure a standardized and a consistent approach across the globe.[34]

However, after the 2015 Germanwings disaster, questions were raised regarding the reinforcement standard and the locking of cock-pit door procedures more widely.[35] This incident revealed a disparity of systems and practices across the globe, in terms of security and safety measures and protocols, not only from one country to another but also among different airlines.

The Germanwings protocol was inline with the rules established by the German aviation safety authority, the Luftfarhrt Bundesamt, which states that when there are two crew members, one can leave the cockpit—but only for the absolute minimum period.[36] However, in contrast, the United States procedure states that a flight attendant is required to go into the cockpit when a pilot leaves it. In terms of US procedures, the US Security Act also included the increased use of video cameras within aircraft (and at airports) and the authorization for arming flight deck crew with less-than-lethal weapons.

While surveillance cameras have now become an increasingly used method utilized to monitor travelers (and indeed staff) to detect security breaches and threats across aviation establishments—permission for the arming of crew is not a process that has been adopted widely across the globe.

However, these need to be monitored in real-time to ultimately be effective, and there are complicating factors to this issue when an aircraft is in flight. Coupled with human fallibility–especially tiredness—artificial intelligence (AI) can be a limiting factor as it remains only as good as the programming and what has been taught or learnt.

Insider threats by aviation staff, has become a major security concern for the industry in recent times. This can vary in severity and includes minor incidents of negligence, to purposeful criminal offences, through to organized crimes, including an opportunity to undertake or assist in a terrorist attack, including seizing or hijacking an aircraft, whether at an airport or in the air. The Germanwings disaster, which was allegedly purposely perpetrated by a sanctioned pilot, gives obvious concerns as to the associated risks involved with permitting certain authorized personnel to have weapons onboard. It also shows the fallibility in terms of insider threats, as the Germanwings incident clearly showed that security threats also manifest themselves from staff and employees.

From a United States perspective, armed personnel have been viewed as a key aid to deter or prevent offences on aircraft and is seen as providing an added security layer. Historically, air marshals precede 9/11. In fact, they have been on US planes for over 50 years, with a sky marshal program being established by President Kennedy in the 1961 because of the then security breaches and threatened or potential risk of such. The FAA began its official Sky Marshal program in 1968, and today the Federal Air Marshal Service (FAMS) comes under the supervision of the TSA, which is part of the US Homeland Security (DHS).[37]

Research data from 1999 argued that a hijacker had an 81 percent chance of seizing control of an aircraft as compared to the success of bombing an aircraft, which was stated at being lower, at 76 percent.[38] Given today's security measures, these statistics may well have changed; however, the effectiveness of air marshals has not been researched more recently, and there remains questions as just how effective and equipped they are to cope with a group of terrorist and today's security challenges.[39]

https://digitalcommons.usf.edu/jss/vol14/iss3/6
DOI: https://doi.org/10.5038/1944-0472.14.3.1964

The Right to Protection: But Whose Responsibility and by What Means?

The Universal Declaration of Human Rights (UDHR) identifies that "[e]veryone has the right to life, liberty and security of person,"[40] but arguably this leads to questions as to whose responsibility is this to ensure? When considered from an aviation perspective, enquires after incidents have often levied criticism at several organizations—including airlines, airports, physical security measures (or the lack of these) and agencies—ranging from a whole host, given the international variances within countries. Particularly highlighted is the inability to coordinate. The preamble of the UDHR reaffirms the intention of Member States to ensure the adherence to human rights through their pledge to work in cooperation with the UN to achieve this. However, the degree of cooperation for aviation security could at times seem to be questionable.

It is a common criticism after an event, and in subsequent investigations, that there has been a failure, at some level, in coordinating and sharing information—such as intelligence and data of an impending threat. Many enquiries have found that a coordinated response may have aided in mitigating or even preventing the higher-level of exposure to the risk or the event itself. This said, where terrorist attacks have been successful, the ultimate culprit is the terrorist(s) or offender(s) and any related network behind it. In more recent attacks, the possibility of seeking redress from the perpetrator(s) and associated group has proved problematic (suicide bombers) and contentious (Lockerbie) and only in rare cases has compensation from a source (other than an insurer) been possible.

Lying at the opposite end to security perhaps remains the entitlement to privacy with Article 12 declaring that, "[e]veryone has the right to the protection of the law against such interference or attacks." However, there is one key phrase here that is perhaps overlooked and that is in terms of whether security is viewed as arbitrary interference or action that is needed to keep someone (or others) safe and secure.

Security remains a shared responsibility both at airports and even on aircraft, as there remains an inherent linkage between security failures at airports which translate to terrorist atrocities in the air or involving aircraft. Coupled with this, of course there is the role of the State, or State's

agents, such as security and policing bodies that also factor both in terms of culpability and responsibility.

Tools in the Kit: Sharing Information

In the aftermath of 9/11, more emphasis was given to the need for government security and law enforcement bodies to collectively work together to gain data in a bid to prevent another terrorist attack but amidst this there were claims levied (particularly in the United States following the creation of Homeland Security). This was viewed as an essential tool in the aviation security tool kit.

However, the converse side of this was that this was leading to a mountain of digital data being collected on individuals who were never a threat to security.[41] Privacy activists claimed that the depth and degree of data mining was not justified and invaded personal privacy rights, which undermined civil liberties and was contrary to constitutional rights and other established civil protections. In addition, it was stated that such routine collecting meant that potential individuals or groups stood to be missed due to the sheer volume.

In today's digital and cyber age, these issues are increasing becoming interlinked and invariably more controversial, as technology presents both a challenge to security and equally an opportunity as a means to utilize to address threats.[42] On the one hand, the Internet is celebrated as a way to connect millions of people each day, whereby information is willingly shared via this method, yet on the other hand, objections are raised when travel records are transferred across borders and biometric data is shared.

This said cooperation and building intelligence and trust is recognized to be the most effective way to combat and fight terrorism, which therefore ensures freedom of the individual and ultimately preserves their right of life.[43] The Final Report of the 9/11 Commission, identified the reluctance by different security authorities to share information with one another and this being one of the main causes of the failure to prevent terrorist attacks. The clear need to remove silo mentalities was identified.[44]

Prior to 9/11, some governments, including the United States, used passenger lists to screen travelers before departure against watchlists. As a

https://digitalcommons.usf.edu/jss/vol14/iss3/6
DOI: https://doi.org/10.5038/1944-0472.14.3.1964

result of 9/11, the United States demanded that other nations adopted a more advanced process, as a coordinated approach, and shared passenger information. However, at times, this had proved one of the most contentious requirements—particularly for the European Union.

Passenger Name Records (PNR): Profiling—The Privacy of Data vs. Security Debate

Since 9/11, the focus has shifted to preventing terrorist attacks and monitoring those so far unidentified by using more of the detailed information collected by airlines and travel agencies when an individual books a flight. The revisions to US security led to a requirement for other nations to supply the USA with what is called Passenger Name Records.[45] Passenger Name Records (PNR) contains information, such as travel itineraries and payment details that can be analyzed to identify high-risk travelers before they board their planes.[46] But the transmission of such sensitive information outside of the originating country has remained a controversial issue, which has required numerous barriers having to be negotiated.

The United States requirement for airlines to supply PNR data to the Bureau of Customs and Border Protection (CBP) within the DHS ran contrary to Article 25 of the 1995 EC (European) Data Protection Directive.[47] This stated that personal information originating from within EU Member States may be transferred to a third country only if that country "ensures an adequate level of protection."

The Commission decided that the United States did not ensure this adequate level of protection that would allow the PNR data to be transferred from Member States. This presented a predicament for the airlines, as they were left in a situation of either breaching European Union law (and of the (then) respective national laws implementing such) should data be transmitted; fly without supplying the data and receive sanctions in the United States, including the potential loss of landing rights for the airlines; or, not flying at all to the United States.

While it is appreciated that data and intelligence need to be shared to prevent terrorist attacks, there is no denying the concern in sharing information of passengers and the storage of the information (including

how long the data is stored for). Most of the controversy, however, surrounds the use to which PNR data is used, for example automated profiling based on passenger data and the use of data mining programs to obtain computer-generated risks assessment scores which aim to identify passengers who may pose a risk but who are not on any Government watch list.[48]

In relation to the United States-European Union compromise, it in fact took many years of negotiations, whereby there was a succession of interim agreements and annulments. Part of the initial difficulties related to the competence of the European Union to negotiate on behalf of the Member States for what was a security matter. Only as late as 2012 was a final agreement reached.[49]

Sending information outside of the European Union has remained a highly sensitive issue for the Member States collectively.[50] The European Union advocated early on that there was a key role to be played by ICAO, who later developed a series of guidelines for PNR transfers to governments.[51] That said, the European Union has continually reinforced the challenges and hence concerns regarding international PNR transfers, as countries continue to establish their own systems and call upon States to supply data on passengers.[52]

In 2016, the European Union eventually adopted a PNR Directive, which is additional to an existing Advanced Passenger Information (API) Directive[53]—which is an identification mechanism.[54] In the PNR Directive, the mandate is to obtain data specifically to fight terrorism and other serious crime. This has been described as one of Europe's most controversial directives to date.[55] At the same time, it advocated that the measures within would "save lives, protect rights, catch criminal and make Europe a safer place for citizens." but that said, it has taken virtually five years to achieve, approved by plenary on 14 April 2016.[56]

There is no doubt that collecting widespread data on passengers, commencing earlier than the initial flight, builds up an extensive profile on a person, but this has led to concerns of global surveillance programs. It is therefore argued that the events of 9/11 merely provided justification for the United States to extend it existing mechanisms, such as the earlier Computer Assisted Passenger Pre-Screening (CAPPS–I).

https://digitalcommons.usf.edu/jss/vol14/iss3/6
DOI: https://doi.org/10.5038/1944-0472.14.3.1964

Basics to Extreme Measures

The key invariably remains acceptability of practices and methods by the end users alongside the ability to gather and share relevant and valuable intelligence that enables crimes to be detected and ideally (alongside this) terrorism prevented. There are other tools in the kit box, starting from the basic and more generally accepted actions through to the more controversial methods, such as PNR and other means of profiling.

