Ruwantissa Abeyratne

Rulemaking in Air Transport

A Deconstructive Analysis

Springer

Rulemaking in Air Transport

Ruwantissa Abeyratne

Rulemaking in Air Transport

A Deconstructive Analysis

Springer

Ruwantissa Abeyratne
Aviation Strategies International
Montreal, Québec
Canada

ISBN 978-3-319-44656-1 ISBN 978-3-319-44657-8 (eBook)
DOI 10.1007/978-3-319-44657-8

Library of Congress Control Number: 2016950568

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG Switzerland

To Wybo Heere for his excellent contributions and dedication to Air and Space Law

Preface

This book embarks on a discussion of rulemaking in air transport and its processes and legalities, starting with a deconstruction of work carried out at the time of writing in various fields of air transport by the International Civil Aviation Organization (ICAO) which should be at the apex of rulemaking. This initial discussion, which demonstrates the weakness of rulemaking in the air transport field for lack of direction, purpose, and structure in the development of authoritative rules and regulations that should serve as compelling directives from the main organization responsible for aviation, leads to an evaluation of the fundamental principles of rulemaking in ICAO, the Federal Aviation Administration (FAA) of the United States, and the European Commission (EC).

Essentially, rulemaking is the process where governments convert the broad policy embodied in the bilateral or multilateral treaties they ratify into rules that are applicable to their people, thus providing direction and purpose to the governance process. Rules define the mission of a government and bind people to certain conduct that accord with international and internal policy.

Rules are not legislation. They are the results of deliberations of the people in their constituent assemblies that have passed a vote. As Justice Oliver Wendell Holmes put it aptly, rules are the skin of a living policy that crystallizes an inchoate normative policy into hard words that are clear and intelligible to the ordinary person. Of course, the living policy has its genesis either in ratified treaties or enacted local laws, or even decisions of the legal hierarchy of a land.

The problem with rulemaking in air transport is that, particularly in the economic field but other fields as well, there are no global rules applicable to States that can be enforceable. This is largely because of an inherent anomaly in the realm of international civil aviation. For instance, the Convention on International Civil Aviation (Chicago Convention) in its preamble states that air services will be operated soundly and economically, giving each player equality of opportunity. At best, this statement is ambiguous as it has not been elaborated upon or defined. As a result, regional bodies such as the European Commission and local bodies such as the Federal Aviation Administration (FAA) of the United States have developed

their own system of rulemaking and adopted their own rules. From a competition point of view, airlines—constrained by a curious provision in the Chicago Convention that no scheduled air service may be operated into and out of the territory of a State unless permission of that State is obtained—have adopted what is called "spontaneous private deregulation" which is essentially a process which ignores dubious or obsolete concepts such as "equality of opportunity" and apply innovation and creative marketing strategy that circumvents such restraints.

As already stated, at the apex of this anomaly is ICAO, which is neither a legislative body nor a judicial tribunal, although on the subject of legislation, ICAO can have some persuasive authority on States in terms of its policies and guidance material which may or may not be incorporated by States as their domestic rules and regulations. To make matters worse, academics (who have not worked at ICAO) often misquote the Chicago Convention or demonstrate their ignorance of the meaning, purpose, and functions of ICAO as happened at the ICAO Air Transport Symposium with the ambitious title *Addressing Competition Issues: Towards a Better Operating Environment* held at ICAO Headquarters on March 30–31, 2016. At this symposium, one academic was vocal and vehement that ICAO should proclaim a global competition law on air transport. This claim is not only both baseless and unfounded but also plain wrong. The same person advocated that ICAO should establish a judicial tribunal to adjudicate on disputes between States, only to be endorsed by another academic who misquoted ICAO's dispute resolution provisions in the Chicago Convention saying that ICAO could indeed adjudicate disputes as it was a judicial body.

The first step therefore is to know what we are talking about and determine the rulemaking process in air transport accordingly. It is hoped that this book sheds some light on the subject.

Montreal, QC, Canada Ruwantissa Abeyratne
July 2016

Contents

Chapter 1
How Not to Make Rules

1.1 Introduction

Rulemaking is intrinsically linked with the perceived inadequacy of international law, the sources of which should be the genesis of rulemaking by a State. While on the one hand the entrenched principle of sovereignty of States enable a State to make its own rules and laws, on the other hand, the Sate may be circumscribed by the ambivalence of international law. In air transport, the law which stands as the fundamental postulate is the Chicago Convention which in its Article 1 recognizes State sovereignty. The provisions of the Chicago Convention give rise to its Annexes, policies of the ICAO Council, Assembly Resolutions and guidelines issued by ICAO. At the cornerstone of international law lies the concept of State sovereignty which Jean Bodin defined as the absolute and perpetual power within a State.[1] Sovereignty, according to Bodin therefore the highest power wielded over citizens of a State and was exercised by a State on its subjects and anyone else who was present in the State's territory at the time in question. This power also included a State authority and power to make laws. Bodin however, believed that sovereignty of a State was subject to divine laws (presumably, religious tenets) and laws of nature. He also believed that the sovereignty of a State was subservient to certain human laws common to all nations.[2] The idea that a law of nations, common to all mankind, was at least theoretically applicable to all sovereign States was thus conceived.

The International Court of Justice in 1970 judicially recognized this principle in the *Barcelona Traction* case when it recognized that international law places certain obligations upon States***, erga omnes,*** i.e. obligations owed to the international community as a whole. The Court opined:

[1]Bodin (1955), pp. 25–36.

