Flying challenges for the future: Aviation preparedness – in the face of cyber-terrorism

Sarah Jane Fox[1]

Accepted version: 2 September 2016
(Published online 28 September 2016 – subject to numbering/footnote amendments)
Journal of Transportation Security ISSN 1938-7741
J. Transp Secur DOI 10.1007/s12198-016-0174-1

Abstract

Transport has always been, and will continue to be, a means to serve to eradicate world inequalities bringing relief and salvation across the globe and no transport mode more so perhaps than aviation. However, aviation has served as both the salvation and the aggressor, having also itself been the victim of terrorist attacks. Arguably (to date) in 2016, the world could consider itself fortunate not to have witnessed a devastating cyber-terrorist attack on an aircraft. Certainly concerns were raised after the disappearance of MH370 in terms of cockpit tampering; and yet, these reports only touched upon the surface of an effervescing iceberg – set to erupt into a tsunami of devastation. The question inevitably remains 'when' rather than 'if' this will occur. This research reviews the vulnerability of air travel and the preparedness of the industry in terms of coordination (prevention and protection) from the perspective of policy, legislation (regulation) and organisation.

KEYWORDS: Aviation; cybersecurity; cyber-attack; cyber-terrorism; coordination; policy/legislation; risk

[1] This paper formed part of a discussion at the United Nations (WSIS Forum) 2016 – EC Medici Framework on Safety and Security: 2016, 2-6 May, 2016 (Geneva).
BIO: Sarah Jane Fox was awarded a post-doctoral Fulbright-Lloyd's of London, Law Research Scholarship in 2015/16, and took up a post as a visiting Professor at DePaul University, (IALI) Chicago. Sarah's research focuses on EU and International law, strategy, security, international relations and policy conflicts. Sarah specialises in the field of transport law/policy (particularly aviation and other vulnerable infrastructure) and adjacent measures such as security, terrorism, safety, enforcement, organisations/governance. Sarah holds a Ph.D. and Masters degree in EU law (with comparison law analysis – regional and international). She is also a Fellow (law) of the University of Liverpool and supports the Law (PG) Programmes at the University of Liverpool, UK, whilst also undertaking a role in risk management for the Institute of Risk Management (IRM).

1. INTRODUCTION

Transport remains essential to humanities very survival, as was commented upon,

> *'Transport is fundamental to our economy and society. Mobility is vital to the ..... quality of life of citizens as they enjoy their freedom to travel.... Transport is global, so effective action requires strong international cooperation'* (COM 2011/144 Final).

The United Nations (UN) Sustainable Development Goals (SDG's) relate to a vision for humanity as well as a social contract between the people of the world. And, whilst sustainability remains the cross cutting focus, the aspect of mobilisation of resources and technology is viewed as a critical aspect in realising development and ultimately pursuing related goals.[2] The overall aim of which is to 'banish a whole host of social ills by 2030.' However, as old challenges are addressed, new ones ultimately develop and become the fresh nemesis to be tackled, which ultimately require *international cooperation.*

The importance of transport to the attainment of the SDG's has often been overlooked and the security of such a vital world component is too often compromised. Transport remains a way of uniting the world and is an invaluable and irreplaceable asset to the highly globalised society we live in. Hence transport requires protection – alongside the critical infrastructure that supports it. Yet, of late, it has become a target of attack and a means of striking fear into users and the greater society it serves.

There is no doubt that transport has often stood at a crossroads whereby it has been used to take lives and save lives. On a global perspective, one such challenge remains the alarming number of deaths attributed to road transport; whilst, the use of aircraft in warfare has equally resulted in the unacceptable loss of countless lives through acts of purposeful aggression (Fox 2014a). This research paper directly relates to this latter and relatively new mode, aviation, which whilst being engaged in aggressive acts, has also brought salvation to many, through humanitarian relief aid. Yet this division has become blurred, with civil aviation being a victim of terrorist attacks and aircraft being used as a weapon of destruction (Fox 2014a). It remains a fact that air transport, arguably, more so than any other transport, serves to eradicate world inequalities, it has shrunk the world and has been a key player in quickening the pace of globalisation. Economies, societies and cultures have become more than ever intertwined because of this connectivity (Fox 2014a). Trade networks are essential to global integration and hence, communications and transportation are fundamental enablers and constituents, imperative to world integration. However, the mixture of both of these key aspects could also lead to devastation; and, debatably (to date) in 2016, the world could consider itself fortunate not to have witnessed a devastating cyber-terrorist attack on or against an aircraft. The raising of concerns as to the vulnerability of aviation is not new (Fox 2014a). Press reports were particularly significant in this respect after the disappearance of MH370, whereby, certainly, the

[2] Agenda 21 made specific reference to transport in several of the chapters, for example Chapter 9 on Atmosphere and Chapter 7 on Human Settlement. At the 2012 UN Conference on Sustainable Development (Rio+20) the 'Future We Want' outcome document emphasised that transport and mobility had a crucial role to play in sustainable living.

potential of cockpit tampering was raised[3]; and yet, these reports arguably only touched upon the surface of this issue and the potential for devastation, as witnessed for instance, in and on the scale of the 9/11 terrorist atrocities. The question inevitably remains how vulnerable and prepared is civil aviation? And, is it a case, of 'when' rather than 'if' this will occur? Certainly this remains a new challenge in terms of social ills against a transport mode, and hence society.

This article therefore undertakes analysis and reflection of the challenges faced by aviation in terms of cyber-attacks, specifically focusing on terrorism through cyberspace. Initial reflection is provided through means of a contextualised background before the response of a coordinated approach is considered in terms of preparedness and a framework to tackle cyber-attacks and terrorism. Ultimately the paper concludes by considering aviation and the need of such in terms of facing the future.

The paper is presented through the discipline of law and is structured in the following way: (as per Chart 1)

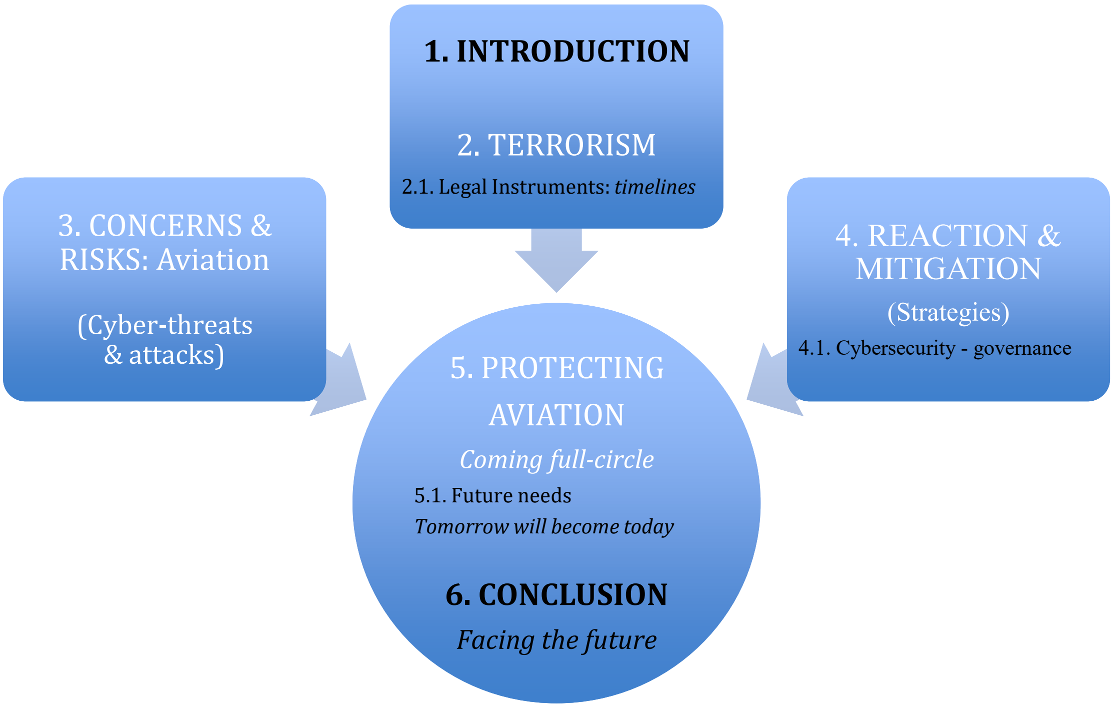

Chart 1: Structure of the paper (Author)

2. TERRORISM

Terrorism is far from a new phenomenon, arguably when it actually began remains contestable. The root of the word comes from a Latin term which means 'to frighten'

[3] The Telegraph. Jonathan Pearlman. 'MH370: New evidence of cockpit tampering as investigation into missing plane continues.' 29 June, 2014. Sydney, Australia.
Also see: S. J. Fox (2015) CONTEST'ing Chicago origins and reflections: *lest we forget! Int. J. Private Law*, Vol. 8, No.1, 2015 pp 73-98.

and is traceable back to 105BC when '*terror cimbricus*' was a state of panic applied in response to an attack by the Cimbri tribe. During the French Revolution the term, 'a reign of terror' was also applied, although, somewhat ironically perhaps as imposed by a government.[4]

Sergey Nechayev is said to have described himself as a 'terrorist' later founding in 1869, the 'People's Retribution' organisation (Avery 2010).[5] Today, the associated word is hence linked to this application, and the term 'terrorist' remains a word associated with a group (or individual) who carries out atrocities, which normally has as a result, the loss of innocent lives and/or mass destruction. In more recent times such acts have been taken against a State and have increasingly been targeted at high profile areas – which has included transport and its supporting infrastructure.