Identification of the traveler will always remain a fundamental, but somewhat basic and acceptable requirement of air travel. An essential element is therefore the related travel document, which is largely recognized to be the passport—particularly for international travel. Since 9/11 biometrics are seen as an essential factor to aid security, which had been added to passports.

ICAO have developed the worldwide standard for machine readable passports (MRP) as part of the Machine Readable Travel Document (MRTD) program. The MRTD has been rapidly growing and developing into a traveler identification management system—largely a development of the TRIP (Traveler Identification Program) into a wider strategy.

The TRIP Strategy recognizes and adheres to the principle of interconnectivity—from registration and issuing of the passport, through to the travel document industry (production), regional entities, the aviation security authorities, law enforcement bodies, border agencies, international organizations and the role of airlines and airports (during the travel period). In this way, the emphasis remain on ensuring aviation security is viewed as a shared goal with various players taking an active role, and is linked to the overarching aim concerning combatting terrorism—with a special focus on effective border control management.[57] The premise is, as ICAO's Secretary General explained, that the

> "strategy harmonizes the global line of defense in [the] shared battle to confront international terrorist movements, cross border crime, and many other threats to civil society and international aviation."[58]

These key messages continue to be reinforced—ICAO clearly recognizing the need to work closely with other bodies including, those of the UN (for example the Counter Terrorism Committee (CTC) of the United Nations Security Council (UNSC), in order to mitigate the threats of terrorism to international civil aviation.

Checks and scans at airports–whether of the travel document or person or luggage have become an everyday occurrence, but the level of advancement and technological use continues to vary across the globe. There remains a variance of differing systems and practices being tried and implemented. Nevertheless, it is also advocated that despite these differences, security checks at airports have become, according to some security experts—too predictable whereby the focus is largely being directed towards finding items rather than individuals.[59] And while profiling through the gathering of data (data mining) is controversial—profiling at airport provides another means of locating a would-be terrorist.

However, the acceptability of practices and methods, as used, for example in some quarters (Israeli intelligence and border or security authorities) would no doubt lead to further contention and issues being raised regarding ethical or discriminatory practices if utilized more extensively in some countries. Targeting, based upon selected or even random ethnic linkage—or preconceived associations—would simply not be acceptable, and indeed legal, in many societies. But that said, it is also argued that there is value in modified practices based upon demeanor and behavior profile analysis at the airport.

Tactical risk assessment of people—in other words behavioral analysis—allows for the adoption of various methodologies for identifying threatening or potentially disruptive individuals through observation or questioning techniques. As it is every increasingly recognized that security and terrorism prevention is becoming a shared responsibility, the practice of Israel's El Al airline, in training its workers in psychological observations techniques, is seen as another essential layer in the safety or security process that should be more widely applied and implemented. While border force agencies, such as customs and immigration have their role to play, there is often criticism that this occurs after the passenger has traveled rather than before. Applying a similar technique prior to the flight

https://digitalcommons.usf.edu/jss/vol14/iss3/6
DOI: https://doi.org/10.5038/1944-0472.14.3.1964

and as part of the checking-in or security process could assist in detecting not only terrorists, but those who could become a problem in the air to the crew and fellow passengers. Flight Safety Councils have endorsed such an approach, which is based largely upon accepted practices undertaken by customs and immigrations on arrival.[60]

The human versus machine debate remains another critical concern in the process of detecting potential offenders and terrorists. Alongside the human component in interpreting behavior lies the dilemma and anxieties of using the next level of automated decisions—particularly, the use of artificial intelligence (AI) and the role to be played by AI in aviation security going forward. Today, automated decision taking and making are becoming increasingly part of the equation and this is set to increase with technological developments. There remains concern as to transparency in the logic used for such decisions, and essentially the harm that could arise should and when an error occur, versus the risk of a terrorist attack in the first instance. This apprehension remains an extension of the argument relating to the security of data (much of it alleged to be unnecessarily obtained in the first place)–namely, the associated risks (of gathering and storing it) measured against the merits and successes of its analysis and use.

Critics and fundamental rights activists, alongside identifying the intrusive and often secretive nature concerning the way the data is gathered and the use to which it is put, also identify the opportunity to create a false record by or for a criminal or terrorist in a time when cybercrime and cyber security is becoming a major challenge.[61] Hence, achieving management solutions to the storage of data, therefore, is a reoccurring parallel issue. Increasingly, there are more worrying factors for aviation security to address. As aviation development (alongside other major and critical infrastructures) intensifies its reliance on a networked and linked information and technology-based framework and support system, it opens itself up to newer security and cyber security challenges.[62] Worryingly, this includes cyberterrorism.[63]

Clear and Present Dangers: Tomorrow Will Become Today

The current security threats to aviation are multifaceted and diverse, ranging from the basic to the extreme possibility and scenario. Speaking at

a Special Meeting convened by the Counter-Terrorism Committee of the UNSC, Dr. Liu stated:

> Foreign terrorist fighter movements, landside attacks, threats posed by insiders and airport staff, and the use of increasingly sophisticated improvised explosive devices are all of significant concerns.[64]

It remains a fact that aviation will continue to remain a high-profile target for the extremists. There remain clear and present dangers to aviation, but to say that one method presents a higher risk than another would be difficult to quantify. That said, going forward there is little doubt that the risks from the reliance on ICT systems will become a higher priority, which was equally recognized by both ICAO and the UNSC "expanding reliance on information technology in all areas of aviation–from navigation to communications to security—exposes us to cyber threats."[65]

Cyber Security and Cyber Threats

Cyberattack is terminology applied to when there has been illegal penetration of systems which could cover a whole range of malicious activities—such as hacking (or arguably cracking), jacking and spoofing.[66] Aviation has become increasingly subjected to such cyberattacks. The use of cyberspace has become a means by which perpetrators enter computer systems without permission and authority, while cyber security involves techniques put in place to prevent or mitigate such attacks. [67] These defensive mechanisms can range from processes and practices to technology developed walls, and other shielding means, whereby the intention is to reduce the risk and any threat posed by such illegal breaches.

At the 21st Aviation Security Panel Meeting of ICAO a new Recommended Practice relating to cyber threats was proposed for adoption by the Council. [68] It was subsequently adopted on 17 November 2010.[69] The emphasis, however, is for each Contracting States to develop their own measures to protect information and communications technology systems used in civil aviation. As with other aspects of aviation within the European Union, regionally there has been a noticeable collective approach, not only through the European Union mechanism but also

https://digitalcommons.usf.edu/jss/vol14/iss3/6
DOI: https://doi.org/10.5038/1944-0472.14.3.1964

through the European Civil Aviation Conference (ECAC) which consists of not only E.U. States but other countries which are members to the body.[70] ECAC have been described as an effective 'think-tank' for aviation that feeds into the European Union (including European Aviation Safety Agency (EASA) and EUROCONTROL).[71]

In 2016, Luc Tytgat the Director of Strategy and Safety Management at EASA, reported that aviation systems were subject to an average of 1,000 attacks each month.[72] Today, it is increasingly recognized that the day-to-day booking systems, and hence, storage of passenger information continues to be subject to penetration. While these breaches vary in nature and method, there nevertheless remains the potential for more devastating consequences where lives are ultimately lost.[73] From the airplane perspective, EASA has acknowledged, that in the last few years, representatives of the pilot community have stated that, pilots' awareness of cyber risks in aviation is increasing but there remains a need to constantly revisit cybersecurity learning objectives in the pilots' academic training syllabus.[74]

Perhaps most worrying is the risk posed to computer-based navigations and communications systems—both on-board and at air traffic control centers across the globe. These areas of technological development remain subject to both insider abuse and unlawful external interference, which ultimately could compromise the security and safety of passengers traveling within the aircraft, as well as those on the ground. National Airspace Systems (NAS)—such as NextGen (in the United States)—increasingly use advanced technology that is interconnected via network systems, which, while improving safety through less isolated and separated regional (or national) operations, arguably, intensifies the possibility of a cyberattack.[75] A 2015 report to Congressional Requesters clearly highlighted the fallibilities and weakness in the US air traffic control system.[76]

In Europe, the director of the European Aviation Safety Agency (EASA) also warned of;

> the intensified possibility of a serious cyber-attack through hacking into the critical systems of an aircraft from the ground. In fact, the director, Mr. Ky, openly revealed to the Association des Journalistes

> Professionnels de l'Aéronautique et de l'Espace (AJPAE) that his organisation had in fact hired someone to test the vulnerability of the Aircraft Communications Addressing and Reporting System (ACARS) used to transmit messages between aircraft and ground stations. It took the hacker, who was also a professional pilot, only five minutes to penetrate the messaging system and a further few days to then gain access to aircraft control systems.[77]

Warnings had previously been given by Hugo Teso (cyber security specialist and pilot) concerning the possibility of hijacking a plane armed only with a mobile phone, but despite this as late as 2014 ICAO continued to play down the risk, arguing that as the aircraft navigation and other control systems were effectively separated from non-critical systems such as entertainment that, the risk of hacking critical systems was low.[78]

In 2013 the U.S. FBI Director expressed the thought that:

> I do not think today it [cyber] is necessarily the number one threat, but it will be tomorrow. Counterterrorism and stopping terrorist attacks, for the FBI, is a present number one priority. But down the road, the cyber threat, which cuts across all programs, will be the number one threat to the country.[79]

The issue is that tomorrow keeps happening and cyber threats are today a number one threat and arguably one that we are not prepared for.