[2]See Rajan (1958), p. 3.

R. Abeyratne, *Rulemaking in Air Transport*, DOI 10.1007/978-3-319-44657-8_1

> such obligations derive, for example, in contemporary international law from the outlawing of acts of aggression, and of genocide, as also from the principles and rules concerning the basic rights of the human person, including protection from slavery and racial discrimination.[3]

International law anchors its validity on two elements: The sources of international law; and the general principles of law applicable to treaties.[4] The sources of international law are reflected in Article 38 of the Statute of the International Court of Justice which provides that when the Court exercises its jurisdiction to adjudicate upon disputes according to the principles of international law, the Court shall apply:

(a) international conventions, whether general or particular, establishing rules expressly recognized by the contracting States;
(b) international custom, as evidence of a general practice accepted by law;
(c) the general principles of law recognized by civilized nations; and,
(d) subject to the provisions of Article 59,[5] judicial decisions and teachings of the most highly qualified publicists of the various nations, as subsidiary means for the determination of rules of law.

There are certain fundamental inconsistencies that are identifiable with the sources of international law when they are applied practically. Firstly, the basic techniques that are applied to any system of law in order to establish its compelling and binding nature tend to be left confused in the realm of international law. These techniques are:

1. lex superior derogat inferiori : rules derived from one source prevail over rules derived from another;
2. lex posterior derogat priori : latter rules prevail over earlier ones;
3. lex specialis derogat generali : a particular or special rule prevails over a general rule.

The problem with the application of the above techniques to international law is that sources such as international custom and the general principles of international law as recognized by civilized nations cannot be determined in a chronological sense to accord with the above since custom and the acceptance of legal principles as universal law take time and hence would be indeterminable as applicable law at a given time.[6]

The next problem to be considered is the application by the International Court of Justice of the "general principles of law recognized by civilized nations" as provided for in Article 38(c) of the Statute of the International Court. Are the general principles of law "recognized" by the civilized nations the same as those

[3] Case Concerning the Barcelona Traction Light and Power Co., (Belgium v. Spain) 1970 *I.C.J.* 32.

[4] Brownlie (1990), p. 1.

[5] Article 59 provides that the decision of the Court has no binding effect except between the parties and in respect of that particular case.

[6] Akehurst (1974–1975), p. 273.

that are developed and codified as principles of international law, initiated by the United Nations General Assembly by Article of the United Nations Charter? The General Assembly does not have full and universal legislative powers,[7] and any codification of the principles of international law that emanates from being initiated by the United Nations General Assembly would only be persuasive. In this environment, it would remain increasingly difficult for the International Court of Justice to determine as to what laws are "recognized" by civilized nations as the general principles of law.[8]

Over and above the customary and other principles of international law which may be considered as the "recognized" principles of international law, there is also the **jus cogens** or "compelling law" which takes precedence in the realm of international law.[9] Article 53 of the Vienna Convention on the Law of Treaties, which was adopted on 23 May 1969, (hereafter referred to as the Vienna Convention)[10] provides that treaties conflicting with a peremptory norm of general international law (jus Cogens) would be void. The Article states:

> A treaty is void, if, at the time of its conclusion, it conflicts with a peremptory norm of general international law. For the purpose of the present Convention, a peremptory norm of general international law is a norm accepted and recognized by the international community of States as a whole as a norm from which no derogation is permitted and which can be modified only by a subsequent norm of general international law having the same character.

Article 64 of the Vienna Convention runs as follows:

> If a new peremptory norm of international law emerges, any existing treaty which is in conflict with that norm becomes void and terminates.

The *jus cogens* therefore admits of no derogation by the will of the contracting parties whether in the drafting of the treaty provisions or interpretation thereof. It is also generally accepted that the *jus cogens* principle as enunciated in the Vienna Convention and accepted as a general principle of international law applies only to treaties and not to unilateral acts by States such as those that may commonly seen in instances of extradition and violation of security of one State by another.[11] This would then imply that a peremptory norm of international law or the *jus cogens*, if violated by the act of a State does not stand void ab initio at international law but

[7] Fawcett (1971), pp. 65–66.

[8] Lord Oliver has stated:

> a rule of international law becomes a rule – whether accepted into domestic law or not – only when it is certain and is accepted generally by the body of civilised nations; and it is for those who assert the rule to demonstrate it, if necessary before the International Court of Justice. It is certainly not for a domestic tribunal in effect to legislate a rule into existence for the purposes of domestic law and on the basis of material that is wholly indeterminate. (1989) 3 W.L.R. 969 H.L. See also generally, Robert Y. Jennings, An International Lawyer Takes Stock, *I.C.L.Q*. Vol 39, Part 3, July 1990, 513-529.

[9] Whiteman (1977), pp. 609–613.

[10] *Vienna Convention on the Law of Treaties*, U.N. Doc. A/Conf.39/27, 23 May 1969.

[11] Sztucki (1974), p. 69.

rather, requires individual action by States so that the status quo ante is restored. In such instances, logically, the International Court of Justice would, when adjudicating upon breaches of international law and consequent action by States, treat the *jus cogens* as a principle of international law under Article 36(1) of the United Nations Charter. This would, in turn, render the *jus cogens* destitute of its compelling effect on the conduct of nations and relegate it to the same level as any other norm of international law when a unilateral action of a State is adjudicated upon.