2.1. International Legal Instruments - *Timelines: origins and developments*

Terrorism is recognised worldwide by States, and hence has been on the international agenda since 1934. The League of Nations, the forerunner to the United Nations (UN), actually began drafting a convention for the prevention and punishment of terrorism, at this time, although it was never actually to result in the instrument coming into force.

Since 1963, the international community (through the UN) has been actively involved in formulating universal legal instruments to prevent terrorist acts.[6] Such mechanisms have also been specifically aimed at identified industries (such as the atomic sector) and have therefore been developed by the UN and its specialised agencies, such as the International Atomic Energy Agency (IAEA). In this respect, the illegal transport of biological, chemical and nuclear weapons (and related material) has also become subject to international agreement. Furthermore, transport too has necessitated special recognition regarding the vulnerability to terrorist attack, in particular the modes of maritime and aviation, and hence, the International Civil Aviation Organisation (ICAO) and International Maritime Organisation have been actively involved in developing security measures and actions to counter terrorism.
In terms of aviation, for example, this resulted in the Hague Convention of 1970 for the Suppression of Unlawful Seizure of Aircraft[7] and the Montreal Convention of 1971 for the Suppression of Unlawful Acts against Safety of Civil Aircraft.[8]

Although, arguably, there remains no worldwide-accepted definition of terrorism (Fox 2015; Blackbourn et al. 2012: Weinberg et al. 2004; Saul 2005) in December 1972 the UN Sixth Committee referred to the need to take,

> '*Measures to prevent international terrorism which endangers or takes innocent human lives or jeopardizes fundamental freedoms, and study the*

[4] Hwa Chong Institution www2.hci.edu.sg [Accessed 8 April, 2016].
In this respect the Reign of Terror was instigated by Maxmillien Robespierra, who was one of twelve heads of government and used the justification of such as a necessity to transform the state from a monarchy to liberal democracy.
www.crimemuseum.org

[5] Martin Avery (2010) '*Muskoka Terror G8: Activist and Terrorist From Huntsville to Algonquin Park*' Lulu.com. Also see www.encyclopedia.com/article-1G2-3426400063/nechayev-sergei.html [Accessed 9 April, 2016]

[6] un.org [Accessed 8 April, 2016]

[7] United States Treaties and Other International Agreements, vol. 22, part 2 (1971), p. 1644. See FN 13

[8] Ibid., vol. 22, part 2 (1973), p. 1644. See FN 13.

> *underlying causes of those forms of terrorism and acts of violence which lie in misery frustration, grievance and despair and which cause some people to sacrifice human lives, including their own in an attempt to effect radical change.*'[9]

This Resolution affirmed the need for international cooperation to tackle actions that strike at liberty and freedom, and, which invariably transcends boundaries and borders. But, it was not until the 1980's that the UN Security Council actually began to refer more specifically to 'terrorism.'[10] This also was to coincide with specific, direct targeting against aviation.

The 1990's also saw fortification of the need for a cooperative worldwide approach through the adoption of Resolution A/RES/49/60 at the 84th Plenary meeting.[11] Within it, reinforcement was given to need to address, '*criminal acts intended or calculated to provoke a state of terror in the general public*'…… where the circumstances were '*unjustifiable, whatever the considerations of a political, philosophical, ideological, racial, ethnic, religious or any other nature that may be invoked to justify them.*'[12]

The Annex of the Resolution also highlighted the growing list of international treaties, which addressed specific '*aspects of the problem of international terrorism.*'[13] The number of individual Conventions arguably reinforced the need for a more coordinated approach to be taken by the international community by emphasising that acts of terrorism were becoming an ever-growing issue. And, the list highlighted that attacks against transport modes was clearly becoming a 'problem.' Principally targeted were aviation and maritime – and response action included measures to counter such acts of sabotage, hostage-taking, hijacking and other related criminal exploits.

The Resolution, in essence, highlighted that the international community was dis-inherited in terms of a harmonised approach. It could also be viewed that measures

[9] Resolution XXVII – 2114th plenary meeting, 18 December 1972.

[10] United Nations Security Council, Resolution 579 (1985) *Adopted by the Security Council at its 2637th Meeting*, Para's. 1 and 5; see also SC President Statement 8 October [online] http://www.worldlii.org/int/other/UNSCRsn/1985/ [accessed 26 December 2013, 27 April 2016].

[11] 9 December 1994.

[12] As within the Annex at I.3.
Also see discussion within S. J. Fox (2015) CONTEST'ing Chicago origins and reflections: *lest we forget! Int. J. Private Law*, Vol. 8, No.1, 2015 pp 73-98.

[13] 'The Convention on Offences and Certain Other Acts Committed on Board Aircraft, signed at Tokyo on 14 September 1963, the Convention for the Suppression of Unlawful Seizure of Aircraft, signed at The Hague on 16 December 1970, the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, concluded at Montreal on 23 September 1971, the Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents, adopted in New York on 14 December 1973, the International Convention against the Taking of Hostages, adopted in New York on 17 December 1979, the Convention on the Physical Protection of Nuclear Material, adopted at Vienna on 3 March 1980, the Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, signed at Montreal on 24 February 1988, the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, done at Rome on 10 March 1988, the Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf, done at Rome on 10 March 1988, and the Convention on the Marking of Plastic Explosives for the Purpose of Detection, done at Montreal on 1 March 1991.'

taken were largely responsive resulting in reactive Conventions, rather than proactive forethought. Up until this time no foresight had occurred in terms of attacks that could be coordinated or perpetrated through online or other growing technological advancements.

However, in 1994, the General Assembly, at its 49th session, adopted Resolution 49/158 (23 December 1994). This called for a strengthening of the United Nations crime prevention and criminal justice programme, particularly, recognising, the need to address technical cooperation capacity; and hence, 1994 also saw the United Nations Manual on the Prevention and Control of Computer-related Crime.[14] That said, the word 'Internet' was used only once in the Manual and the word 'cybercrime' was never used. However there was considerable foresight shown regarding the need for a more global joined-up approach in relation to 'computer-related' crime, which stated that there was a need for a more collaborative response from law enforcement bodies. The Manual should therefore be regarded as giving an early alert concerning the abuse of the Internet by criminals.

What could perhaps arguably never have been envisaged though was the growth in global electronic connectivity and the need to prioritise this strategy; or conversely, it could equally be said that this should have been anticipated and hence given a higher priority than actually transpired. In 2014, the International Telecommunication Union, in Geneva, stated that there were then over 3 billion Internet users representing approximately 40 per cent of the global population – a growth four times higher than in 2009.[15]

It was not until 2006 that the United Nations adopted its Global Counter-Terrorism Strategy, in the form of a Resolution and an annexed Plan of Action.[16] The Resolution, whilst reaffirming the need to strengthen the global fight against terrorism, made no direct mention to the aspect of cyber-terrorism – instead specific mention was given to the more traditionally perceived acts of terrorism, identifying in particular the concern of terrorist access to nuclear, chemical or radiological materials.

However within section II of the Annex ('Measures to prevent and combat terrorism,' and the related Plan of Action) specific reference to the Internet and terrorism is made. In this regard the dilemma of the Internet, in terms of confidentiality and respecting human rights, and hence compliancy with other areas of international law, is referred to. This potentially strikes at the very difficulty in advancing cooperative plans involving the use of the Internet, not only from the perspective of data protection and human rights, but with regards to jurisdiction of a virtual entity.

Specifically, whilst it is recognised that there is a need '*to explore ways and means to:*

[14] United Nations Manual on the Prevention and Control of Computer-related Crime, International Review of Criminal Policy, Series M, Nos. 43-44 (United Nations publication, Sales No. E.94.IV.5.)
Also see: United Nations Resolution on Combating the Criminal Misuse of Information Technologies GA RES 55/63, UNGA 55th Session, 81st Plenary Meeting UN Doc. A/RES/55/63 (2001).

[15] "The World in 2014: ICT facts and figures" (Geneva, 2014).