A 2016 report investigated the risks as perceived by the transportation sector and identified that the interconnectivity of a global society presented a number of challenges to all modes.[80] The segmentation relating to "digital vulnerability and rapid technological advancements" was clearly viewed as one of the greatest challenges and concerns to the sector.[81] The air industry in particular identified that failure of the critical IT systems was of high concern to aircraft lessors, with airlines identifying their apprehensions due to the risks posed by the rapid pace of technological advancements and an inability to keep pace with it.

In 2020, concerns were repeated to Congress, much in the same way as they had been in the 2015 report, when it was identified that the "FAA should fully implement key practices to strengthen its oversight of avionics

https://digitalcommons.usf.edu/jss/vol14/iss3/6
DOI: https://doi.org/10.5038/1944-0472.14.3.1964

risks."[82] Ultimately, these vulnerabilities continue to remain a concern for the present, which will only intensify and inevitably become increasingly significant and prevalent tomorrow.

A further categorization of risk however also related to the aspect of "geopolitical instability and regulatory uncertainty," with terrorism being identified as a clear issue of concern within this grouping. Risks once considered "emerging" are now clearly viewable as being at the corporate doorstep and hence cyber-terrorism is also beginning to knock loudly. These two top areas of concern, as identified in the Transportation Risk Index report (2016), certainly have the potential to become more linked, which intensifies not only the risk, but also the potential consequences of a cyber-terrorist attack.

Cyberterrorism

The definition for cyber-terrorism remains contested and controversial in terms of what is categorized as a cyberterrorist attack, as distinguished from a cyberattack; however, the clear distinction applied here is that a cyber-terrorist intends (through cyberterrorism) to undertaken a purposeful act which has the intention, or is foreseen as the consequence, to cause mass disruption and normally the death of and loss of lives—by a means perpetrated through some type of internet or computer interaction. Therefore, cyberterrorism can be simplified as the convergence of cyberspace and terrorism (that is, the same two top fears expressed by the CEOs within the transport sector).[83] Put another way, it is the convergence of the real physical world with the virtual environment whereby an action in a virtual (computer) world translates through to real and actual consequences to society. Like terrorism, therefore, the intention is to create terror and a feeling of fear in society.[84]

As early as 1990, the National Academy of Sciences began a report on computer security with the words, "[w]e are at risk. Increasingly, America depends on computers…Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb."[85] This message has continued to be reiterated by a string of US Presidents and their respective advisers (as well as other leaders around the globe):

- In 1999 President Clinton identified, "we must be ready…ready if our adversaries try to use computers to disable power grids, banking, communications and transportation networks"[86]
- George W. Bush, (as a presidential candidate) warned before 9/11, that "American forces are overused and underfunded precisely when they are confronted by a host of new threats and challenges—the spread of weapons of mass destruction, the rise of cyberterrorism, the proliferation of missile technology."[87]
- In 2002, Tom Ridge, director of the Department of Homeland Security, identified, "Terrorists can sit at one computer connected to one network and can create worldwide havoc….[They] don't… need a bomb or explosives to cripple a sector of the economy or shut down a power grid."[88]
- President Obama stressed, during his State of the Union address in 2013, that, "We know hackers steal people's identities and infiltrate private e-mail…now our enemies are also seeking the ability to sabotage…our air traffic control systems."[89]

There is little doubting that the risk of cyber-terrorism is both known and growing, and, with both technological advancements and continuous world instability the risks therefore are set to intensify rather than diminish. The potential is that this period of self-isolation due to Covid-19, has provided the opportunity for attacks to be planed and for skills to be matured in terms of utilization within the cyber domain.

Cyber-terrorism has several obvious key advantages over traditional terrorist methods for would be perpetrators:

- First, it is, in general, a cheaper method compared with most attacks already experienced against aviation. All that is required is a computer with Internet access.
- Second, it provides the ability to target numerous sites and facilities (including from a simultaneous perspective).
- Third, it has the potential, because of a successful attack, to impact upon a larger number of people than more traditional methods—for examples, attacks against the electric, water or transport infrastructures (particularly with simultaneous or sequential attacks).
- Fourth, it remains a more anonymous and untraceable

https://digitalcommons.usf.edu/jss/vol14/iss3/6
DOI: https://doi.org/10.5038/1944-0472.14.3.1964

method—whereby nicknames can be used and methods implemented to distort or hide the originator location.
- And finally, it can be conducted remotely. In essence, it provides the opportunity to evade capture, to stay alive and remain anonymous or untraceable.

In truth, cyberterrorism currently reduces the risk for the perpetrators and arguably increases it for 'possible' targets—for example, to aviation and other infrastructures that rely on the Internet. Coupled with this there is of course the further risk of an insider providing access and information which would facilitate and assist with needed codes and access.

The question remains as to how prepared the international community is at reacting to cyber security breaches, let alone cyberterrorist attacks. At the 2015 Conference on Civil Aviation Cyber Security the Secretary General of ICAO, Raymond Benjamin, stated, that there had been, "no catastrophic cyber security event has been reported to ICAO to this point in time."[90] Again, prevention would be preferable to response action and yet traditional acts of terrorism have notoriously been difficult to prevent.

In many ways protection against cyberterrorism requires more coordination and cooperation than any other form of terrorism prevention and therefore presents a major challenge to the industry. The recent ECA position paper acknowledged that

> "[d]ue to the interdependencies in the realm of aviation, cyber security is a shared responsibility of authorities, aircraft manufacturers, airlines, airports and air traffic control organizations together with their suppliers."[91]

However, due to the nature of cyberspace, the response requires not only the collective measures across aviation, with all of the respective players actively participating, but it also requires action and responses from parallel industries—such as the telecommunications sector and inevitably law enforcement bodies. That said, the aspect of Internet governance is perhaps even more contentious than the sovereignty (ownership) and governance factors relating to aviation.[92] "[W]hile the sky above us has no discernable-physical boundaries" the same is perhaps more true in terms of the cyberspace which largely remains outside the scope of most

instruments, certainly from an international perspective, and hence coordinating policies and approaches across borders continues to prove problematic.[93] Related to this of course remains the collective willingness to cooperate; and, while the threats of cyberattack to the aviation industry are well known, in truth, there has also been a degree of apathy and lethargy in agreeing joined action and initiatives in the past. For example, although the Beijing Treaties were said to respond to "new and emergent threats to [aviation] security," with the Convention being identified by Abeyrante as "a step forward in the right direction with the threat of cyber terrorism looming;" both the Convention and the Protocol remain increasingly unlikely to enter into force due to a lack of signatories, and hence international support.[94]

Arguably, the premise from ICAO, while being directed towards emphasizing the need to strengthen national frameworks clearly also reinforces the need for international cooperation among Member States.[95] And, in the 2017 report on aviation safety, ICAO referred to the fact that at the 39th Session of the ICAO Assembly in October 2016, the ICAO Council had adopted several resolutions related to security breaches, namely, acts of unlawful interference, including:

- Promulgating ICAO policies related to the safeguarding of international civil aviation against acts of unlawful interference, and
- Urging States to support the Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation (Beijing Convention of 2010) and the Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft (Beijing Protocol of 2010.)[96]

While the concept of cyber risk is known to the industry, the concern however remains, as ICAO stated, that unlike certain economic sectors such as banking, wherein cyber-threats and vulnerabilities are well known and comprehended, and hence countermeasures have been implemented to mitigate identified risks; in the aviation domain, "cyber related risks are not always well understood by all States and stakeholders, nor are they addressed in a consistent and systematic manner."[97] The potential reality is questionably as Luc Tytgat said, "[w]e have to be prepared always for the worst," "We have to take it seriously……" "We do not have much time."[98]

https://digitalcommons.usf.edu/jss/vol14/iss3/6
DOI: https://doi.org/10.5038/1944-0472.14.3.1964

There is no doubting that the cyber risk to aviation will intensify along with the number of devices connected to the Internet Protocol (IP) networks, which is anticipated to be almost twice the global population by the end of this decade.[99] Alongside this, the number of passengers taking flights is also set to increase leading to more aircraft occupying the skies and hence ever greater reliance on interconnected computer systems for various operations—related to safety and efficiency. Invariably, these systems will remain vulnerable to cyber penetration (including cyberterrorism) and the obvious starting point to mitigate these risks must be fully understanding the issue in the first instance; and, secondly, adopting a united stance (across sectors—including within aviation) to tackle this nemesis.

Other Threats: Drones, Missiles

Drones or Unmanned Aerial Vehicles (UAV) present another emerging threat to aviation.[100] This risk comes from their general usage in shared airspace plus the fact that they are arguably more prone to cyberattack than civil aircraft. It is estimated that drone use will intensify into the 2020's and beyond—with the drone sector becoming a significant component of the global aviation industry.[101] Predictions are that this will present a "new 'risky' era for aviation," for, although there are immense opportunities, there are also challenges that need to be factored in, too.[102] One recent report questioned whether drones could even prove to be the greatest global security threat of the future.[103]

Like the Internet and cyberspace, currently there is an acute lack of governance relating to the use of drones, certainly there remains divergence and differences across countries, many of which have their own operating rules and guidance. The training of operators (whether in a commercial or hobby or recreational environment) and the registration of craft[104] are therefore key considerations and obvious starting points, in terms of increasing safety as well as minimizing security breaches.[105]

One heightened risk to aircraft is when they are in the vicinity of landing areas (near to airports and airfields) and it therefore remains crucial for drone operators to know where controlled and restricted airspace is and to respect the guidance and legislation that exists. That said, in the UK, for

example, drones weighing 7 kg or less are not required to have the permission of Air Traffic Control (even when flying within Controlled Airspace or within an Aerodrome Traffic Zone—ATZ).[106] However, it is also recognized, that in practical terms, drones of any weight could present a particular hazard when operating near an aerodrome or other landing site due to the presence of manned aircraft. This therefore intensifies existing risks to aircraft when landing and taking off.