A peremptory norm of international law is presumed to be based on morality. Therefore, *jus cogens* would essentially have its origins in moral tenets—such a right of a State to its security and self-determination inter alia. There are also, in close juxtaposition to these moral principles, certain compelling concepts of customary international law such as State sovereignty which in turn are sufficiently peremptory to be considered a form of jus cogens. Where then is one to draw the line between jus cogens and customary international law? As one legal commentator observes.

Jus cogens is something of a contradictio in terminis as far as international law is concerned. For how can jus cogens, as a concept introducing morals into international law, be reconciled with the age old basis of international law, called sovereignty? It can be argued that the principle of sovereignty, which by definition has to be an absolute one in the sense of being "in principle not being accountable in law to any other authority", itself is a rule of jus *cogens* in its purest form; thus, in a way, it is a problem that bites itself in its tail.[12]

To make matters worse, the Vienna Convention in its Article 53 stipulates that a peremptory norm of general international law (jus cogens) is a norm accepted and recognized by the international community of States as a norm from which no derogation is permitted and which can be modified only by a subsequent norm of general international law having the same character. This could only mean that there are norms of international law that can be changed and indeed, can be derogated from. Called jus dispositivum, these norms can be derogated from by mutual consent between States. In this sense, principles of State sovereignty may become jus dispositivum, although the very essence of international law, and indeed air law, is based on this premise of State sovereignty. Although therefore **jus cogens** has priority over jus dispositivum, it does not make sense since the concept of State sovereignty which is the fundamental norm cannot be logically overridden by jus cogens, which arrives on the scene later.

The confusion that has been created by the various types of concepts permeating international law seriously affects the development of clear principles and functional parameters of international law. These concepts should be reconciled though a more cogent system of international law, thereby giving new meaning to the legal protection of the international community against the unlawful interference with international civil aviation.

The most fundamental principle in rulemaking is that the genesis of the rule should be authoritative. The most common form of rulemaking in air transport is the

[12]von der Dunk (1992), p. 219.

adaptation of an international treaty provision or a derivative thereof to a domestic or local regulatory regime. For example, the principles contained in the fundamental postulate of air transport law—The Convention on International Civil Aviation (Chicago Convention)[13]—being the genesis of rules and regulations on the subject, and its derivatives—mainly the 19 Annexes to the Chicago Convention—are generally transposed into the local laws of a contracting State to the Convention, firstly by recognition of its legislature and secondly by executive order or regulation.

Regrettably, this process does not always take place smoothly in air transport due to the weakness of the regulatory process at the top level—The International Civil Aviation Organization (ICAO).[14] I will discuss five current issues of critical importance—cyber terrorism in air transport; leasing and transfer of functions of aircraft; remotely piloted aircraft; climate change; and competition law in air transport, with a discussion on the nature of the issues involved with a view to illustrating where States have not been given the impetus they need to make their own domestic rules due to a watered down and weak foundation built by ICAO with respect to these issues. This will be followed by a chapter which recommends the manner in which rules can be made in air transport, starting with ICAO, followed by discussions in chapters to follow on regional and national rulemaking.

1.2 Cyber Terrorism

The Economist of 4 November 2014 speaks of "cyberjacking"—a phenomenon that refers to the equivalent of hijacking an aircraft with the use of cyber technology. This could happen from outside the aircraft or from the inside. The catalyst in this instance is the increasing popularity with passengers of internet connectivity on board for work, games, movies et.al. The article also mentions that internet signals are routed through existing communications architecture, such as the Aircraft Communications Addressing and Reporting System (ACARS), or the Automatic Dependent Surveillance-Broadcast (ADS-B), which is an anti-collision system, which, both being information communications systems can, in theory be targets of cyber-attacks. In its later edition of 21 May 2015 the same journal highlighted

[13]Convention on International Civil Aviation, signed at Chicago on 7 December 1944. See ICAO Doc. 7300/9:2008. See also, Abeyratne (2013) for a discussion and analysis of the Convention. Also, by the same author, Abeyratne (2012a), for a discussion and analysis of the Annexes to the Chicago Convention.

[14]ICAO is the specialized agency of the United Nations handling issues of international civil aviation. ICAO was established by the Convention on International Civil Aviation, signed at Chicago on 7 December 1944 (Chicago Convention). The overarching objectives of ICAO, as contained in Article 44 of the Convention is to develop the principles and techniques of international air navigation and to foster the planning and development of international air transport so as to meet the needs of the peoples for safe, regular, efficient and economical air transport. ICAO has 191 member States, who become members of ICAO by ratifying or otherwise issuing notice of adherence to the Chicago Convention.

that a hacker had identified a weakness with the in-flight entertainment (IFE) systems on Boeing 737-800, 737-900, 757-200 and Airbus A320 aircraft. He had demonstrated this fact by accessing the systems by plugging a laptop into one of the electronic boxes usually found under the seats either side of the aisle. Once connected, the hacker claims to have accessed other systems on the aircraft.

None of these claims have been validated by the scientific community nor have they been put into practice by terrorists or criminals against civil air transport. Nonetheless, this may be a sign of things to come, particularly when one considers that the National Aeronautics and Space Administration's computers have been hacked in the past and that all computer systems of SONY were hacked in the recent past, allegedly by a foreign State sponsored hacking exercise. As this article discusses, there has been at least one confirmed cyber-attack on a computer system of a commercial airline. The International Civil Aviation Organization has been active in the field of prevention of cyber terrorism, which this article will elaborate on, with some constructive suggestions.