[16] A/RES/60/288 – September 2006.

a. *coordinate efforts at the international and regional level to counter terrorism in all its forms and manifestations on the Internet, and:*
b. *use the Internet as a tool for countering the spread of terrorism,'* it is also recognised *'that States may require assistance in this regards.'*

Further on, within this section, direct reference is made specifically to aviation, whereby, it is stated that there is a need '*to encourage*' the UN Terrorism Committee and its Executive Directorate to continue to work with States and to '*facilitate the adoption of legislation and administrative measures to implement the terrorist travel-related obligations, and to identify best practices in this area, drawing….on… technical international organizations such as the International Civil Aviation Organization…..'*

Inevitably there are several words to draw out for further scrutiny, particularly firstly, the use of, and reference to, the need to actually '*encourage*' States to work together in a bid to achieving legislative measures. Whilst there are issues to overcome (such as human rights, coordination and jurisdiction, etc.,) it undoubtedly remains in the International Community's interests to work collaboratively to seek solutions so as to ensure the '*quality of life of citizens* [including] *their freedom to travel.*'[17]

In this regard the emphasis (within the Strategy and Action Plan) remains arguably on the less contentious areas such as physical travel and risk and '*identifying best practices*.' But, if these rather simplistic and established areas are recognised to still present such a challenge (in terms of coordinated action, which require encouragement and assistance) – it would have to be questioned how on earth can the aspect of achieving legislative measures to prevent, and means to strike back, at cyber-terrorism, perpetrated through cyberspace, ever be tackled….. and consensus achieved?

Transport and particularly aviation and the related supporting infrastructure, have increasingly been targeted by terrorists,[18] and it strikes at gross stupidity and ineptitude not to envisage a day when aviation will be targeted by a cyber-terrorist. Cybersecurity and cyber-terrorism are invariably the current challenges that need to be acknowledged and most importantly collectively reacted to by the international world.

3. CONCERNS AND RISK: AVIATION *CYBER-THREATS & ATTACKS*

The use of cyberspace is a relatively new tactic used by perpetrators to target computer systems - when this is without permission or authority it becomes a breach with various affects and consequences. Cybersecurity involves techniques, such as processes and practices, technology walls, etc., designed to add protection to networks and hence computers and programmes.

[17] First quote in paper – see the lead-in, within the introduction. COM(2011) 144 (final) '*Roadmap to a Single European Transport Area – Towards a competitive and resource efficient transport system.*' Brussels, 28.3.2011.

[18] For further discussions concerning aviation terrorism, see S. J. Fox (2015) CONTEST'ing Chicago origins and reflections: *lest we forget! Int. J. Private Law*, Vol. 8, No.1, 2015 pp 73-98.

It is recognised in general, that in cybersecurity terms, ‘risk’ is the potential for a ‘threat’ – whereby it is recognised that there is a possible or probably danger or hazard, which is exploitable through the ‘vulnerability’ (a ‘flaw, feature or user error’) which may result in some negative consequence.[19] A cyber-attack is when this has occurred and the risk has become a reality. The term ‘cyber-attack’ is to be understood as a range of malicious activities conducted through the use of information and communications technology. The attack can take various forms, such as ‘hacking’ (or arguably ‘cracking’) ‘jacking’ and ‘spoofing.’[20] That said, there is an inherent lack of clarity and definition in respect to cyber-crimes much in the same way as arguably there still remains in terms of defining terrorism.

During the past two years there have been an increase in the number of cyber-attacks aimed at aviation; and, in October, 2015, the director of the European Aviation Safety Agency (EASA) 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 the aircraft control systems. Hugo Teso has long warned over the possibility of hijacking a plane armed only with a mobile phone; and, has, therefore, stated that a cyber-attack, whereby a planes steering system is accessed, could easily lead to the crash of a plane.

Perhaps it is little wonder that airlines and aircraft manufacturers have sought to play down such warnings.[21] The International Civil Aviation Organisation (ICAO) in 2014, disputed the vulnerability of aircraft to direct cyber-attack, fervently proclaiming 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 actually low.[22] However, even the categorising of a ‘low’ risk is arguably a risk that is worthy of being mitigated. The fact that experts[23] have also pointed to the fact that the ACARS is outdated, having not been designed with cybersecurity in mind and hence remains vulnerable to attack, must be viewed as a risk threat - above that of low. This is supported by pilots who have also echoed their

[19] Authors definition based upon UK Government document by the CESG The Information Security Arm of GCHQ ‘Common Cyber Attacks: Reducing The Impact.’

[20] ‘Hacking’ is applied to 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.
Whilst ‘spoofing’ refers to a faked/false sending address of a transmission to gain illegal unauthorized entry into a secure system, Cyber Security Glossary, http://niccs.us-cert.gov/

[21] A widely held view by cybersecurity analysis – see the ‘bizplus’ report, 02 October. 2015.

[22] 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). See also < http://www.scmagazineuk.com/european-aviation-body-warns-of-cyber-attack-risk-against-aircraft/article/444487/>

[23] Supra. FN. 21 & 23.

concerns about the growing risk to aircraft through various cyber methods.[24]

Credence was also given to the increased severity of the actual 'risk' to aviation from cyber-attack (as opposed to purported claims and speculation) when, in 2015, United Airlines grounded all its flights in the US. This was due to concerns that spurious flight plans had appeared in its system.[25] It was furthermore suggested that United Airlines customers' data and records had also been the subject of illegal access.[26] This concern was intensified further when the Polish airline, LOT, additionally reported a cyber-attack that affected their ground operation systems, which prevented them from developing flight plans.[27] Whether these incidents could be said to have been terrorist motivated remains contestable but these attacks against airlines, and the supporting infrastructure, only too clearly reinforce the need to take cyber-crime seriously. Whilst cyber-crime can be directed and motivated for a number of reasons, and may range from external and internal threats where the purpose is aimed at blackmail, extortion, retribution, etc., or even just simply penetrating and testing the vulnerability of systems, the results can also be variable. However, such breaches can inevitably compromise data, efficiency and ultimately safety.

It should be acknowledged that telecommunications difficulties and infrastructure power problems are nothing new in terms of causing operational issues to air transport. As long ago as the 1990's, for example, the Federal Aviation Administration (FAA) listed within a report, 114 major telecom outages in a 12-month period (Neumann 1997). Whilst many of these issues may have been of a result of technological difficulties, the growing reliance on such communication advancements should have served as a clear warning of the vulnerabilities and possible threats in the future. Arguably, this could be said to support the allegation that the authorities (such as international organisations and national bodies) have been too slow to react and respond, and hence be proactive and prepared against the growing risk that exists. Certainly the various governance systems have, for too long, been blind to the possibility, or arguably reluctant to acknowledge the increasing magnitude of the risk of cyber-attacks on the aviation industry. Whilst this may be changing of late, the degree of devastation and havoc that could result from a coordinated cyber-terrorist attack remains speculative – and is a subject rarely broached. It is certainly an area where no harmonised approach exists in order to respond to such.

[24] See the report by The International Federation of Air Line Pilots' Associations (IFALPA), Cyber threats: who controls your aircraft? 5 June, 2013.
http://www.ifalpa.org/store/14POS03%20-%20Cyber%20threats.pdf [Accessed 30 April, 2015]

[25] Security Experts Warn Airlines Face Threat of Cyber Attacks,' Sydney Morning Herald, July 6, 2015.
Also see, Jeffrey Dastin, 'United Airlines awarded hackers millions of frequent flier miles for uncovering gaps in the company's cybersecurity.' Reuters, Jul. 16, 2015.

[26] 'China-Tied Hackers That Hit U.S. Said to Breach United Airlines' Bloomsberg, July 29, 2015
http://www.bloomberg.com/news/articles/2015-07-29/china-tied-hackers-that-hit-u-s-said-to-breach-united-airlines [Accessed 11 April, 2016]

[27] 'Hackers successfully ground 1,400 passengers.' CNN Politics, June, 22, 2015.
http://edition.cnn.com/2015/06/22/politics/lot-polish-airlines-hackers-ground-planes/ [Accessed 11 April, 2016].
Also see other headlines - 'Polish Airline, Hit By Cyber Attack, Says All Carriers Are At Risk', Reuters, June 22, 2015, Warsaw/Frankfurt

Today's increased number of traffic movements warrants the need for advanced computer-based systems in almost every aspect of civil aviation operations such as air navigation systems, on-board aircraft control and communications systems, airport ground systems, day-to-day management and booking systems etc. Each element remains vulnerable, and whilst cyber-attacks can take many forms, including isolated computer viruses, or more concerted and directed attacks that can cause both safety and security concerns, it is the coordinated actions of terrorist groups which seek to undertake a series of attacks levied against various systems simultaneously which has to be of the utmost concern.