In the UK, in April 2017, it was reported that a commercial passenger plane approaching Heathrow Airport (in November 2016) had been involved in a near-miss incident involving several drones and on April 22, 2017 an Airbus A319, when coming into land at Liverpool John Lennon Airport, was involved in what is believed to be the closest near miss to be recorded, when a drone passed by the aircraft's wingtip.[107] Even at significant heights planes remain at risk—in 2020 a drone is said to have nearly hit Manchester easyJet plane window at 8,000ft.[108] The interference or threat of interference to civilian aircraft, by drones, could also be used as a means of extortion, e.g. pay a ransom otherwise disruptions or worse will occur.

Hence, this risk increases further when a drone is operated with malicious intent where the intention is to purposely commit a criminal act including interfering with aircraft. Drones can carry incendiary devices, grenades, and other items (such as radio-active or hazardous material) into the airspace. A swarm of drones would prove to be a formidable army to stop.

There is also the potential for control to be seized through a cyber security breach, whereby criminals or terrorists block the navigation or communication systems of someone else's UAV—thus taking control of it. It remains a fact that the unencrypted data links for command and control and navigation, used by most civilian drones, make them particularly vulnerable to jamming, interception and manipulation.[109] Research has already highlighted the ease with which drones can be attacked in this manner, and hence cyber security, particularly for commercial drone operations, remains a pressing factor for discussion—requiring international coordination, much in the same way as is constantly being stated is necessary for commercial air movements.[110] There can be little doubting that these two issues, cyber security risk to drones and cyber security risk to commercial air transport, are, and will continue to become,

https://digitalcommons.usf.edu/jss/vol14/iss3/6
DOI: https://doi.org/10.5038/1944-0472.14.3.1964

inextricably linked. Cyber threats to manned systems are today's challenge, which will only increase alongside the threats posed by and to drones.[111]

As well as emerging threats, other challenges remain. At times, there has been the potential for conflict in jurisdiction to arise in terms of civil and military use of aircraft. For while States can legitimately protect their territories against unlawful incursions and other perceived acts of hostility from the air, using military and even police intervention (which remains outside the scope of the Chicago Convention) there have been occasions where civil aircraft have purposely been targeted by both States and other third parties in acts of hostility.[112]

September 11, 2001 is said to have led to discussions concerning the possible need to scramble military jets to protect the airspace above Washington following the seizure of aircraft by terrorists.[113] However, although it is known that there was protocol in existence between the FAA and NORAD the 9/11 Commission Report concluded that it was "unsuited in every respect" to the events of that day.[114]

Under Article 3 d) of the Convention contracting States have accepted a legal commitment "when issuing regulations for their State aircraft, that they will have due regard for the safety of navigation of civil aircraft." However, while States remain able to intercept suspect aircraft in the air, they must act in conformity with the requirements stated in Annex 2 of the Convention.[115] It was the shooting down of the Korean Airlines (B-747) flight KAL-007 in 1983 that led to the adoption of this provision by the 25th Session (Extraordinary) of the ICAO Assembly on 10 May 1984, in which it was reinforced that "every State must refrain from resorting to the use if weapons against civil aircraft in flight." Therefore it has been debated and questioned as to whether a State could actually use deadly force against a civil aircraft if there were serious reasons to fear the consequences of non-intervention (as occurred during 9/11)—however, it would have to be deduced that such events were not imagined when ICAO discussed the 1983 shooting; and, in any event, the wording implies that there is an action of last resort which could prevail. This tends to be inconformity with Article 51 of the UN Charter, which concerns self-preservation of the State.

In addition to the launching of state aircraft there is also the risk of n Portable Air Defense System (MANPADS) and other surface-to-air missiles systems (particularly of a moveable nature) to commercial aircraft.[116] Self-guiding weapons can target civil aircraft, especially with the aid of infrared sensors or more sophisticated laser devices. ICAO first addressed this matter in Assembly Resolution A32-23: MANPADS Export Control, and in 2003, in Resolution A35-11: Threats to civil aircraft posed by man-portable air defense systems (MANPADS). The message was later repeated in September 2007 at the 36th session of the ICAO Assembly, which called upon action by States in Resolution A36-19, and later in 2010 in Resolution A37-17. However, on July, 17, 2014, the risk to civil aircraft by such devices was bought home when a Malaysian Airlines Boeing 777 (Flight MH17) was shot down over Donetsk in eastern Ukraine.[117] At the time, the Ukrainian government and the Russian-backed rebel militia were engaged in a civil war. While the circumstances surrounding the bringing down of the aircraft remain disputed in some quarters, the consensus remains (as stated in the official Dutch investigation report) that the aircraft came down as the result of the detonation of a 9N314M-type warhead launched from a Buk missile system.[118] At the time of the attack the plane was flying at 33,000ft (10,000m).

As a result of the events ICAO undertook investigations that followed-up the recommendations of the Netherlands Safety board relating to improving the management of risks associated with flying over conflict zones.[119] Perhaps, in hindsight, many of the Recommendations within the Netherlands report should have already have been implemented, or even considered by ICAO, with State responsibility also being emphasized when there is armed conflict in their territory (including early circulation of airspace restrictions).[120] However, it should be noted that ICAO Annex 17 Safeguarding International Civil Aviation against Acts of Unlawful Interference, at paragraph 2.4.3., already contains a requirement for each State to "establish and implement procedures to share with other Contracting States threat information that applies to the aviation security interests of those States, to the extent practicable."[121] ICAO has also emphasized that this is not just limited to information concerning threats within a State's national borders but where threats in foreign jurisdiction could impede the safe movement of civil aircraft. Once again this reinforces that sharing of information and related data is viewed as being a

https://digitalcommons.usf.edu/jss/vol14/iss3/6
DOI: https://doi.org/10.5038/1944-0472.14.3.1964

key defense mechanism at preventing attacks, where security and safety stand to be compromised.

Going forward, any future recommendations and implementation of practices and procedures that aim to improve the safety of civil aviation are to be welcomed, but it also must be noted that there has been a steady rise of man-portable air defenses systems across the globe, which extends outside the competence of State actors and increasingly include operation by terrorists and other guerrilla factions. Additionally, the understood risk of such systems was largely associated with the capacity to fire at low-flying aircraft, but the shooting down of MH17 has shown the increased vulnerability of aircraft outside a previously perceived range. This therefore will continue to remain a security and safety concern to civil aircraft, particularly given the instability across the globe and the lack of defenses available to aircraft used in civilian passenger and freight movements.[122] The technical capability of such devices is also likely to increase with time, which makes this a potential increased area of risk to aircraft in the future.

Continued concerns for air safety also arise from the increase of laser attacks, particularly during the critical phases of flight, like taking off and approaching to land. And, while most attacks have occurred at lower altitudes of a few thousand feet, the FAA has received reports from flight crews of attacks at 10,000 ft. and higher.[123] Attacks have also been recorded by air traffic control staff; and, recognizing this to be a growing problem, various working groups have been established to review legislation and the seriousness of such interference to aircraft and the respective personnel affected.[124] This is currently viewed as an “evolving menace”[125] and hence stands to be both a safety and security concern to aviation.

20/20 vision: 2021 Challenges

Twenty years on as we remember the events of September 11, 2021, there should be some reassurance that security protocols and systems have improved in this time to mitigate the failing of that day. This said aviation, is now challenged by newer and more advanced (technology) risks, that arguably we are not fully prepared to deal with. The Year of Security Culture coincides with the risk presented from Covid-19 to date (2020-

2021). This virus has also dramatically affected aviation in terms of movement, but as stated at the start it might also have allowed terrorism and other security attacks to be planned, including against aviation. As we continue to return to more international flights, aviation looks noticeably different, especially in terms of safety protocols to prevent further escalation of the pandemic. In doing, so we also run the risk of taking the eye of the ball from a security perspective.

The European Union has clearly recognized the impact of Covid-19, which has also included limiting the number of on-site visits for the designation and re-designations of air carriers and cargo operators in third countries. The virus has severely impeded this and has led to change of practices. It is also recognized that the ability of airports in the European Union to complete the process of installing standard three explosive detection systems (EDS) equipment (technology for the screening of hold baggage) has also been severely impacted by Covid-19 pandemic.[126] This has led to a new road map—one based upon further flexibility being applied. Consequently, there is likely to be more variations of approaches across the European Union and specifically in relation to screening methods used.

Coupled with this, the 2012 PNR Agreement between the United States and European Union has now been declared invalid in terms of the adequacy of the protection of data provided by the European Union-United States Privacy Shield Framework. As of July, 2021 the linchpin aviation security agreement between the European Union and United States has not been agreed and sees a return to the earlier position in terms of the ability to share information, which by itself compromises security or runs the risk of illegal transactions to the United States. The irony however is that in terms of safety due to the pandemic, medical records are however now being shared across nations. The implications of Covid-19 could, therefore, stand to impact directly on security resilience.

Conclusion

There is no doubt that terrorist attacks, such 9/11, come at a high price and that there are a multitude of victims, in terms of not only the physical casualties (and the effects to relatives/friends of those who lose their lives or are injured and maimed) but to infrastructure, airlines, airport and

https://digitalcommons.usf.edu/jss/vol14/iss3/6
DOI: https://doi.org/10.5038/1944-0472.14.3.1964

other stakeholders–including respective governments and the insurance community.

However, while there has been widespread condemnation of terrorism and terrorist attacks, the conviction of the international community has not been consistent and long-lasting. This inevitably links to the findings relating to many of the terrorist attacks against the aviation sector, namely that there have been failings in relation to communicating and sharing intelligence of impending attacks and that there has been, and arguably remains, an inherent failure in cooperating and collaborating not only across country borders but within countries.