On 21 June 2015, hackers attacked the computer system of LOT Polish Airlines, grounding several aircraft, resulting in the grounding of 10 flights and delay caused to 12 other flights. This caused severe inconvenience to nearly 1500 passengers. Cyber-attacks on facilities and infrastructure are here. They are no longer viewed as things to come. For instance, it has been reported that Chinese hackers broke into the computer networks housing the personal information of all federal US government employees in March 2015 in an apparent attempt to target people who had applied for top-secret security clearances. Cyber interference, cybercrime and cyber terrorism against air transport are all offences against civil aviation that end up in unlawful interference with civil aviation, which has been addressed on three major occasions, though the Tokyo Convention of 1963, The Hague Convention of 1970 and the Montréal Convention of 1971. Yet none of these conventions refer, directly or indirectly, to cyber terrorism. The first such Treaty to do so, the 2010 Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation adopted in Beijing, provides in Article 1d) that an offence is committed when a person destroys or damages air navigation facilities or interferes with their operation, if any such act is likely to endanger the safety of aircraft in flight. This clearly refers, inter alia, to cyber terrorism, but links the offence exclusively to the safety of aircraft in flight. Regrettably the Beijing Convention—the only international attempt at hinting at cybercrime—does not seem to cover the LOT Polish situation.

At the apex of the issue is the International Civil Aviation Organization (ICAO) which has been charged by the international community with leading efforts in curbing aviation cybercrime.

1.2.1 Definitions and Issues

At the outset it becomes necessary to define the terms cybercrime and cyber terrorism. In a proposal for an international convention on cybercrimes and terrorism, a cybercrime is defined as conduct with respect to cyber systems that is

classified as an offence under the draft convention.[15] Although cyber terrorism has been simplistically defined as "an assault on electronic communication networks", the proposed convention defines cyber terrorism as the intentional use or threat of use, without legally recognized authority, of violence, disruption or interference against cyber systems, when it is likely that such use would result in death or injury of a person or persons, substantial damage to physical property, civil disorder, or significant economic harm. The Federal Bureau of Investigation of the United States has given a more extensive definition: "the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against non-combatant targets by sub-national groups or clandestine agents".[16]

The term "cyber terrorism" was coined in 1980 by Barry Collins who defined it as "the intimidation of civilian enterprise through the use of high technology to bring about political, religious, or ideological aims, actions that result in disabling or deleting critical infrastructure data or information".[17]

Since the author published his article on cyber security and aviation in 2011[18] the threat of cybercrimes on air transport has decidedly increased.[19] This is because the overall threat on computer security of industry has increased in general terms in

[15]Crime in Cyberspace – First Draft of International Convention Released for Public Discussion, European Committee on Crime Problems (cdpc) Committee of Experts on Crime in Cyber-Space (pc-cy), *Draft Convention on Cyber-crime* (Draft N° 19): 2000. See http://www.iwar.org.uk/law/resources/eu/cybercrime.htm. The Convention, in Article 3 states that if any person unlawfully and intentionally engages in any of the following conduct without legally recognized authority, permission, or consent: (a) creates, stores, alters, deletes, transmits, diverts, misroutes, manipulates, or interferes with data or programs in a cyber-system with the purpose of causing, or knowing that such activities would cause, said cyber system or another cyber system to cease functioning as intended, or to perform functions or activities not intended by its owner and considered illegal under this Convention; (b) creates, stores, alters, deletes, transmits, diverts, misroutes, manipulates, or interferes with data in a cyber-system for the purpose and with the effect of providing false information in order to cause substantial damage to persons or property; (c) enters into a cyber-system for which access is restricted in a conspicuous and unambiguous manner; (d) interferes with tamper-detection or authentication mechanisms; (e) manufactures, sells, uses, posts or otherwise distributes any device or program intended for the purpose of committing any conduct prohibited by Articles 3 and 4 of the Convention. Article 4 covers aiding and abetting the aforesaid offences. See Sofaer et al. (2000), Jointly Sponsored by: The Hoover Institution The Consortium for Research on Information Security and Policy (CRISP); The Center for International Security and Cooperation (CISAC) and Stanford University.

[16]http://defensetech.org/2011/09/12/cyber-terrorism-now-at-the-top-of-the-list-of-security-concerns/.

[17]Tafoya (2016); See also, Abeyratne (2010a), pp. 24–25.

[18]Abeyratne (2011d), pp. 337–339.

[19]President Barack Obama, in his State of the Union Address of 2013 said: "America must also face the rapidly growing threat from cyber-attacks . . . our enemies are also seeking the ability to sabotage our power grid, our financial institutions, our air traffic control systems. We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy." *President Obama Acknowledges Cyber Threat and Signs Executive Order for Improving Critical Infrastructure Cybersecurity*, February 13, 2013. See https://www.cigital.com/blog/president-obama-acknowledges-cyber-threat-and-signs-executive-order/.

recent years. In specific terms, as aviation digitized baggage handling systems, air traffic management information and communication technologies including flight information display systems, the digital sophistication introduced into these systems has spawned opportunity for hackers to exploit the vulnerabilities that came with such advancement. Added to this, computers, which have graduated from desktops and laptops to peoples' pockets are now found in all sorts of gadgets. This trend has prompted Cisco—a manufacturer of network equipment—to point out its concern, that there are currently as many as 15 billion connected devices in the world which could increase to 50 billion by 2020.[20] These have the potential of causing significant damage to life and limb as well as severe financial and economic damage. For example, in 2006 the US Federal Aviation Administration was forced to shut down air traffic control systems in Alaska as a precautionary measure against an attack on the internet. Two years later, in a scary scenario, accident investigators investigating the crash of *Spanair* Flight 5022 of 20 August 2008 involving an MD 82 aircraft,[21] concluded that the aircraft crashed due to the computer system monitoring technical problems on board was infected with malware.[22]