Perhaps one of the most damning acknowledgements of the actual threat, and, the state of unpreparedness was the United States Government Accountability Office (GAO) Report to Congressional Requesters in 2015.[28] This related specifically to the responsibility of the Federal Aviation Administration (FAA) to the national airspace system (NAS)[29] but nevertheless revealed serious vulnerability in this respect, one that is undoubtedly replicated throughout the complex and various computer networks that support air transport. This report found that whilst the FAA had taken some steps to protect its air traffic control systems from cyber-attack it had, nonetheless, not fully implement its agency-wide information security program, a requirement of the Federal Information Security Management Act of 2002.[30]

Identified failures included:

- 'Not always sufficiently test security controls to determine that they were operating as intended;'
- Not resolving identified 'security weaknesses in a timely fashion; or complete or adequately test plans for restoring system operations in the event of a disruption or disaster.'

Furthermore, it was also identified that the group responsible for incident detection and response for NAS had 'insufficient access to security logs or network sensors on the operational network, limiting FAA's ability to detect and respond to security incidents affecting its mission-critical systems.'[31]

The report showed alarming shortcomings and an unacceptable risk to air transport, which the FAA clearly acknowledged. The report made 17 recommendations relating to the information security programme and the need to establish an integrated management approach to security risk. And, a separate report, with limited public access, made a further 168 specific actions to address further weaknesses. The fact that these risks remain unexposed to the public could be seen as a blessing on the one hand – one that prevents the identified risks being acted upon by the criminally

[28] GAO, 'FAA Needs to Address Weaknesses in Air Traffic Control Systems.' Jan, 2015.

[29] To contextualise the actual scope the FAA concludes that this relates to 'more than 19,000 airports, nearly 600 air traffic control facilities, and approximately 65,000 other facilities, including radar, communications nodes, ground-based navigation aids, computer displays, and radios, intended to provide safe and efficient flight services for the public. Over 46,000 FAA personnel and approximately 608,000 pilots operate about 228,000 aircraft within the NAS, including up to 2,850 flights at any given moment.'

Operational use is on a continuous basis, 24 hours a day, and every day of the year.

[30] Pursuant to Title III of the E-government Act of 2002 (P.L. 107-347).

[31] GAO, 'FAA Needs to Address Weaknesses in Air Traffic Control Systems.' Jan, 2015.

minded; or, a concern on the other hand - risks that are unknown but whereby the travelling public remain oblivious to the actual vulnerability that still surrounds their flights.

Whilst the older systems rely on point-to-point communications, NAS systems, and particularly the NextGen (US) systems, increasingly use IP technologies to communicate over interconnected computer networks. With this new technology arguably the threat and potential risk of attack intensifies, as it is recognised that integrated critical infrastructure systems with information technology networks provides 'significantly' less isolation from the outside world than the more dated systems. This message is replicated in Europe, where it has long been advocated that the newer, next generation of air traffic management systems, such as the Single European Sky ATM Research (SESAR), requires further protection. The modern, next generation aircraft, like the Boeing 787 Dreamliner and Airbus A350 and A380, also face the same challenges – that is, susceptibility to cyber-sabotage.[32] Clearly these identified concerns demand the need to secure all these systems from remote, external threats, whereby preventative action against proven, known and perceived vulnerabilities is taken.

Safeguarding computer systems that are part of not only a nation's but invariably growing global infrastructure systems remains critical. And whilst the GAO report was specific to the US, the message is clear across the globe – 'aviation is and remains vulnerable to cyber-attack!' A cyber-terrorism attack will undoubtedly be coordinated and hence the industry and regulators need to equally be coordinated and furthermore prepared!

4. REACTION AND MITIGATION – STRATEGIES

President Clinton clearly recognised this threat over 20 years ago, and, in 1996, formed a Commission on Critical Infrastructure Protection, which later published a report (1997) summarising the findings. In this it was stated,

> '*A personal computer and a simple telephone connection to an Internet service provider anywhere in the world are enough to cause a great deal of harm.*' And the report warned, '*[t]he right command sent over a network to a power generating station's control computer could be just as effective as a backpack full of explosives, and the perpetrator would be harder to identify and apprehend.*'[33]

In 1999 President Clinton identified that,

> '*open borders and revolutions in technology have spread the message and the gifts of freedom, but have also given new opportunities to freedom's enemies...*

[32] Ibid.

[33] The President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures* http://www.iwar.org.uk/cip/resources/pccip/report_index.html [Accessed 5 May, 2016]

> *we must be ready...ready if our adversaries try to use computers to disable power grids, banking, communications and transportation networks...*'[34]

Nearly some 15-years on, President Barack Obama again addressed these matters in his State of the Union Address (2013) specifically this time identifying the vulnerabilities to the air traffic control systems, saying,

> '*America must 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.*'

Whilst this may show acceptance of the risks and hence good intention to address the situation, when this is not acted upon it surely must be deemed a negligent failure. The GAO Report coming some two-year later, contentiously perhaps, clearly showed this to be the case.

In 2012 the UK produced a report identifying the need for a general approach to cybersecurity for civil aviation.[35] Within it, it was advocated that this should be a two-pronged approach (i) 'bottom-up' through technology[36] and (ii) 'top-down' from a coordinated control system.

In this regard it was identified that the top of aviation should be deemed to be the UN specialised agency, the International Civil Aviation Organisation (ICAO) – however, it should be commented on (as earlier stated) that as late as 2014, ICAO were criticised by the EASA for adopting an approach which played down the risk to aviation. Perhaps then, it should come as little surprise that in 2016 (to date) the progress has been slow and arguably globally inadequate in formulating a suitable international framework. In essence, achieving consensus amongst the current 191 ICAO member nations has often provided difficult. Even after more 'traditional' perpetrated terrorist attacks, where utterings of good intention were initially made, the resolve to commit to action has been slow. Inherently, there are protracted deliberations, which do not serve as quick way to provide a rapid means to address critical issues.

In 2014, Fox wrote '[t]he events of 9/11 were arguably the most high profile tragedy to highlight that when things go wrong, the cost can be enormous, both in terms of loss of life and the respective financial consequences' (Fox 2014b). She advocated that a framework was needed to deal with the aftermath of such. The framework should also be proactive and preventative - from anticipating the future vulnerability through to serving as a means to mitigate for such future atrocities. Fox stated that the

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

[35] CPNI - 'Cyber Security in Civil Aviation' (Centre for the Protection of the Critical Infrastructure) August 2012.

[36] In this regard, it should be noted that this paper concerns the legislative and regulatory framework.

international community, after Lockerbie,[37] should have been prepared for such an event as 9/11, with a pre-indicator having perhaps been provided by the hijacking of the Air France Flight 8969.[38] The reasoning for hijacking this plane was allegedly based upon the intention to blow the plane up over Paris, or to crash it into the Eiffel Tower in Paris (Fox 2014b). In this respect, it could be construed that aviation has not learnt from past events and anticipated effectively mitigating against future risks, albeit from a cyber perspective – of cyber-attacks and specifically cyber-terrorism. Ultimately, it has not shown the drive needed to be prepared and internationally coordinated.

4.1. Cybersecurity - governance

Whilst there is clear '*pointing*' to the fact that direction needs to come from ICAO in terms of protection against aviation related cyber-attacks, arguably this is a far more extensive and complicated matter, extending past the realms of aviation into general governance for cybersecurity.

It is really only over a short period, of some 20-years, that a series of UN General Assembly Resolutions relating to cyber-security have been adopted. The UN has therefore only relatively recently recognised the need for international experts to come together in order to build 'cooperation for a peaceful, secure, resilient and open ICT environment' by agreeing upon 'norms, rules and principles of responsible behaviour by States' and identifying confidence and capacity-building measures, including for the exchange of information.[39] The report from the group of experts identifies that 'international law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment.' Although the report points to the fact that countries recognise the need for 'full applicability of international law to state behaviour in cyberspace,' experts have labelled it only as 'a landmark step toward universal acceptance of the legal framework.'[40] In essence the report is one of intention rather than that of asserted action. This is perhaps reinforced by the report itself, which added a note of caution in terms of identifying that there remains a common lack of understanding as to how these norms should apply. And, hence there is no common consensus as to how this is to be achieved, with the experts, also stressing that further study is ultimately needed in this respect before any leaps forward are possible.

Consequently, at the present time there remains no international, legally binding instruments to regulate inter-state relations in cyberspace. Whilst pocketed action maybe being taken, by isolated States and regions that recognise the obvious and

[37] The bombing of Pan American flight (Pan-Am) 103 over Lockerbie in 1988.

[38] Ibid.

[39] See the Sixty-eighth session, 'Developments in the field of information and telecommunications in the context of international security.' 24 June, 2013. A Report from the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.

The Group was established pursuant to paragraph 4 of General Assembly Resolution A/RES/66/24, Developments in the field of information and telecommunications in the context of international security.