Today, there remain continuous challenges to aviation (both to aircraft and to the supporting infrastructure). Old challenges remain but new ones are also developing and intensifying the risk. And, while 9/11 highlighted the vulnerability to this transportation mode, the prevailing years have since shown the increased risks and vulnerability to other modes and to general society through international terrorist attacks. This escalation of terrorism directed at other modes could be concluded to be because of the systems, practices and protocols put in place to directly reduce the risks to aviation (for example at the airports, with increased screening of passengers and advanced sharing of passenger data and information). However, it has also been shown that there is a lack of consistency in terms of aviation too—which leave some airlines and airports being more vulnerable than others.

There is no denying the investment into aviation security, which, at airports, is said to be "the closest to comprehensively addressing terrorism."[127] However, close does not equate to being the maximum provisions to eradicate prevailing risks. Infiltration of aviation systems remains a clear and present risk, both from a safety and security perspective—while the intention may vary, the consequences can be catastrophic. The developing challenges relating to the Internet, IT systems and cyberspace undoubtedly produce the biggest test that still needs to be overcome. And it would be realistic to conclude that for the aviation industry this remains an area that all players (governments, airlines, and other actors) are continuously struggling with; arguably, firstly there must be a need to recognize the full extent of the challenges, and then secondly, to then stay ahead of these challenges. But again, this is

not isolated to aviation alone and therefore this complicates the actions to prevent and mitigate such risks. These challenges face many industries and critical infrastructures and crossover into adjoining areas—not least the area of telecommunications and computer networks. These are not national issues but global problems, which require an international response. One then will be better synchronized than it has been in the past.

Throughout this article reference has continually been made for the need to share information and coordinate data and responses. While on occasions this approach has been seen to challenge human rights through the sharing of data on individuals, repeatedly it is confirmed that without this close liaison, responses will not be sufficient at a national or regional level to deal with threats and abuse, which now has taken on a clear transnational dimension.

There is a role to be played by everyone to prevent security breaches and terrorist attacks, the latter of which are progressively aimed, not only at governments but ordinary citizens of states. This is the clear message by ICAO—security is everyone's responsibility. In 2021, the direction of travel is aimed at changing the security culture.

Terrorists wish to strike fear into communities, increasingly terrorizing civilians, ultimately with the aim of coercing governments and the international political community into giving into their demands and hence, recognizing their cause. The Internet has long been seen to be a tool for recruitment and a means to promote propaganda, now it is increasingly being seen as a weapon by which "[t]errorists can sit at one computer connected to one network and can create worldwide havoc."[128] Aviation is set to remain a key target—because of it is high profile appeal and clear connections to states' governments, in terms of both ownership and control, and the aspect of sovereignty of their skies.[129] This makes detection particularly challenging.

Not recognizing the risk to aviation of terrorism and other security violations and offences was ultimately short-sighted of the international community at the 1944 Chicago Conference. Arguably, since this time, aviation has been perpetually in a state of trying to play catch-up for one security breach after another. And while it has ultimately been successful

https://digitalcommons.usf.edu/jss/vol14/iss3/6
DOI: https://doi.org/10.5038/1944-0472.14.3.1964

in many respects, the challenges of cyberspace are set to present the greatest challenge of them all, and certainly will be a more prevalent risk as we enter the second decade of this century.

Automation and new transport systems, such as drones, add another complexity to the skies, and therefore are risks to the airline industry; viewed arguably, from both a negative and positive stance (as a challenge and opportunity). The skill going forward will be in reducing the risk vulnerabilities while developing and maximizing the opportunities of their use in a positive way. Insider threats transcend many of the areas of risk and vulnerability to airlines—including at airports, within the aircraft and through Internet and linked or connected systems (such as air traffic control centers).

Vigilance is paramount to minimizing risks and stopping terrorist attacks, this includes amongst staff and passengers and extends into the area of information and data sharing (within organizations, across organization and around the globe). Technology advancements are set to continue, while these are aimed at improving safety and increasing efficiency, ultimately there are associated risks, not least of security penetrations.

It remains disputed as to whether the world has in fact become more unstable, but what is known is that the potential for, and ability to cause, destruction and havoc on a mass scale has increased alongside the accessibility and ease of acquiring such weapons to do so. And, arguably, we are still not sufficiently prepared for these challenges. September 11, 2001 showed that aircraft themselves could be easily turned into a weapon and used to target states and citizens. Taking over an aircraft by remote means may well be the next development and disaster to be faced by aviation.

In 2021, society is still being challenged by a global pandemic which, has, without doubt, unbalanced the world but it may have ironically also presented an opportunity for zealots and would-be terrorists to plan events to further destabilize society. Invariably, there will be lasting implications and consequences to society, aviation is once again being challenged, financially and potentially in terms of security risks.[130] Even basic methods, that are readily available, such as laser devices, stand to affect the safety of passengers as well as those on the ground.

The sad truth is that there will always be threats to aviation (along with other vulnerable sectors).[131] In all reality, achieving zero risk will invariably never be possible—safety and security will always stand to be comprised, whether by purposeful or unintentional actions or events. This said, the aim must always remain to achieve zero safety or security incidents, or—in failing to achieve this—attain the closest possible result to zero through mitigation methods that address, not only for today's knowns, but tomorrow's perceived challenges and threats.

In this changed world, it will not be enough to address aviation security in isolation.[132] Concerted effort needs to be given across sectors, each player accepting a degree of responsibility and duty to act. The protection of aviation also rests on targeting the root cause of terrorism and the '*will and want*' to take lives. This undeviatingly remains the greatest challenge to society and one wherein we all have a shared responsibility to stop this emerging and troubling trend.

Endnotes

1 Sarah Jane Fox, "Mobility and Movement Are 'Our' Fundamental Rights". . . Safety & Security—Risk, Choice & Conflict! *Issues in Aviation Law and Policy* 17, no. 1. (Autumn 2017): 7-43, https://heinonline.org/HOL/LandingPage?handle=hein.journals/isavialp17&div=5&id=&page=;

2 In addressing the topic of security in this chapter—primary consideration is given to the act of terrorism and loss of life.

3 Giovanni Bisignani, *Shaking the Skies* (London: LID Publishing Ltd., 2013).

4 Andrew Sinclair, *An Anatomy of Terror: A History of Terrorism* (London: Pan Books, 2003).

5 David Gero, *Flight of terror* (Somerset, UK: Patrick Stephens, 1997) Sarah Jane Fox, "Safety & Security: *The influence of 9/11 to the EU Framework." Research in Transportation Economics*—Special Edition DOI: 10.1016/j.retrec.2014.07.004 Vol. 45 (2014): 24–33. Sarah Jane Fox. "CONTEST'ing Chicago. Origins and Reflections: *Lest we forget!" International Journal of Private Law* Vol. 8, no. 1, (2015): 73-98, DOI: 10.1504/IJPL.2015.066719**.** Sarah Jane Fox, "To practice justice and right'—international aviation liability: have lessons been learnt?" *International Journal of Public Law and Policy* Vol. 5, no. 2 (2015): 162-182, DOI: 10.1504/IJPLAP.2015.071027

6 Sarah Jane Fox, "CONTEST'ing Chicago. Origins and Reflections: *Lest we forget!" International Journal of Private Law* Vol. 8, no. 1, (2015): 73-98, DOI: 10.1504/IJPL.2015.066719. Sarah Jane Fox "To practice justice and right'—international aviation liability: have lessons been learnt?" *International Journal of Public Law and Policy* Vol. 5, no. 2 (2015): 162-182, DOI: 10.1504/IJPLAP.2015.071027. Sarah Jane Fox, The evolution of aviation: In times of war and peace—blood tears and salvation! International *Journal on World Peace* Vol. XXXI no. (4 Dec. 2014): 49-79

https://digitalcommons.usf.edu/jss/vol14/iss3/6
DOI: https://doi.org/10.5038/1944-0472.14.3.1964