Concerns have also been expressed with regard to the disappearance in March 2014 of Malaysian Airlines Flight MH 370—that someone may have hacked into the airplane's computer system and taken control of the entire flight. One theory (in a newspaper report, which has not been subjected to any formal investigation) was that the hackers could have infiltrated the inflight entertainment system of the aircraft to gain access to the security software on board. It has been reported that a former security adviser to the Home Office of the United Kingdom had advised that the controls of the Boeing 777 (which operated Flight MH 370) could be accessed through a radio signal sent from a small device.[23] It has also been reported that the manufacturer of the Boeing 777 has since introduced modifications to the model 777-200 and -300Er series airplanes which will now have novel and unusual design features associated with the connectivity of the passenger service network systems to the critical airplanes systems and data networks.[24]

[20]Hacking the Planet, *The Economist*, July 18–24 2015, p. 10. In this article *The Economist* also mentions that on 9 July 2015 hackers had infiltrated the US Office of Personnel Management and stolen personal information of 22 million government employees. In another incident in January of the same year hackers had accessed the systems of *Anthem*, a large insurance firm, and purloined security information of 80 million employees. *Ibid.*

[21]Span air flight 5022, operated with a McDonnell Douglas MD82, crashed just after take-off in Madrid-Barajas Airport on 20 August 2008, killing 154 people.

[22]In July 2013 passport control at Istanbul Ataturk International Airport was shut down due to a cyber-attack and in the same year 75 airports in the United States were affected as a result of a cyber-attack and phishing. See Lim (2016) (20182-92), p. 85.4.

[23]Cyber Threats against the Aviation Industry, Posted in *SCADA* on April 8 2014. See http://resources.infosecinstitute.com/cyber-threats-aviation-industry.

[24]*Ibid.*

The disconcerting trend, although based on theoretical conjecture is that, while the industry is forging ahead with installing anti-hacker measures in their software, hackers are evolving new methodology to counter these measures by employing such techniques that could hijack virtual private networking (VPN) security and evade detection. This way, hackers continue to steal information and credentials and compromise software environments.[25] One of the profound weaknesses in aviation cyber security is that cyberspace is not so much a 'space' but a network of systems connected by multiple nodes which has an amorphous reach whereas cyber security in aviation is treated on the basis of cyber security regions, which divide the cyberspace networks into various sectors, thus isolating security controls at such sector nodes and making them vulnerable to attack.[26]

1.2.2 Air Traffic Management Systems

A particular vulnerability is seen in air traffic management systems where security challenges pose a two pronged threat. For one, if established systems are not fitted with the appropriate information and communication security measures, they could be vulnerable to attack. Just as an example, the common use of radio frequency in air traffic management for communication between air traffic control and aircraft, navigation, and surveillance could make it easy for the hacker to execute unauthorised transmissions through very high frequency transceivers. To circumvent this possibility one could encrypt radio transmission but this would seriously circumscribe the number of channels available for communication between air traffic control and aircraft. The radio transmission approach has an added vulnerability in that radio transmissions could easily be jammed, as in a reported instance when a portable transceiver was used to jam the Unicom frequency at Central Maine Airport.[27]

The other threat lies in new technology that may be introduced into the air traffic management networks which could create unsecured access points through which critical information and systems can be compromised in new and innovative ways. One such innovative air traffic management system, which is expected to become popular over the coming decade is Remote Tower Services (RTS) where air traffic at an airport is performed remotely, away from the local control tower. The European Cockpit Association (ECA) has suggested that cyber-security portends an ominous scenario where the very nature of the concept would lay it open to susceptibility and vulnerability. ECA therefore suggests precautionary measures to be put in place and procedures established so that possible attacks could be circumvented or at least minimized in their consequences. One of the measures

[25]M-Trends 2015: A View from the Frontlines, *Mandiant Threat Report*, info@mandiant.com at 1.
[26]Siu et al. (2014), pp. 73–81 at 74.
[27]Mark (2016).

suggested, as part of an efficient security management system in RTS, is a mandatory reporting system by air navigation service providers and aircraft operators that would alert authorities to occurrences related to illegal or questionable cyber conduct. This brings to bear the need for identification of the person who transmits the message as well as the potential recipient of the message. There is a critical need in this regard to adopt technical and legal measures that could ensure that the identity of the message transmitter can be authenticated, and their messages to selected recipients can be limited.[28]

1.2.3 The ICAO Role

The compelling importance of putting technical and legal measures in place is compounded by the fact that cybercrimes, whether they be through hacking or mere disruption to computer systems, take multifarious forms. Past instances have shown non-malicious mistakes; mischief; thrill seeking disruptions calculated to cause interference and inconvenience; and premeditated attacks to intentionally harm an air transport service.