[40] Wolter, Detlev. "The UN Takes a Big Step Forward on Cybersecurity", Arms Control Today, 43, September 2013, http://www.armscontrol.org/act/2013_09/The-UN-Takes-a-Big-Step-Forward-on-Cybersecurity [Accessed 30 April 2016]

'certain' threats of cyber-attack, this is leading to a patch-work approach of national laws and reasoning. For example, such initiatives have included the African Union Convention on Cybersecurity and Personal Data Protection; the Agreement on cooperation among the States members of the Commonwealth of Independent States in combating offences related to computer information; the (2001) Council of Europe Convention on Cybercrime[41]; Directive 2013/40/EU of the European Parliament and of the Council, on attacks against information systems; the League of Arab States Convention on Combating Information Technology Offences; and the Shanghai Cooperation Organization Agreement on Cooperation in the Field of International Information Security, etc.

Whilst 2015 saw some agreements on Internet Governance, these were made under the UN General Assembly (UNGA) on the WSIS 10+ Outcomes Document;[42] and, hence, the 'agreements,' remain an understanding in principle, rather than affective assertive and collaborative action. The UNGA Resolutions have no binding effect and are as much as anything aimed at confidence building rather than serving as a definitive and ultimately effective means of governance and solution.

The difficulty in terms of effective governance and consensus, debatably, centres a round two aspects (1) the conflict of security vs. human rights; and, (2) the very fact that cyberspace remains a contestable area, specifically in terms of trust and ownership. The latter two aspects, that of trust and ownership, acutely are comparable to the very issues that concern aviation and the related legacy of sovereign control and political '*will,*' or apathy, which invariably have stood to prevent liberalisation and fairness of competition equally across the globe (Fox 2014a, b; Fox 2016).

Like aviation (air services), there remains stark political differences largely related to the economic interests of governments, as well as corporate entities, to contend with, and factor in, when discussing Internet governance, and hence cyber protection against attacks. Determining boundaries for each respective party, let alone country jurisdiction, remains controversial. Whilst some boundaries have remained less contentious, with the EU clearly showing the possibility to create a borderless trading zone, (internally at least) the same cannot be said of airspace (Fox, 2016). Equally and comparatively, whilst the sky above us has no discernable-physical boundaries, it is acutely recognised as a State asset. Hence, the airspace above a State has remained a key sovereign right, which is closely safeguarded and inevitably protected (Fox, 2016). For all intents and purpose the same ethos has arguably been adopted in terms of cyberspace. However, reference to cyberspace largely remains outside the scope of most instruments and whilst physical space and airspace above States are recognised by law, international law remains wholly inadequate in offering the protection and definition needed in terms of boundaries and border re cyberspace control and governance.

[41] Convention on Cybercrime *ETS 185 – Convention on Cybercrime, 23.XI.2001* (Budapest).

[42] For example A/RES/70/125 (17th Session) Resolution adopted by the General Assembly on 16 December 2015 in relation to the Outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society.

The word 'cyber-terrorism' maybe set to increase within our everyday vocabulary and ultimately reference; but the very definition and understanding of such will no doubt remain debated and contested (much in the same way as 'terrorism' is[43]). The USA PATRIOT Act 18 U.S.C. 2332b's referred to 'acts of terrorism transcending national boundaries' and made reference to some activities and damage defined in the Computer Fraud and Abuse Act (CFA) 18 U.S.C. 1030a-c. That said, it has also been interpreted that the later Act concerns a criminal act rather than an act of terrorism.

Without much needed clarity in these matters, there invariably remains uncertainty and the raising of issues and questions, in respect to offences in cyberspace, responses and jurisdiction issues. A question of concern would be whether a war could be declared after a cyber-terrorist attack? (Much in the same way as the US contentiously applied 'the war on terror' philosophy and rationale after 9/11.)

Prior to the 2013 report by international experts,[44] the US State Department, in 2012 had already made clear reference to its interpretation and the fact that cyber activities could constitute a use of force under Article 2(4) of the UN Charter and customary international law. According to, Harold Koh, the then-legal advisor, '[c]yber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force.'[45] And hence, the right to self-defence could also be applicable under Article 51 of the U.N. Charter.

A US Congressional Research Service document stated that 'cyberterrorists are state-sponsored and non-state actors who engage in cyberattacks to pursue their objectives;' whilst furthermore adding that 'cyberwar[46] is typically conceptualized as state-on-state action equivalent to an armed attack or use of force in cyberspace that may trigger a military response with a proportional kinetic use of force.'[47] Whilst presenting very powerful terminology, the reality is that a cyber-attack could easily result in retaliation of further cyber-attacks or physical reaction, which could see an escalation of global conflict.

This remains a real danger and one where concerted action needs to be agreed now, before such a serious attack actually occurs and peace is threatened. The US Congressional Report also questioned territorial boundaries and what constitutes an armed attack in cyberspace, making reference to the so-called "Law of War," (also known as the law of armed conflict, embodied in the Geneva and Hague Conventions and the U.N. Charter) offering substantiation to the fact that (in some circumstances)

[43] The legal analysis, Baldor, offered that cyber-terrorism is the 'premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives.'
Lolita Baldor, "Cyber Security Added to US-Australia Treaty," Security on NBCNews.com, 2011, http://www.msnbc.msn.com/id/44527648/ns/technology_and_science-security/t/cyber-security-added-us-australia- treaty/ [Accessed 12 April 2016].

[44] Supra. FN 39.

[45] Harold Hongju Koh, Legal Advisor U.S. Department of State, speaking at a USCYBERCOM Inter-Agency Legal Conference, Ft. Meade, MD, 18, September 2012.

[46] Like cyber-terrorism there remains no clear definition or understanding as to what constitutes cyberwar/cyberwarfare.

[47] Catherine A. Theohary and John W. Rollins. 'Cyberwarfare and Cyberterrorism: In Brief. Congressional Research Service. 7-5700 www.crs.gov R43955. 27 March, 2015.

cyber-attacks, may indeed come within the remit of typically perceived means of warfare. However, the true significance and understanding of its applicability, and therefore the response of nations, remains unclear. For as stated earlier, cyberspace is complicated by the use of remote computers, and retaliation through using such remains highly contentious (but unfortunately foreseeable) particularly when reviewed in terms of the possible harm to third parties from cyber counterattacks. In addition, the Report also raised the issue of territorial boundaries, and what constitutes an armed attack in cyberspace.

There is every reason to believe that terrorism will eventually take a sinister cyber turn, whereby vulnerabilities in critical infrastructure, including within aviation, are targeted. And, inevitably such an attack will invariably test other vulnerabilities that exist, not only in terms of the targeted area but also the lack of understanding and governance for such. This includes the lack of an overarching framework, of agreements, of action and for response.

In 2011 NATO established the Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estonia, which, whilst having honourable intentions, also reinforced the current situation in terms of the lack of a coordinated mechanism. The workshops held, stress the need to be ethical in cyberspace, but this remains a point that will no doubt be missed by the cyber-terrorist. In 2013 the Tallinn Manual on the International Law Applicable to Cyber Warfare was produced. The Tallinn Manual reinforces the global disparity - in the main part, by relating to the *jus ad bellum*, the international law governing the resort to force by States as an instrument of their national policy, and *the jus in bello*, the international law regulating the conduct of armed conflict. However, the manual remains only the expression of scholarly opinions of a group of independent experts. Nonetheless, it draws attention to the conflict between international law and national law, and States' acceptance as to the best way to proceed when such contentious matters arise concerning cyberspace.

Inevitably, there remains a conflict between openness vs. protection. On the one hand, digital and information technology facilitates transnational dialogue, facilitating the global flow of goods, people and services. On the other hand, it is recognised that there is a need to protect (internally) what is perceived as critical national life-sustaining infrastructures, such as electricity and water. However, due to globalisation and increased connectivity, this has become even more complicated by adding a transnational dimension to systems such as air traffic control, which depend on networked information systems, that, in many cases, now extend past national boundaries.

This has created a complex, interconnected and layered dimension. Arguably, the underlying infrastructure that must be protected is the digital enabler of the other critical infrastructures (previously mentioned). Hence, for all nations, the digital infrastructure is increasingly being seen as a key asset - albeit with an increasing international dimension. Aviation, from this perspective, could therefore be viewed as a valuable substructure – which equally needs protecting.

5. PROTECTING AVIATION – *coming full-circle*

Aviation and air travel remains a social and economic enabler of international trade, tourism and everyday living. It is mechanism of survival to many. Whilst air travel is recognised as one of the safest forms of transport,[48] it equally relies on a safe and efficient network to support it. Disruption to these movements would invariably lead to a ripple affect across the globe, much as happened in the aftermath of the 9/11 attacks, where aircraft were used as a means to carry out terrorist atrocities.

ICAO, as a specialised agency of the UN, cites that its current objectives are strongly linked to 13 of the 17 UN's Sustainable Development Goals (SDGs), stating that the Organisation is fully committed to work in close cooperation with States and other UN Bodies to support related targets. But a risk to obtaining these targets remain modern day challenges that compromise safety and security; and, ICAO lists both safety and security (and facilitation of security) in respect to aviation as two of its key objectives.[49] Cybersecurity breaches are inevitably a major cause for concern, and given the history of terrorist-attacks against aviation, aviation has to be viewed as highly vulnerable to the risk of cyber-terrorism.