[7] The research article does not look to revisit the actual circumstances of this attack.
[8] Convention on International Civil Aviation, Chicago, 1944. Opened for signatories - 4 Dec, 1944, 61 Stat. 1180, 15 U.N.T.S. 295 (entered into force 4 April, 1947).
[9] This has since been updated a number of times since.
[10] Sarah Jane Fox. "CONTEST'ing Chicago. Origins and Reflections: *Lest we forget!" International Journal of Private Law* Vol. 8, no. 1, (2015): 73-98, DOI: 10.1504/IJPL.2015.066719.
[11] Fox, 'CONTEST'ing Chicago. Origins and Reflections: *Lest we forget!*
[12] ICAO Aviation Security Manual - Doc 8973.
[13] David L. Glassman, "Keeping "The Wild" out of "The Wild Blue Yonder": Preventing Terrorist Attacks Against International Flights in Civil Aviation," Penn State International Law Review: (1986) Vol. 4: No. 2, Article 6. http://elibrary.law.psu.edu/psilr/vol4/iss2/6 https://elibrary.law.psu.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1045&context=psilr; Sarah Jane Fox, "Policing aviation and keeping peace: intelligence-fed security," International Journal on World Peace. Vol. XXXVI, no.1 (March - 2019): 63-92. https://ijwp.org/annual-indexes/volume-xxxvi-2019/
[14] The ad-hoc Group of Experts was established on 30 January, 1989.
[15] Sarah Jane Fox. "CONTEST'ing Chicago. Origins and Reflections: *Lest we forget!" International Journal of Private Law* Vol. 8, no. 1, (2015): 73-98, DOI: 10.1504/IJPL.2015.066719. Sarah Jane Fox "To practice justice and right'—international aviation liability: have lessons been learnt?" *International Journal of Public Law and Policy* Vol. 5, no. 2 (2015): 162-182. DOI: 10.1504/IJPLAP.2015.071027
[16] The investigations determined that the cause of the explosion was due to a bomb hidden within a radio-cassette player in a suitcase. The explosive was identified as the plastic explosive SEMTEX, which was used by the military services and for legitimate industries—such as mining. However, it was not detectable by X-ray, possessing a low vapor mass with no discernable smell. One of the first roles for the ad-hoc Group of Experts was to investigate the means to stop the use of the explosive in the future which led to the Convention on the marking of Plastic Explosives for the Purpose of Detection, signed at Montreal on 1 March 1991 and entering into force on June 21, 1998.
[17] During the Court proceeding it was concluded that the responsible suitcase(s) came from the Pan Am feeder flight (Pan Am 103A) from Frankfurt.
[18] The Aviation Security Improvement Act of 1990, Joint Hearing and Markup Before the Committee on Foreign Affairs and the Subcommittee on Aviation of the Committee on Public Works and Transportation, House of Representatives, One Hundred First Congress, Second Session, on H.R. 5200 and H.R. 5732, July 26, and September 27, 1990—United States. Congress. House. Committee on Foreign Affair. Recommendation VIII to DOT and FAA—Title I. H.R. 5200. https://www.congress.gov/bill/101st-congress/house-bill/5732
[19] Located in Arlington County, Virginia, US.
[20] Michael Milde, *Essential Air & Space Law* (The Hague, Netherlands: Eleven International Publishing, 2016), 271; and Sarah Jane Fox, 'To practice justice and right'—international aviation liability: have lessons been learnt? International Journal of Public Law and Policy. (2015) Vol. 5, No. 2, pp. 162–182.
[21] Sarah Jane Fox, "Past Events: *in hindsight! 20-years after 9/11." Issues in Aviation Law and Policy* (in press: Autumn 2021)
[22] Sarah Jane Fox. "CONTEST'ing Chicago. Origins and Reflections: *Lest we forget!" International Journal of Private Law* Vol. 8, no. 1, (2015): 73-98, DOI: 10.1504/IJPL.2015.066719
[23] Entry of the 9/11 Hijackers into the United States. Staff Statement No. 1
[24] Entry of the 9/11 Hijackers into the United States. Staff Statement No. 1
[25] As well as the current 28 Member States of the EU this extends to Norway, Liechtenstein, Iceland and Switzerland. Sarah Jane Fox, "Safety & Security: *The*

influence of 9/11 to the EU Framework." Research in Transportation Economics— Special Edition DOI: 10.1016/j.retrec.2014.07.004 Vol. 45 (2014): 24–33. Note: that 1992 saw the EU's Internal Market for Aviation being born.

[26] Regulation (EC) 300/2008 of the European Parliament and of the Council of 11 March 2002 on common rules in the field of civil aviation security and repealing Regulation (EC) 2320/2002. Also note: that in 2016 the whole set of previous implementing legislation was updated: Commission implementing Regulation (EC) N° 2015/1998 lays down detailed measures for the implementation of the common basic standards on aviation security; Whilst - Commission Regulation (EU) N°72/2010 lays down procedures for conducting Commission inspections in the field of aviation security. Regulation (EC) 2320/2002 of the European Parliament and of the Council of 16 December 2002 establishing common rules in the field of civil aviation security. OJ L355, 30 December, 2002.

[27] Noting the UK left the EU at the end of 2020.

[28] Malcolm Gladwell, Safety in the skies (2001), accessed July, 2021, http://gladwell.com/safety-in-the-skies/

[29] "World Terror," accessed July, 2021, http://edition.cnn.com/2006/WORLD/europe/08/10/uk.terror/ "Airline Terror Trial," Telegraph, accessed July, 2021, http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/6153243/Airline-terror-trial-The-bomb-plot-to-kill-10000-people.html

[30] This relates to the failed bombing of Northwest Flight 253 bound for Detroit (from Amsterdam) by Umar Farouk Abdulmutallab, who had explosives sewn into his underpants. In November 2011 the European Commission adopted the framework on security scanners, which has since been integrated into the new Commission Implementing Regulation (EU) 2015/1998.

[31] Article 5 - Regulation (EC) 300/2008.

[32] Aviation and Transportation Security Act of 2001, Pub L No. 107-71, 115 Stat. 597 (2001)

[33] "Shoe-bomber," In December 2001 there was a further attempt in the US by Richard Reid (also known as Ariq Eja—and as the shoe-bomber) to cause damage/destruction to American Airlines flight 63 by igniting explosives in his shoes, accessed July 29, 2021, http://www.telegraph.co.uk/news/worldnews/northamerica/usa/11388442/Failed-shoe-bomber-Richard-Reid-describes-tactical-regrets-that-mass-murder-mission-failed.html. The Security Act, § 104, 115 Stat. 6060.

[34] The Chicago Convention later updated Annex 6 to read, "From 1 November 2003, all passenger-carrying aeroplanes of a maximum certificated take-off mass in excess of 45,500 kg or with a passenger seating capacity greater than 60 shall be equipped with an approved flight crew compartment door that is designed to resist penetration by small arms fire and grenade shrapnel, and to resist forcible intrusions by unauthorized persons. This door shall be capable of being locked and unlocked from either pilot's station." Convention on International Civil Aviation, Chicago, 1944. Opened for signatories - 4 Dec, 1944, 61 Stat. 1180, 15 U.N.T.S. 295 (entered into force 4 April, 1947).

[35] "Germanwings Flight 9525 - 24 March 2015," accessed July 31, 2021, https://www.bea.aero/uploads/tx_elydbrapports/BEA2015-0125.en-LR.pdf

[36] "EASA," later re-issued advise for minimum cockpit occupancy in Europe—EASA SIB_2016-9 21 July 2016. https://ad.easa.europa.eu/ad/2016-09

[37] 49 U.S. Code § 44917 - Deployment of Federal air marshals 49 CFR 1544.223 - Transportation of Federal Air Marshals.

[38] Ariel Merari, "Attacks on civil aviation: Trends and lessons," in *Aviation terrorism and security,* ed. Paul Wilkinson & Brian M. Jenkins (London: Frank Cass Publishers, 1999), 2-6.

[39] In Europe, Regulation 300/2008 specifies that it is for each Member State to determine whether to deploy in-flight security officers on aircraft registered in that

https://digitalcommons.usf.edu/jss/vol14/iss3/6
DOI: https://doi.org/10.5038/1944-0472.14.3.1964

Member State or on flights of air carriers licensed by them in accordance with paragraph 4.7.6 of Annex 17 to the Chicago Convention. 'ANALYSIS - Federal Air Marshal Service's Failure To Adapt To New Aviation Threats Is Alarming' by Clay Biles, 8 March 2015 and 23 February 2017: http://www.hstoday.us/single-article/analysis-federal-air-marshal-services-failure-to-adapt-to-new-aviation-threats-is-alarming/3cbd3070399904dbb5d5af426e778efd.html http://www.hstoday.us/briefings/daily-news-analysis/single-article/special-analysis-federal-air-marshals-fail-to-assess-capabilities/78940370dd6aa9cddb801ef4cd1d6085.html; Schneier blog (2010) https://www.schneier.com/blog/archives/2010/04/the_effectivene.html

40 Article 3 - United Declaration of Human Rights. Paris 10 December 1948 General Assembly resolution 217A.

41 The following issues were identified by the EU and UK Parliaments: The collection of more information than is needed for this purpose, standards of accuracy slip, and the sharing of information with those not responsible for counter-terrorism and/or used for other purposes. EP Resolution on EU judicial cooperation with the United States in combating terrorism accessible http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P5-TA-2001- 0701+0+DOC+XML+V0//EN&language=EN . According to this text the EP considered "... that the US Patriot Act, which discriminates against non-US citizens, and President Bush's executive order on military tribunals are contrary to the principles established. ..."

42 For example—it is identified that personal records run the risk of being hacked or compromised, which again presents a security threat.

43 It is argued that national security is therefore compatible with Article 3 of the UDHR: which recognizes that: "Everyone has the right to life, liberty and security of person." Sarah Jane Fox, "Mobility and Movement Are 'Our' Fundamental Rights". . . Safety & Security—Risk, Choice & Conflict! *Issues in Aviation Law and Policy* 17, no. 1. (Autumn 2017): 7-43.

44 Fox, "Mobility and movement" "The post 9/11 review suggested the need for strong institutions that overcome national and organizational silos that prevent inefficient coordination"—this finding was instrumental in leading to the creation of the Department for Homeland Security. UN WSIS Conference, Geneva, 12 June, 2017.

45 The Aviation and Transportation Security Act of 2001 in the US (adopted on 19 November 2001) gave the Bureau of Customs and Border Protection (CBP), within what is now the DHS, and the Transportation Security Administration (TSA) authority to require access to Passenger Name Record data.

46 Note this is different to the transfer of advance passenger information or the Advance Passenger Information System (APIS). APIS simply allows the country of destination to access at the time of departure of a flight information about the identities of passengers which it would otherwise receive on the arrival of the passengers. This basic information is held on the airlines' own departure control systems and is mostly derived from the machine-readable sections of passports.

47 Directive 95/46 of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L281, 23 November 1995, p 31.

48 Data profiling is the determination of characteristics or combinations of characteristics which might identify someone or something as being potentially worthy of investigation. Data mining is the use of advanced algorithms to trawl through huge databases to discover someone or something matching that profile. This has often been raised as a concern: "Ryan – Letter"—as identified in a letter to from Ms Joan Ryan MP, Parliamentary Under-Secretary of State, Home Office, UK (30 March, 2007), accessed July 15, 2021, https://publications.parliament.uk/pa/ld200607/ldselect/ldeucom/108/10805.htm. The Consultative Committee of the Centre for the protection of individuals with regard to automatic processing of personal data. 'Passenger Names Records, data mining and data protection: the need for strong safeguards. Council of Europe. Strasbourg, 15

June, 2015, accessed July 29, 2021, https://rm.coe.int/16806a601b. "Frattinin–Letter" Letter of 9 January 2007 from Privacy International to the EU Vice-President, Frattini, accessed July 15, 2021, https://publications.parliament.uk/pa/ld200607/ldselect/ldeucom/108/10805.htm

49 Agreement between the United States of America and the European Union on the use and transfer of Passenger name records to the United States Department of Homeland Security, OJ L 215, 11.8.2012, p. 5.