The complexity and enormity of the threat of cybercrime and cyber terrorism has prompted a strong view that an overarching rule that ensures cyber security should be implemented 'top-down' through direction as well as 'bottom up' through technology:

> The 'top' of the Civil Aviation control system is the International Civil Aviation Organisation (ICAO). As a result, ICAO needs to have appropriate measures and management strategies to implement, support and secure civil aviation, particularly the new 'eEnabled' aircraft[29] and the future Air Traffic Management (ATM) systems, being designed by the SESAR, NextGen and Carats projects. A single cyber security architecture will be required to enable these new systems to inter-operate seamlessly, securely, and safely worldwide.[30]

The question is how far ICAO should go in collaborating with the industry and other key stakeholders in seeking a way forward towards guiding the rest in the context of its leadership role. The ICAO Twelfth Air Navigation Conference (AN-Conf/12), held from 19 to 30 November 2012, recommended that ICAO establish, as a matter of urgency, an appropriate mechanism including States and industry to evaluate the extent of the cybersecurity issues and develop a global air traffic management architecture taking care of cybersecurity issues. At the 38th Session of the ICAO Assembly, held from 24 September to 4 October 2013, the Assembly adopted Resolution A38-15 (Consolidated statement of continuing ICAO policies related to aviation security), Appendix A of which directs the ICAO

[28] Siu et al. (2014), p. 76.

[29] Boeing 787, Airbus A380 and A350 and similar aircraft.

[30] Cyber Security in Civil Aviation, Centre for the Protection of National Infrastructure, August 2012 at 1.

Council to continue, as an urgent priority, its work relating to measures for prevention of acts of unlawful interference, on the basis of the strategic direction provided by the ICAO Comprehensive Aviation Security Strategy (ICASS), and ensure that this work is carried out with the highest efficiency and responsiveness.

Strategic Focus Area 1 of this Strategy recognizes that global civil aviation operations are facing new and evolving threats, such as those posed by improvised explosive devices, unconventional terrorist attacks on airports and aircraft facilities, cyberattacks on aviation systems, including Air Traffic Management Systems, and threats to general aviation. ICAO has undertaken that it will adopt an approach in this regard that will employ a more proactive strategy to address such threats, working through the AVSEC Panel Working Group on Threat and Risk (WGTR), which monitors and evaluates new and existing threats on a regular basis, and identifies gaps in Annex 17 (Security) to the Chicago Convention,[31] for subsequent amendments. *Strategic Focus Area 2* of the overall ICAO strategy recognizes that an integral part of a proactive method of promoting innovative, effective and efficient security approaches entails a regular review and amendment of existing guidance material. This Focus Area goes on to say that ICAO, using the expertise of the AVSEC Panel Working Group on Technology, will assist member States and industry towards employing new and innovative security measures, including but not limited to, the use of advanced technology. In this context, ICAO is continuing the development of a web-based platform, named "*AVSECPaedia*", to encourage the exchange of information of a sensitive nature between States including, but not limited to, screening techniques and emerging security technologies. ICAO will also ensure the timely development of guidance material to reflect the most recent developments in aviation security and technology.[32]

1.2.4 The Work Of ICAO: Progress So Far

In a report detailing progress made by ICAO and industry partners up to 2015, presented to the ICAO Council at its 205th session in mid-2015, the ICAO Secretariat defined "cyber security" as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment as well as organizations' and user's assets. It encompasses the protection of electronic systems from malicious electronic attack and the means by which to deal with the consequences of such attacks".[33] As to what "user's assets"

[31]Convention on International Civil aviation, signed at Chicago on 7 December 1944. The Convention came into force 4 April 1947. See ICAO doc 7300/8, 2006.

[32]ICAO Comprehensive Aviation Security Strategy (ICASS), presented by the Council of ICAO, *A37-WP/18EX/2, 28/6/10* at 2.

[33]Report on Civil Aviation and Cybersecurity, *C-WP/14266*, 21/04/15 at 2.

represented in this context, were not identified by ICAO, although this definition was followed up with the categorization of vulnerability that fundamental characteristics of information and communications technology systems were exposed to as follows: *confidentiality*, i.e. information can be accessed or used only by the authorized or intended recipients; *integrity,* i.e. information has not been tampered with in transit and therefore remains as foreseen by the sender/source; and *availability*, i.e. information is available within agreed, reasonable timelines without undue delays.[34]

It is noted that, arguably for the purpose of reaching consistency in international terminology and language, ICAO had copied almost verbatim (without acknowledgment) the aforementioned definition and categorization from the International Telecommunications Union.[35] Another fact worthy of note is that the WGTR—which is ICAO's main tool in addressing aviation cyber security—has concentrated so far (up to 2015)—3 years after the Air Navigation Conference requested that ICAO establish, "as a matter of urgency, an appropriate mechanism including States and industry to evaluate the extent of the cybersecurity issues and develop a global air traffic management architecture taking care of cybersecurity issues"—only on cyber terrorism *i.e.* terrorist related attacks only, leaving the entire issue of other cyber-attacks or disruption by hacktivists and other persons who indulge in crimes for personal thrill or mere disruption of air transport, totally ignored. No reason is given for this exclusion[36] although ICAO's remit is clearly to "evaluate the extent of cybersecurity issues". The fact of the matter is that currently, and over the past several years, there has been no cyber terrorist attack but several individual "hack" attacks on aviation although the cyber terrorist individual or organization will be a corollary to the individual hacker. As German insurer *Allianz* said, cyber terrorism may replace the hijacker and bomber and become the weapon of choice on attacks against the aviation community.[37]

It was reported in May 2015 that a security researcher had alerted US agents of the Federal Bureau of Investigation that he had been able to successfully hack into aircraft computer systems mid-flight numerous times through the in-flight entertainment systems, and at one point had caused a plane he was on to move sideways.[38] The process with which the hacking was accomplished is called reverse

[34] *Ibid.*

[35] See Definition of Cybersecurity referring to ITU-T X.1205, Overview of cybersecurity, http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx.

[36] Report on Civil Aviation and Cybersecurity, s*upra* note 19, para. 3.3.