The 1944 Convention on International Civil Aviation[50] (also known as the Chicago Convention) is a constituent instrument of ICAO. The Preamble to the Convention states the reasoning of the contracting parties for formulating the agreement and summarises the aims and objectives of ICAO (as per Article 44) recognising that,

> 'WHEREAS the future development of international civil aviation can greatly help to create and preserve friendship and understanding among the nations and peoples of the world, yet its abuse can become a *threat to the general security;*'[51]

In reality, this 1944 agreement related to the concept of general security and perceived risks relating to that era.[52] The likelihood of hijackings, seizures and other terrorist events, were arguably not predictable at that time, or at least not to the rate that has transpired and has to date been experienced. And it is said, with almost certainty, that the founders would never have foreseen the risks from cyberspace.[53]

Today, there maybe some common vision as to the risk from cyber-attacks, but arguably there is no firm strategy. A framework has still not been sufficiently developed that is pro-active or reactive, as it may need to be for the future, and the aspect of jurisdiction and response are clearly missing. In December 2014, ironically some 70-years since the Convention, whilst ICAO acknowledged this risk, it was

[48] See amongst other sources: http://ec.europa.eu/transport/modes/air/safety/index_en.htm [Accessed 12 April, 2016]

[49] The others being: air navigation capacity and efficiency, environmental protection and the economic development of air transport.

[50] Convention on International Civil Aviation (1944) Doc. 7300. (Also known as the Chicago Convention)

[51] Emphasis added.

[52] See further discussions within, S. Fox (2014) 'The evolution of aviation in times of war and peace: blood, tears, and salvation', *International Journal on World Peace*, December, Vol. 31, No. 4, pp.49–79.

[53] Ibid.

somewhat underplayed, when it was stated that the 'global aviation system [is] *potentially* vulnerable to attacks from hackers and other cyber criminals.'[54] The declaration was made by five major key stakeholder and players coming together (ICAO, the Airports Council International (ACI), the Civil Air Navigation Services Organisation (CANSO), the International Air Transport Association (IATA) and the International Coordinating Council of Aerospace Industry Associations (ICCAIA)) and agreeing on a common roadmap to align their respective actions on cyber threats. Although, this must be viewed as a progressive step in the right direction, it is arguably one that is very late in coming and certainly cannot be seen as a significant leap. Again it is an intention rather than a decisive measure; although, that said, it is firmly stated that the aim is to be 'more proactive in sharing critical information such as threat identification, risk assessments and cybersecurity best practices.'[55] Invariably, such statements serves only to reinforce and identify that there has not been a sufficiently proactive stance of preventative measures taken to date. However, perhaps worryingly, with the emphasis on '*encouraging* more substantial coordination at the *State level* between their respective government and industry stakeholders on all cybersecurity strategies, policies, and plans,'[56] there is clear recognition that there is not only a lack of governance internationally but at a national, State level too.

The emphasis should be on *ensuring* coordination and cooperation as a means to prevent cyber-attack and cyber-terrorism. In essence the assertion is merely the aspirations for a common goal, 'to work more effectively together to establish and promote a robust cybersecurity culture and strategy for the benefit of all actors in [the] industry.'[57] In other words, there remain no firm underlining enforceable strategy, which includes, standards, and policies. The roadmap does not provide the means to prevent, detect, respond and ultimately recover in the face of a cyber-attack and cyber-terrorism.

At the 2015 Conference on Civil Aviation Cyber Security[58] 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,' which perhaps intimated at the real level of threat to aviation. Such uttering further identifies, that, to date, the world could consider itself fortunate not to have experienced the devastating of cyber-terrorism against an aircraft and/or the supporting infrastructure.

Whilst the 2014 agreement was based upon formalising common responses against 'hackers,' 'hacktivists,' 'cyber criminals' and 'terrorists' who have general 'malicious intent ranging from the theft of information and general disruption to potential loss of life,'[59] Benjamin acknowledged that ICAO Aviation Security Panel's Working Group on Threat and Risk had only recently expanded the scope of its analytical work to include cyber threats. This being part of its continuous review of risks facing civil aviation security, and hence impacting its recommendations for updating the ICAO Global Risk Context Statement.

[54] Emphasis added. 'Aviation unites on cyber threat.' MONTRÉAL, 10 December 2014.
[55] Ibid. http://www.icao.int/Newsroom/Pages/aviation-unites-on-cyber-threat.aspx [Accessed 30 April, 2016]
[56] Emphasis added.
[57] Supra. 54 & 55.
[58] Singapore, 9-10 July 2015.
[59] Emphasis added. 'Aviation unites on cyber threat.' MONTRÉAL, 10 December 2014.

It should be commented upon, that it was only in 2011 that a provision on measures, relating to cyber threats, was introduced by ICAO into Annex 17 to the Chicago Convention,[60] and in this respect, it should be further noted that this relates in the main to Standards and Recommended Practices (SARP's) – wherein it was specifically recommended that States should develop measures to protect information and communications technology systems used for civil aviation from interference that may endanger the safety of our network.

The fact that ICAO's AVSEC Panel's Working Group, is currently considering a number of key initiatives seeking to identify and assess possible cyber-attacks points again only serves to indicate how unprepared the industry has been and arguably remains. This process includes scenarios relating to the aircraft cockpit, cabin and maintenance systems, the inter-related information and communications technologies (ICTs) which support modern air traffic management (ATM) capabilities, and airport-based systems for requirements such as departure control and flight information display.

In 2014-15 new guidance material on cyber threats to critical aviation ICT systems was introduced within the ICAO Aviation Security Manual,[61] with the First Edition of the ICAO Air Traffic Management Security Manual providing further technical guidance.[62]

However ICAO clearly acknowledges that cybersecurity remains a challenge for many industries and that there are difficulties in ensuring the means to coordinate and achieve a consensus approach, which habitually remains a challenge from a governance perspective. ICAO acknowledges that Member States continue to take isolated action, which does not always involve the Civil Aviation Authority (CAA) of the Member State; and, hence, ICAO is currently assembling Member States own framework and guidance documents into a series of reference materials to provide support to the 191 ICAO Member States. This, in essence, reinforces the point that the risk extends beyond aviation and hence involves a multitude of stakeholders and supporting agencies that actually need to be also involved in cybersecurity through a multi-layered framework approach.

5.1. Future needs: tomorrow will become today

In 2013 the (US) FBI Director said,

> '*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.*'[63]

Whilst in 2013 cyber threats may not have been the number one concern – inevitably, tomorrow will become today.

[60] Convention on International Civil Aviation (1944) Doc. 7300.

[61] Doc 8973 - restricted

[62] Doc 9985 – restricted.

[63] Department of Defense – Defense Science Board (DBS), *Task Force on Resilient Military Systems and the Advanced Cyber.'* January, 2013

Statistics confirm that there was an alarming increase of 38% of recorded cyberweb-based attacks in the EU and around the world during 2015. Whilst these are not specifically cyber-terrorist related, it does, nevertheless, show the increase of threat level to that perceived in 2013.[64]

In 2012 the CPNI in consultation with the Joint Coordination Group (JCG) strongly advocated that cybersecurity should be part of all civil aviation considerations. Whilst aviation has achieved an unprecedented level of safety, it is acknowledged that in respect to facing new security threats, 'the global aviation system is at a crossroads.'[65]

Although ICAO has been working on security SARP's for a number of years in relation to the Air Traffic Networks (ATN), cybersecurity aspects are relatively new. Inevitably, there are many remaining challenges for ICAO to overcome in terms of governance before coordinated action can be taken by all contracting States. For example, one governance perspective relates to the complicated inter relationship of the States that are not only Members to the Chicago Convention but to many other Conventions and agreements. Invariably this can lead to conflicts and jurisdiction issues. Taking the Internet as a starting point, it can be seen that the Internet crosses over into the realms of various international bodies, such as the Internet Engineering Task Force (IETF) and Internet Corporation for Assigned Names and Numbers (ICANN). Hence, there remains a conflict in respect to Member States decisions in terms of telecommunications systems passing through their territories and related areas such as security per se and aviation/security matters.

5.1.1. Lessons from Europe

In terms of aviation, Europe has shown perhaps a more coordinated approach particularly through the European Civil Aviation Conference (ECAC) which is an inter-governmental organisation of not only EU States but other Member Countries. Currently there are 44 members. The aim is to harmonise civil aviation policies and practices amongst its Member States and to promote policy understanding. Security is one of the three strategic priorities of ECAC, and, ECAC has investigated cyber threats to aviation being pro-active in producing a handbook on aviation security with a chapter (chapter IV) dedicated to the aspect of cybersecurity. The idea of a European air transport body was first envisaged in 1951, when the Consultative Assembly of the Council of Europe considered made the proposal aimed at achieving the greatest possible degree of co-ordination in inter-European air transport. The origins and formulation involved close liaison with ICAO and at the end of 1955 ECAC held its inaugural session in Strasbourg. ECAC in many ways could be viewed as an aviation 'think-tank' providing an opportunity for discussion but nevertheless without binding implications. That said, the suggestions feed into the European Union (including EASA) and EUROCONTROL. But it should here again be noted that it is only since 2002 that the EU Commission has established common rules in the field of civil aviation security aimed at protecting persons and goods from unlawful interference with civil aircraft.