50 This said some members (such as the UK) have operated a stand-alone system for PNR.

51 ICAO Guidelines on Passenger Name Record (PNR) Data Doc 994.

52 It should also be identified that airlines have collected and processed their passengers' PNR data for their own commercial purposes.

53 Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. OJ L 119, 4.5.2016, p. 132–149. The API Directive—Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data. OJ L 261, 6.8.2004, p. 24–27.

54 Aimed at immigration control in the main.

55 European Parliament 13 April 2016—"On the arrivals board: airline passenger data sharing," https://www.europarltv.europa.eu/en/programme/security/on-the-arrivals-board-airline-passenger-data-sharing. Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. OJ L 119, 4 May, 2016, p. 132–149.

56 Directive (EU) 2016/681 requires Member States to bring into force the laws, regulations, and administrative provisions necessary to comply by May 25, 2018 - Article 18.

57 United Nations Security Council Resolution 2178 (2014) and 2309 (2016).

58 Dr Fang Liu—Hong Kong, August 12, 2021 (ICAO TRIP Seminar Hong Kong, China). Note: Juan Carlos Salazar will succeed Dr Fang Liu as the Secretary General of the International Civil Aviation Organization from 1 August 2021.

59 A view expressed by Philip Baum a UK aviation security consultant, author of *Violence in the Skies: a history of aircraft hijacking and bombing*, (UK: Summersdale Publishing, 2016).

60 Dai Whittingham (Chief Executive of the UK Flight Safety Council), "Would passenger profiling at airports stop terrorists?" *Daily Mail,* March, 30 2016 https://www.dailymail.co.uk/travel/travel_news/article-3458787/Would-passenger-profiling-airports-stop-terrorists-Expert-says-controversial-Israeli-techniques-successful-predictable-checks-scans.html

61 Cybercrimes are criminal acts that are committed online by using electronic communications networks and information systems.

62 The USA PATRIOT Act of 2001 (42 U.S.C. § 5195c(e)) defined 'critical infrastructure' as systems and assets, whether physical or virtual, so vital to our nation that their incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these.

63 Sarah Jane Fox, "Flying challenges for the future: Aviation preparedness—in the face of cyber-terrorism," *Journal of Transportation Security*. Volume 9, Issue 3, (December 2016): 191–218, https://doi.org/10.1007/s12198-016-0174-1. Part delivered to the UN—ITU: Challenges for the future: preparedness!—In the face of cyber-terrorism. Safety, Security and Disasters. WSIS Forum EC Medici Framework. 2-6 May, 2016—UN, Geneva.

64 ICAO Secretary General, Dr. Fang Liu—7 July, 2017, Montréal and New York.

65 ICAO Secretary General, Dr. Fang Liu—7 July, 2017, Montréal and New York

66 Sarah Jane Fox, "Flying challenges for the future: Aviation preparedness—in the face of cyber-terrorism," *Journal of Transportation Security*. Volume 9, Issue 3, (December 2016): 191–218, https://doi.org/10.1007/s12198-016-0174-1. Whereby

https://digitalcommons.usf.edu/jss/vol14/iss3/6
DOI: https://doi.org/10.5038/1944-0472.14.3.1964

definitions are applied for 'hacking' ('cracking') 'jacking' and 'spoofing.' Namely, 'Hacking' is explained as a "technical effort to manipulate the normal behaviour of network connections and systems which are connected. Whilst it is often cited that malicious attacks on computer networks are officially known as *cracking*, as *hacking* is often applied to activities having good intentions." "Jacking" refers to the emission of radio signals aiming at disturbing the transceivers operations," "Advances in Intelligent Systems and Computing International Joint Conference," SOCO'13-CISIS'13- ICEUTE'13, Springer, 2014. And "spoofing' refers to a faked/false sending address of a transmission to gain illegal unauthorized entry into a secure system." Cyber Security Glossary, accessed October, 2016, http://niccs.us-cert.gov/

67 According to the CPNI (UK Centre for Protection of the National Infrastructure), "Cyberspace" 'is the term used to describe the electronic medium of digital networks used to store, modify and communicate information. It includes the Internet but also other information systems that support businesses, infrastructure and services.'

68 AVSECP/21, 22-26 March 2010.

69 It became effective on March 26, 2011 and applicable on July 1, 2011

70 Sarah Jane Fox, "Flying challenges for the future: Aviation preparedness—in the face of cyber-terrorism," *Journal of Transportation Security*. Volume 9, Issue 3, (December 2016): 191–218, https://doi.org/10.1007/s12198-016-0174-1.

71 European Aviation Safety Agency website: https://www.easa.europa.eu/home European Centre for Cybersecurity in Aviation: "ECCSA is an initiative supported by EASA aimed at increasing collaboration and information sharing amongst aviation stakeholders, a key enabler for implementing a resilient aviation cyberspace."

72 Jorge Valero, "Hackers bombard aviation sector with over 1,000 attacks per month," Euractiv.com, 11, July 2016, accessed August 1, 2021, https://www.euractiv.com/section/justice-home-affairs/news/hackers-bombard-aviation-sector-with-more-than-1000-attacks-per-month/

73 Sarah Jane Fox, "Flying challenges for the future: Aviation preparedness—in the face of cyber-terrorism," *Journal of Transportation Security*. Volume 9, Issue 3, (December 2016): 191–218, https://doi.org/10.1007/s12198-016-0174-1.

74 EASA. https://www.easa.europa.eu/faq/46475

75 "What is Next Gen?" Federal Aviation Administration (FAA), accessed July 28, 2021, https://www.faa.gov/nextgen/what_is_nextgen/

76 US Government Accountability Office (GAO) Report 'FAA Needs to Address Weaknesses in Air Traffic Control Systems.' Reference - GAO-15-221 FAA Air Traffic Control Information Security, last modified January, 29 2015, accessed August 1, 2021. Sarah Jane Fox, "Flying challenges for the future: Aviation preparedness—in the face of cyber-terrorism," *Journal of Transportation Security*. Volume 9, Issue 3, (December 2016): 191–218, https://doi.org/10.1007/s12198-016-0174-1.

77 Sarah Jane Fox, "Flying challenges for the future: Aviation preparedness—in the face of cyber-terrorism," *Journal of Transportation Security*. Volume 9, Issue 3, (December 2016): 191–218, https://doi.org/10.1007/s12198-016-0174-1. Patrick Ky (Director of EASA speaking at the Association de Journalistes Profeeionnels de l'Aéronautique et de l'Espace (AJPAE) in 2015 making reference to an ICAO report the previous year (2014), http://www.scmagazineuk.com/european-aviation-body-warns-of-cyber-attack-risk-against-aircraft/article/444487/

78 Ky Aviation body warns of cyber attack risk.

79 "*Task Force on Resilient Military Systems and the Advanced Cyber"* Department of Defense—Defense Science Board (DSB), last modified January, 2013, https://fas.org/irp/agency/dod/dsb/.

80 "Transportation Risk Index Analyses report (2016)," Willis Towers Watson, accessed August 1, 2021, https://www.willistowerswatson.com/en/insights/2016/09/transportation-risk-index-2016

81 Transportation Risk Index (2016)

82 US Government Accountability Office (GAO) Report 'FAA Should Fully Implement Key Practices to Strengthen Its Oversight of Avionics Risks.' Reference—GAO-21-86.

October 2020, https://www.gao.gov/assets/gao-21-86.pdf. Highlights of GAO-21-86 - https://www.gao.gov/products/gao-21-86

[83] "Transportation Risk Index Analyses report (2016)," Willis Towers Watson, https://www.willistowerswatson.com/en/insights/2016/09/transportation-risk-index-2016

[84] Sarah Jane Fox, "Mobility and Movement Are 'Our' Fundamental Rights". . . Safety & Security—Risk, Choice & Conflict! *Issues in Aviation Law and Policy* 17, no. 1. (Autumn 2017): 7-43.

[85] National Academy of Sciences, 1991, p.7. Myriam Dunn Cavelty, "CyberTerror–Looming Threat or Phantom Menace? The Framing of the US CyberThreat Debate," *Journal of Information Technology & Politics*, (2007) Vol. 4(1).

[86] Speech to the National Academy of Sciences. *Keeping America Secure for the 21st Century*. Proc Natl Acad Sci USA, 96(7) (Mar 30 1999): 3486–3488, http://www.ncbi.nlm.nih.gov/pmc/articles/PMC34291/ accessed 15 May, 2016.

[87] Gabriel Weimann, "Cyberterrorism How Real Is the Threat?" United States Institute of Peace. December 2004, https://www.usip.org/sites/default/files/sr119.pdf

[88] Remarks by Homeland Security Director Tom Ridge to the Electronics Industries Alliance. Washington D.C. April, 23, 2002, https://georgewbush-whitehouse.archives.gov/news/releases/2002/04/20020423-15.html.

[89] Feb. 12, 2013

[90] Singapore, 9-10 July 2015.

[91] "Cyber Threat to Civil Aviation," European Cockpit Association, Brussels, 28.04.2017. https://www.eurocockpit.be/file/2833/download?token=b6rQSd9g

[92] Sarah Jane Fox, "Flying challenges for the future: Aviation preparedness—in the face of cyber-terrorism," *Journal of Transportation Security*. Volume 9, Issue 3, (December 2016): 191–218, https://doi.org/10.1007/s12198-016-0174-1.