[37] Zolfagharifard (2016). It is curious that although the ICAO Report does not mention "hacktivists" an ICAO press release talks of them: "The five major international aviation organizations signed a new cybersecurity agreement late last week formalizing their common front against the hackers, 'hacktivists', cyber criminals and terrorists now focused on malicious intent ranging from the theft of information and general disruption to potential loss of life". See http://www.icao.int/Newsroom/Pages/aviation-unites-on-cyber-threat.aspx.

[38] Thompson (2016).

engineering.[39] Whether or not these claims can be authenticated or accepted for their credibility, the fact remains that at the present time, hacking by individuals who are not entirely impelled by terroristic intent cannot be ignored.

In February 2014 the ICAO Council adopted two Recommended Practices to Annex 17 to the Convention on International Civil Aviation which became effective on 17 November 2014 and which provide that each Contracting State should, in accordance with the risk assessment carried out by its relevant national authorities, ensure that measures are developed in order to protect critical information and communications technology systems used for civil aviation purposes from interference that may jeopardize the safety of civil aviation.[40] The new provisions also exhort States that they should encourage entities involved with or responsible for the implementation of various aspects of the national civil aviation security programme to identify their critical information and communications technology systems, including threats and vulnerabilities thereto, and develop protective measures to include, *inter alia,* security by design, supply chain security, network separation, and remote access control, as appropriate.[41]

Whilst the Assembly Resolution A 38-15 calls for ICAO to provide strategic direction according to ICASS, which involves ICAO's assisting member States and industry towards employing new and innovative security measures, including but not limited to the use of advanced technology, ICAO has instead come up with two recommendations on what States ought to be doing by themselves. This raises the question as to how States could encourage each other to adopt measures without any assistance by ICAO with regard to the introduction of new and innovative security measures. This disconnect has to be addressed, through the initial question: are Recommended Practices the answer to a problem described as the foremost threat on the security list after the events of 9/11?[42]

This conundrum involves another dimension—as to whether ICAO should employ the role it has been assigned in cyber security in a prescriptive manner. There has been a suggestion that ICAO guidance developed in this regard should be non-prescriptive and non-excessive.[43] This is a platitude as ICAO's very nature resonates the fact that it is a non-prescriptive Organization. Even the Standards of the ICAO Annexes (except for those of Annex 2 on Rules of the Air) are non-obligatory as States can file differences to any Standard if they are unwilling or unable to abide by them. However, it must be noted that at least a difference filed would provide some indication as to why a State does not agree to implement a Standard and therefore have some degree of persuasive authority.

[39]Reverse engineering is taking apart an object to see how it works in order to duplicate or enhance the object. The practice, taken from older industries, is now frequently used on computer hardware and software. See http://www.hackersonlineclub.com/reverse-engineering.

[40]14th Amendment to Annex 17, Recommendation 4.9.1.

[41]Id. Recommendation 4.9.2.

[42]Reed (2001).

[43]Cyber Security in Aviation (presented by the International Air Transport Association), *AVSECP/25-WP/34*, 28/2/14, para. 5.1.d).

On 5 December 2014, ICAO signed with four other Organizations—Airports Council International (ACI), the Civil Air Navigation Services Organisation (CANSO), the International Air Transport Association (IATA), and the International Coordinating Council of Aerospace Industries Associations (ICCAIA) an agreement to establish what is called a "Roadmap"[44] on cyber security based upon an agreement to establish an Industry High-level Group (IHLG) as a mechanism for high-level cooperation on issues of common interest and importance. The IHLG has determined that cybersecurity in civil aviation was a high priority transversal issue requiring collective alignment. The five organizations signed the Civil Aviation Cyber Security Action Plan and accompanying Roadmap. ICAO claims that this cooperation enables the participating parties to draw together all elements of the aviation industry to ensure a shared vision, strategy and set of commitments to tackle the cyber threat.

It is not enough for the five organizations to share a vision and strategy, even if there is one. Cooperation of States is essential and such cooperation must be insisted upon and seen to exist. This is where ICAO should come in as the United Nations specialized agency for aviation. As Director General of IATA Tony Tyler said: "governments have resources and access to intelligence that the private sector can never achieve". They also have a responsibility to use these resources to support industry efforts. We have an example of this approach in the decades of successful government-industry cooperation on safety. Unfortunately, we have not achieved that level of cooperation in security. As the threat of malicious cyber-attacks increases, the need for consultation, coordination and cooperation built on trust—among governments, between governments and industry, and within industry—becomes more critical.[45]

The key to a cybersecurity strategy is cooperation achieved through standardization and harmonization, and this is yet to be achieved in aviation security. As the author pointed out in an earlier publication, this glaring lack of sharing of information created a serious lacuna in aviation security in 2014.[46]

---

[44]ICAO claims that the Roadmap is a dynamic document containing a number of tasks and deliverables that will evolve over time to address key issues of cybersecurity. Its purpose is manifold: to support the development and promotion of a robust cybersecurity culture; to promote the use of information security and cyber protection best practices in the industry; and to share information on cyber threats and risks. It is also claimed that the Roadmap recognizes the best practices and standards on cybersecurity as provided by the International Organization for Standardization (ISO) and National Institute of Standards and Technology (NIST), recognizing that the industry is making substantial progress in developing and implementing cybersecurity tools, such as CANSO's Cyber Security and Risk Assessment Guide. See Report on Civil Aviation and Cybersecurity, supra, note 19, para 5.1.