[64] EU data: Digital Single Market: Cybersecurity & Privacy – (last updated on 11/04/2016 - 17:01) https://ec.europa.eu/digital-single-market/en/cybersecurity-privacy [Accessed 1 May, 2016]

[65] AIAA Decision Paper, 'A Framework for Aviation Cybersecurity.' August 2013

On 27 September 2011 the European Commission hosted a high level conference on security. The timing was perhaps apt, given that it came in the wake of the ten-years anniversary of the terrorist attacks of 11 September in 2001 in the United States.

The purpose was said to discuss the 'future' of civil aviation security but it should be noted that arguably more reference was given to the past decade, rather than appreciating the true significance of future threats. In particular, the following were discussed:

(i) What lessons were learnt from incidents in the past few years?
(ii) What further measures could be taken on an international level to improve risk assessment and resilience to terrorist attacks?
(iii) Should the move be to a more risk based approach to security controls in passenger and cargo traffic?
(iv) How can common platform of sharing and use of available information be developed?
(v) How can better use be made of existing tools and mechanisms in counter-terrorism and customs for the purpose of civil aviation security?
(vi) How successful has the work on a European Union common risk assessment method been so far?
(vii) Is today's model of aviation security controls sustainable in the long term?
(viii) How can the security measures be implemented adequately relative to the threat assessment results with minimum impact on travel and commerce, especially between high-security countries? (Does facilitation have to be at the expense of security?)
(ix) Should further consideration be given to more unpredictable controls/more differentiated controls based on risk? How should the improvement be made in terms of the approach to developing security technologies in the EU?

The conclusion of the Conference[66] was that since 9/11 'civil aviation '*is*' protected by a robust security regime and that the extensive controls in place combined with continued strong intelligence attention have been instrumental in foiling attempts at unlawful interference.' The reference to 'is' may be applicable to the normally perceived risk of terrorism and unlawful interference based upon passed events – but arguably not to cyber-terrorism which the FBI have openly acknowledged is tomorrow's real threat (and hence is arguably now today's).

Statistically it is said, 'the security threat posed to aviation remains relatively small.'[67] That said, arguably this fails to take into account the relative ease of a cyber-attack and the remoteness of a terrorist attack – for which no key statistics are known. However, if key evidence is analysed the potential for a terrorist attack based upon the arguable ease of a cyber breach are enormous.

[66] High Level Conference 'Protecting Civil Aviation Against Terrorists.' Brussels, 27 September 2011 http://ec.europa.eu/transport/modes/air/events/doc/2011-09-27-avsec-conclusions.pdf [Accessed 1 May, 2016]

[67] Ibid.

The following two reported 'real' examples provided serve merely to provide a scenario of the risk of a terrorist attack based upon a cyber breach and a follow-on physical terrorist attack:

> (1) 'A recent Freedom of Information request revealed that the DVLA has been subjected to 264,484 attempted cyberattacks in the past three years, equating to more than 200 a day. Almost 6,000 incidents have been classed as structured query (SQL) attacks. Attacks such as SQLi (SQL Injection) are extremely frequently used by cyber criminals to insert malicious code to exploit computers.'[68]
>
> (2) On 28 April, 2016 it was reported that, 'Hackers target Goldcorp Inc, [and] release reams of private data online including payroll and passports.'[69] Although the attack was aimed at one of Canada's largest mining companies, it highlights the fact that whilst such companies remain at risk, copious amount of private details on individuals are available from various sources.

Whilst arguably these two unrelated events relate to 'remote' access to computer held records, and range from malicious to a criminal intent (exploitation – blackmail) there are obvious lessons to aviation in terms of related risks.

- ✈ For example, passports and driving licences are now linked-records in the UK; so, any breach to the DVLA's computer systems (the Driver and Vehicle Licence Authority in the UK) should be seen as of high concern. The possibility of gaining access to either of these documents (a driving licence or a passport) potentially could lead to terrorists physically gaining access to an aircraft, by distorting information held so as to make the passport appear genuine or through the copying and replication of a true passport. In either case this would mean that a person would be more unlikely to be challenged before boarding an aircraft.

Biometric information, which is now a key feature of a passport is itself an electronic constituent and therefore is subject to illegal access and manipulation. The passport, containing Radio Frequency Identification (RFID) chips, supposedly introduced for purposes of increased security, is also said to be vulnerable and easy to access.[70]

Although UK passports purport to use a strong crypto algorithm to protect their biometric data, the encryption key apparently is easy to steal. As the ICAO's website acknowledges, the key consists of the passport number, the holder's date of birth and the expiration date of the passport, which all are valuable information to a terrorist.

[68] https://threatintelligencetimes.com/tag/dvla-hacked/ [Accessed 1 May, 2016]

[69] http://business.financialpost.com/news/mining/goldcorp-inc-confirms-it-was-hacked-begins-investigation-to-determine-full-scope-of-breach [Accessed 1 May, 2016]

[70] 'A report in the British newspaper The Guardian found the passports surprisingly easy to read and copy. Using a device purchased for £250, a Guardian reporter was able to view and copy information from several of the new passports': see https://www.eff.org/deeplinks/2006/11/british-rfid-passports-easily-hacked referring to: https://www.theguardian.com/technology/2006/nov/17/news.homeaffairs [Accessed 1 May, 2016]

However, potentially a more alarming variable of a cyber-attack can be seen based upon another mode of transport – the automobile, and the fact that in 2015 Fiat Chrysler was forced to issue what was said to be a '*safety* recall affecting 1.4m vehicles in the US' after security researchers showed that one of its cars could be hacked.[71]

The relative ease in penetrating a vehicle could easily translate to aviation and various related systems; and, whilst it potentially is of little benefit to a terrorist to target individual motor vehicles the same could not be advocated of an aircraft.

As was said at the conclusion of the 2011 European Commission on security,[72]

> … '*aviation is a symbol of international trade, freedom, and entrepreneurship. The public is highly risk averse when aviation is concerned, and creating a climate of fear and suspicion is part of the terrorist game-plan. Attackers may target not only loss of life but also disruption of business operations. That makes aviation an attractive target to international terrorism*.'

Debatably, the travelling public remain oblivious to the real risks that exist when they fly, and arguably, this has to date, not been exploited by a terrorist. Whilst the ultimate findings were that there is still more to be done, little acknowledgement was specifically made to the area of cybersecurity.

However, Europe has shown 'preparedness' in terms of a response and crisis management approach in the event of a cyber-attack (and hence cyber-terrorism). Whilst this may not be aimed at preventative measures, the European Aviation Crisis Coordination Cell - EACCC[73] is actively engaged in ensuring an improved level of preparedness in Europe for any kind of crisis potentially having an impact on air traffic. In the main this is aimed at safety factors, however security incidents (terrorism) are also stated, which includes the possibility of massive cyber-attacks.

From a EU perspective securing network and information systems is viewed as essential to ensuring prosperity and to keeping the online economy running. In 2013 the Commission put forward a proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union. Whilst it has taken some time for the Parliament and Council to agree on the text of the Network and Information Security Directive (NIS)[74] it will nevertheless serve as a

[71] http://www.bbc.co.uk/news/technology-33650491 [Accessed 1 May, 2016]

[72] High Level Conference 'Protecting Civil Aviation Against Terrorists.' Brussels, 27 September 2011 http://ec.europa.eu/transport/modes/air/events/doc/2011-09-27-avsec-conclusions.pdf [Accessed 1 May, 2016].

[73] European Aviation Crisis Coordination Cell (EACCC) was given a legal basis in Commission Regulation (EU) No 677/2011 of 7 July 2011 on the ATM network functions (under Chapter IV, Articles 18 and 19) which set the requirements for its establishment and the responsibilities of the Network Manager to support the EACCC.

[74] Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union. COM(2013) 48 final. Brussels, 7 February, 2013.
Agreement was reached on the Commission's proposal on 7 December 2015 and the draft proposal for the NIS Directive was published 11 days later. On 14 January 2016, the EU's Internal Market

global indicator in terms of the ability for coordination and cooperation under a specific legislative act and furthermore of the ability to add the same level through to specific industries and sectors.[75] The Directive will also stand to address the fact that the EU is often criticised for championing user privacy, and has lagged behind the US when it comes to network security.[76] That said, the comparison of the two is arguably not relative and misleading. In many ways, the EU has always demonstrated the ability and success of a union of countries coming together and achieving common goals. There remains no other example of a unity of countries accomplishing the same in the world in terms of agreements (including legislatively). From an aviation perspective, the degree of liberalisation across (the current) 28-individual States is held up to be an example of what is able to be achieved. And this may yet be translated through into cybersecurity.