[93] Sarah Jane Fox, "Challenges for the future: preparedness!—In the face of cyber-terrorism. Safety, Security and Disasters." WSIS Forum EC Medici Framework. 2-6 May, 2016, UN, Geneva.

[94] The Convention on the Suppression of Unlawful Acts relating to International Civil Aviation. ICAO Doc. 9960, Signed at Beijing on 10 September 2010. Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft (Beijing Protocol of 2010) (ICAO Doc. 9959). Ruwantissa, Abeyratne, "The Beijing Convention of 2010 on the suppression of unlawful acts relating to international civil aviation—an interpretative study," *Journal of Transportation Security*, Vol. 4, no. 2, (2011): 131–143, https://doi.org/10.1007/s12198-011-0062-7.The 2010 Beijing Protocol (to the 1971 Hague Convention on the Suppression of Unlawful Seizure of Aircraft.)

[95] "Each Contracting State must develop measures in order to protect information and communication technology systems used for civil aviation purposes from interference that may jeopardize the safety of civil aviation." (Chapter 4—Annex 17*)*

[96] ICAO Safety Report, 2017 Edition. https://www.icao.int/safety/Documents/ICAO_SR_2017_18072017.pdf

[97] ICAO Working Paper, Assembly — 39th Session Executive Committee Technical Commission. Cyber Resilience in Civil Aviation (Agenda Item 16 Aviation security & Agenda Item 36: Aviation safety and air navigation implementation support) A39-WP/99, 27 July, 2016.

[98] The Director of Strategy and Safety Management at European Aviation Safety Agency, reported by Jorge Valero, "Hackers bombard aviation sector with over 1,000 attacks per month" Euractiv.com, 11, July 2016.

[99] "The Zettabyte Era—Trends and Analysis," Cisco—whereby this is anticipated to occur within 2018, accessed August 1, 2021, http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/VNI_Hyperconnectivity_WP.html.

[100] As Fox explains drones are known by various names and abbreviations, such as UAV's (the Unmanned Aerial Vehicle's)—"mostly used as a general reference (alongside drone) by the general population. RPA/S (Remotely Piloted Aircraft or Remotely

https://digitalcommons.usf.edu/jss/vol14/iss3/6
DOI: https://doi.org/10.5038/1944-0472.14.3.1964

Piloted Aircraft System)—used mostly by International and National Aviation Agencies; UAS (Unmanned Aerial System)—still largely used by the US (and UK); UA (unmanned aircraft) cited within EU (proposed) legislation." Sarah Jane Fox, "THE RISE OF THE DRONES: *Framework and Governance—Why risk it!*" *82 J. Air L. & Com.* (2017): 683-715, https://scholar.smu.edu/jalc/vol82/iss4/2.

[101] "The global commercial drone market size was valued at USD 13.44 billion in 2020. It is expected to expand at a compound annual growth rate (CAGR) of 57.5% from 2021 to 2028." https://www.grandviewresearch.com/industry-analysis/global-commercial-drones-market. Sarah Jane Fox, "THE RISE OF THE DRONES: *Framework and Governance—Why risk it!*" *82 J. Air L. & Com.* (2017): 683-715, https://scholar.smu.edu/jalc/vol82/iss4/2.

[102] Fox, THE RISE OF THE DRONES: *Framework and Governance—Why risk it!*

[103] "Biggest National Threat," Information Age, last modified April 2, 2017: http://www.information-age.com/drones-biggest-threat-national-security-123465587/

[104] The UK government announced plans to introduce drone registration and safety awareness courses for owners of the small unmanned aircraft, last modified July 22, 2017. http://www.bbc.co.uk/news/technology-40684581. This now affects anyone who owns a drone which weighs more than 250 grams (8oz) Civil Aviation Authority (CAA), https://register-drones.caa.co.uk/individual.

[105] Not only to those using the airspace but also for those on the ground. In 2020 two new EU Regulations came into force: which went someway to creating standardization: Commission Implementing Regulation (EU) 2019/947, which relates to the acceptable means of compliance (AMC) and guidance material (GM), and the Commission Delegated Regulation (EU) 2019/945 on unmanned aircraft systems (UAS) and on third-country operators of UAS.

[106] Civil Aviation Authority (CAA) - Airspace restrictions for unmanned aircraft and drones, https://www.caa.co.uk/Consumers/Unmanned-aircraft/Our-role/Airspace-restrictions-for-unmanned-aircraft-and-drones/.

[107] The report in the Independent stated that an "Airbus A320 was flying over east London when the crew spotted two white orb-shaped drones below the aircraft," accessed July 21, 2021 http://www.independent.co.uk/news/uk/home-news/drones-plane-crashes-airbus-a320-heathrow-airport-near-miss-incident-london-multiple-civil-aviation-a7709841.html. Telegraph (online) "Crackdown on drones planned after latest near miss" last modified June, 24 2017, accessed July 21, 2021, http://www.telegraph.co.uk/news/2017/06/24/crackdown-drones-planned-latest-near-miss/

[108] BBC News Online, last modified November, 17, 2020, accessed June 26, 2021, https://www.bbc.co.uk/news/uk-england-manchester-54972831

[109] Sarah Jane Fox, The Rise of the Drones: *Framework and Governance—Why risk it! 82 J. Air L. & Com.* 683-715 (2017). Emerging Risk Report—2015, *Innovation Series. Drones Take Flight—Key issues for insurance*. Lloyd's.

[110] Emerging Risk Report—2015

[111] Sarah Jane Fox, "Flying challenges for the future: Aviation preparedness—in the face of cyber-terrorism," *Journal of Transportation Security*. Volume 9, Issue 3, (December 2016): 191–218, https://doi.org/10.1007/s12198-016-0174-1. Sarah Jane Fox, "The Rise of the Drones: *Framework and Governance—Why risk it!*" *82 J. Air L. & Com.* (2017): 683-715, https://scholar.smu.edu/jalc/vol82/iss4/2.

[112] Article 3 says: Civil and state aircraft "(a) This Convention shall be applicable only to civil aircraft, and shall not be applicable to state aircraft. (b) Aircraft used in military, customs and police services shall be deemed to be state aircraft. (c) No state aircraft of a contracting State shall fly over the territory of another State or land thereon without authorization by special agreement or otherwise, and in accordance with the terms thereof."

[113] See for example the controversy as reported in Popular Mechanics (online) 1, August, 2017: "Debunking the 9/11 Myths: Special Report - The Planes," http://www.popularmechanics.com/military/a5654/debunking-911-myths-planes/

http://www.nbcnews.com/id/5232563/ns/us_news-security/t/panel-bid-intercept-jets was-flawed/#.Wa0j2K2ZO80.

[114] The National Commission on Terrorist Attacks Upon the United States (The 9/11 Commission Report): 18, http://govinfo.library.unt.edu/911/about/index.htm.

[115] The interception of a civil aircraft.

[116] Surface-to-air missile (SAM) systems; ground-to-air missile (GTAM) and other anti-aircraft missiles.

[117] It had left Amsterdam, bound for the Malaysian capital Kuala Lumpur.

[118] The Dutch Safety Board report, https://www.onderzoeksraad.nl/en/onderzoek/2049/investigation-crash-mh17-17-july-2014/publicatie/1658/dutch-safety-board-buk-surface-to-air-missile-system-caused-mh17-crash

[119] ICAO will complete the work program in 2018. This will also see the Dutch Safety Board drawing its conclusion in 2018.

[120] This concerns both the crash and the processing of passenger information.

[121] Emphasis added.

[122] Transportation Risk Index Analyses report (2016) Willis Towers Watson, https://www.willistowerswatson.com/en/insights/2016/09/transportation-risk-index-2016

[123] "Laser strikes," according to the Aviation Week Network (online) "[i]n one incident, an airline pilot claimed a laser strike at 16,000 ft.; another, experienced by a different aircraft, allegedly occurred at FL 300," last modified Jan. 15, 2016, accessed July 23, 2021, http://aviationweek.com/business-aviation/risk-laser-attacks-pilots-real-and-growing

[124] "Laser strikes," Aviation Week. UK CAA response: https://www.caa.co.uk/Safety-initiatives-and-resources/How-we-regulate/Safety-Plan/Mitigating-key-safety-risks/Lasers/. FAA: https://www.faa.gov/about/initiatives/lasers/hazards/. ICAO Working Paper A38-WP/252: Addressing the aviation safety concerns affecting flight safety involving laser emitters.

[125] Civil Aviation Navigation Services Organisation, https://www.canso.org/sites/default/files/Article%20-%20Airspace%20Q4%202014%20-%20Laser%20attacks.pdf

[126] Commission Implementing Regulation (EU) 2021/255 of 18 February 2021 amending Implementing Regulation (EU) 2015/1998 laying down detailed measures for the implementation of the common basic standards on aviation security (Text with EEA relevance), C/2021/992OJ L 58, 19.2.2021, p. 23–35.

[127] Clifford R. Bragdon, *Transportation Security and Its Impact*, *in Transportation Security* (Butterworth-Heinemann, 2008). Sarah Jane Fox, "Mobility and Movement Are 'Our' Fundamental Rights." Safety & Security—Risk, Choice & Conflict! *Issues in Aviation Law and Policy* 17, no. 1. (Autumn 2017): 7-43,

[128] See section on *Cyber-terrorism* (comments of Tom Ridge).

[129] See comments within the Introduction.

[130] Sarah Jane Fox, An '*obligation*' to provide air travel: *In the Covid-19 era* (A European perspective). *Issues in Aviation Law and Policy* (Autumn 2020).

[131] Particularly critical to the infrastructure, or where crowds gather on mass.

[132] Reference to Giovanni Bisignani's comments (cited earlier) concerning, September, 11, 2001 as "*the day that changed the world*."

https://digitalcommons.usf.edu/jss/vol14/iss3/6
DOI: https://doi.org/10.5038/1944-0472.14.3.1964