[45]Remarks of Tony Tyler at the Civil Aviation Cyber Security Conference, Singapore, 9 July 2015 at http://www.iata.org/pressroom/speeches/Pages/2015-07-09-01.aspx.

[46]In the instance of the disappearance of Malaysian Airlines Flight MH 370, where it was revealed post facto that unbeknownst to the Malaysian authorities, two passengers had forged passports. These forgeries had been recorded in an INTERPOL maintained database and the database's existence had not been brought to the notice of ICAO member States. The author pointed out that

1.2.5 Exhortations to ICAO by Other Entities

1.2.5.1 IATA

At the twenty-fifth ICAO AVSEC Panel Meeting held from 17 to 21 March 2014, IATA advised that there are many players in the field of cyber security taking different approaches and looking at specific issues. Frameworks are emerging from many organizations and there is little coordination of approach. Therefore, vulnerabilities will increase due to the sheer volume of parties involved in the development and supply chain of computer systems, the data used in aviation and the increasing trend to outsource.[47] IATA advised the Panel that airline and airport networks have hundreds, if not thousands of entry points, through connectivity with the internet, mobile devices, connections with other organizations and systems such as Global Distribution Systems, governments, other airlines, financial systems, remote check in systems and more. With the increases of networked technologies and automated systems, availability and integrity of those systems increases. The evolving convenience of systems and processes, their efficiency and integration brings to bear the likelihood of increasing vulnerability of the systems to potential cyber threats.[48] It is in this context that IATA exhorted ICAO to recognize the compelling need for "the development of *specific measures* (my emphasis) and best practices focusing on the aviation industry".[49] ICAO's response to this request is reflected in the Rapporteur's Report to the AVSEC Panel—submitted to the twenty-sixth meeting of the Panel held from 13 to 17 April 2015—which says that despite broad encouragement for individuals to undertake "electronic jihad", no specific examples of terrorist cyber-attacks against aircraft have been identified. There was no evidence of meaningful advances in terrorist capability in this area. The Rapporteur further said that although individuals, including hackers, commonly make claims about the vulnerabilities of aircraft information systems, there no evidence that this has influenced terrorist intentions. However, this could encourage terrorists to try to develop this capability in the future. Somewhat flippantly, the Rapporteur's Report says that: "simply connecting or interacting with aircraft systems does not constitute the capability to manipulate the function of a safety critical system so as to endanger the aircraft. In some scenarios, the uncertainty around the likely impact of exploiting a particular vulnerability may mean they have limited appeal to a terrorist. As ever, the possibilities offered by a skilled insider need to be considered.

---

both ICAO and the International Criminal Police Organization (INTERPOL) failed to advise States and airlines of the existence of a database at INTERPOL on forged or fraudulent passports, and that ICAO and other key players concerned would have to adopt a more serious approach to the problem. Information sharing is a central process through which team members collectively utilize their available informational resources. See Abeyratne (2015), p. 18.

[47]CYBER SECURITY IN AVIATION, *AVSECP/25 -WP/34*, 28/2/14 at 3.

[48]*Id.* 1.

[49]*Ibid.*

But overall the current threat likelihood is expected to be LOW".[50] This statement is somewhat puzzling, particularly since the vulnerability of air transport was placed before ICAO by the ICCAIA[51] which, at the Twelfth Air Navigation Conference of ICAO held in Montreal in November 2012, stated that there are already a number of examples of cyber security and vulnerabilities and detailed them in a working paper to the Conference.[52]

It is noteworthy to consider IATA's three pronged approach in this regard*: risk management*—the objective being to help the industry understand the risks and put a framework in place to enable stakeholders to manage those risks consistently and effectively; *advocacy*—the objective being to work with airlines, airports, suppliers, manufacturers and regulators to ensure that standards are developed and implemented where they need to be, and to advocate for emerging regulation to be risk-based and globally coordinated; *reporting and communication*—the objective being to raise awareness of cyber issues and look for mechanisms to allow better sharing of threat information, incidents and mitigation strategies, across the industry.[53] If ICAO were to adopt this approach towards States, both ICAO and IATA would be in sync and collective work in addressing the cyber threat in aviation would be much easier. One of the conclusions of IATA is that the AVSEC Panel recommend that Member States be encouraged to consider the regulation of cyber security for aviation as part of a comprehensive and holistic national plan which covers all enterprise activities within a State, taking into account the vulnerabilities of the larger IT ecosystem.[54]

1.2.5.2 CANSO

On the subject of cybersecurity in air traffic management CANSO advised the AVSEC Panel its fivefold approach to aviation cyber security: *enterprise-wide approach*—as cyber-attacks grow in intensity and become increasingly sophisticated, changing constantly in response to the defensive systems they encounter, it will become necessary to adopt an approach to cybersecurity that is proactive, dynamic, and adaptive, evolving beyond the realm of traditional IT management

[50]INITIAL REPORT ON THE RISK OF CYBER ATTACK ON AIRCRAFT SYSTEMS, *AVSECP/26-WP/27,* 20/2/15 at 3.

[51]The International Coordinating Council of Aerospace Industries Associations (ICCAIA) is the international organization of aerospace industry associations. Their members are engaged in the design, development, manufacture and in-service support of aeronautical and space products and technologies, including related ground-based systems.

[52]CYBER SECURITY FOR CIVIL AVIATION, *AN-Conf/12-WP/122*, 9/10/12 at 2–3.

[53]CYBER SECURITY IN AVIATION, *supra*, note 33 at 2.

[54]*Id*. 4.