The purpose of the EU NIS Directive is to provide a legal measure to 'boost the overall level of cybersecurity in the EU by:'

- 'increasing the cybersecurity capabilities in the Member States
- enhancing cooperation on cybersecurity among the Member States
- ensuring a high level of risk management practices in key sectors (such as energy, transport, banking and health).'

In this respect it should be noted that transport is specifically noted in terms of being a vital sector. Hence, the Directive[77] stands to build upon and develop previous legislation and agreements in relation to linked areas, such as telecommunications, security, etc.

Within the overall EU Cyber Strategy[78] - The Commission has included cybersecurity and e-privacy at the heart of its political priorities. Once again, on the one hand, this arguably reinforces the conflict between security and privacy, yet, on the other hand, it also stresses the alignment of these areas and hence the need for privacy to be adequately protected through appropriate security measures. Arguably, these are the same very issue that the computer giant, 'Apple' recently experienced in the US with regards to granting access to telephone information following a terrorist incident.[79]

Trust and security remain at the core of the Digital Single Market Strategy which was launched in 2015; whilst, the European Agenda on Security for the period 2015-

Committee voted to support the political agreement.

[75] It should be noted that the EU is active within an EU-US Working Group on Cybersecurity and Cybercrime, as well as an active participant of the Organisation for Economic Co-operation and Development (OECD), the United Nations General Assembly (UNGA), the International Telecommunication Union (ITU), the Organisation for Security and Co-operation in Europe (OSCE), the World Summit on the Information Society (WSIS) and the Internet Governance Forum (IGF).

[76] http://www.computerweekly.com/feature/What-the-EUs-cyber-security-bill-means-for-UK-industry [Accessed 1 May, 2016]

[77] Following the second reading it was adopted by the European Parliament on 6 July 2016.

[78] The Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. JOIN(2013) 1 final. Brussels, 7 February, 2013.

[79] This followed the attacks committed by a married couple with ties to fundamentalist jihadists in San Bernadino, California, in 2015.

2020[80] aims at Member States' cooperating in order to tackle security threats and establish common efforts in the fight against terrorism, organised crime and cybercrime.

The implementation of NIS is seen as key legislative means to overcome the fact that networks are not bound by geography and nationality and hence the success of such a Directive may have key implications in the formulation of further legislative instruments, and hence, aviation cybersecurity. But this again remains inevitably a regional initiative.

6. CONCLUSION – *facing the future*

There can be no denying that the day has come when one of the biggest threats to aviation safety and security lies in attacks, in, or related to, cyberspace. Whilst at the present time these attacks may be said to be of a minor nature they are nevertheless increasing, and will no doubt also increase as to the consequences too.

In a three-week period between 17 January, 2015 and 1 February, 2015, it is stated that US based airlines were targeted with more than 50 threats posted upon social media site. These related to bomb threats, which resulted in a F-16 fighter jets being used to escort a Southwest flight and a Delta flight into Atlanta's Hartsfield-Jackson International Airport.[81] Although these incidents were no doubt malicious, no bombs were actually found, and the Internet purely served as a means to scare and alert to the threat. Inevitably the interconnectivity of the Internet and the use of cyberspace poses a much greater risk to aviation – the infrastructure and to the aircraft flying above us, particularly in the form of a terrorist attack.

Whilst the threat towards aviation has been apparent for some time, it has only more recently seen measures being introduced to reduce threats that have included a cyber dimension.

There remains a magnitude of cybersecurity vulnerabilities to aviation, and future attacks are likely to see less direct intrusion measures, such as physically into the cockpit, where risks have been minimised due to lessons learnt from past events. Instead, catastrophic attacks will no doubt be perpetrated against aircraft through vulnerable access points, such as a gate links and ground support networks when the aircraft is on the ground, or inevitably eventually through a direct cyber-attack when the aircraft is inflight. Whilst technical solutions will aid to reduce these vulnerabilities, it will nevertheless result in a race to stay ahead in terms of ensuring that terrorists remain one step behind. In this respect, it should be noted, that this paper has not ventured into the realms of technology advancement – save for the vulnerability of such from the Internet.

Inevitably, the solutions to tackle cybersecurity lie within the hands of numerous stakeholders, including governments and industries both within and external to

[80] EU Press Release, 'Commission takes steps to strengthen EU cooperation in the fight against terrorism, organised crime and cybercrime.' Strasbourg, 28 April 2015

[81] Rene Marsh, '*Airlines Get More Than 50 Online Threats Since January 17.*' CNN Politics. http://www.cnn. com/2015/01/28/politics/airlines-online-threats-50/ [Accessed 1 May, 2016]

aviation. But the challenge is not an easy one to tackle and resolve.

Like aviation (particularly in respect to sovereignty of the skies above a State) the Internet and cyberspace suffers from national protectionism related largely to an intangible asset. There is also the dilemma in terms of privacy of Internet data and the sharing of this information – even when it comes to the implementation of security mechanisms to protect such. Hence, rule makers and regulatory bodies find themselves, in the main, only being able to rely on cooperative agreements and acceptable practices.

In the first instance, the true awareness of the vulnerability faced by civil aviation needs to be realised and an effective multi-layered defensive and reactive framework needs to be established.

At the present time ICAO identifies that,

> *'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.'*[82]

But, like aviation, cybersecurity extends beyond boundaries and whilst defences can be created nationally and regionally through ensuring that there is some form of legislative approach, (including a national civil aviation cybersecurity policy) there is arguably the need for a civil aviation security architecture. This should encompass legislation and technology standards, extending into adjacent policies addressing shared risks relating to cybersecurity breaches (and inevitably terrorism).

It is perhaps alarming to consider, that, in 2016, when the threats of cyber-attack are not only upon us but are evidently occurring – that such a tool and apparatus still has not been agreed. Particularly given,

- the 1994 Manual[83] (followed by the 1999 UN Manual on Cybercrime[84])
- plus the UN Resolution of the same year (1994[85])
- and in particular the later UN Resolution 55/63[86] - which implied the need of a law enforcement mechanism to tackle the problems that 'may' arise from cyber-technology.

Yet, in truth, aviation remains only a small part of this challenge – which necessitates determining how best to mitigate the risks of cyber-attacks to all critical infrastructure. That said, aviation, more so arguably than other critical infrastructure – save the Internet and cyberspace, extends well beyond national borders. In many ways, cyberspace and aviation share so many common factors and problems - both

[82] Chapter 4 of Annex 17 – (2011 and 2014 amendments).

[83] United Nations Manual on the Prevention and Control of Computer-related Crime, International Review of Criminal Policy, Series M, Nos. 43-44 (United Nations publication, Sales No. E.94.IV.5.

[84] United Nations Manual on the Prevention and Control of Computer Related Crime, International Review of Criminal Policy nos. 43 and 44 (1999).

[85] Resolution 49/158 of 23 December 1994 on strengthening the United Nations crime prevention and criminal justice programme.

[86] Also see: United Nations Resolution on Combating the Criminal Misuse of Information Technologies GA RES 55/63, UNGA 55th Session, 81st Plenary Meeting UN Doc. A/RES/55/63 (2001).

provide a means to communicate, one physically and the other remotely, and both have been instrumental in quickening the pace of globalisation.

The very point that aviation stands at a crossroad[87] is largely due to the fact that, in expanding so rapidly and providing the means to join the globe through quick travel, it has needed to use innovative technologies that have caused a dependency on information and communication provided via the cyberspace. Inevitably, it is the same technology which is also vulnerable to attack and for which there is a lack of coordination to protect.

Like other parts of humankinds history, it appears that lessons have not been learnt from past aviation events. In the case of *Lockerbie,* joint investigations were conducted by the US and UK authorities, however there were considerable judicial complications with regards to prosecutions. *Lockerbie* visibly showed the conflict of international and national law, and hence politics.[88] It clearly tested the international legal order of the United Nations and the International Court of Justice following a terrorist attack; and, whilst there have been calls for a UN Treaty for a stand-alone International Court or Tribunal for Cyberspace, progression has been once again been slow in terms of achieving consensus and inevitably drive to pursue this. However, this reluctance is not new. The Convention on the Suppression of Unlawful Acts relating to International Civil Aviation[89] (The 'Beijing' Convention) was said by Abeyrante to be '*a step forward in the right direction with the threat of cyber terrorism looming, affecting the peace of nations'* (Abeyrante 2011). Fox, furthermore added that *'[a]ir transport could well be a target towards the erosion of that peace*.'[90] Yet, whilst the Beijing Treaty may have been a 'basis' for responding to 'new and emergent threats to security,'[91] (for the first time perhaps, revealing the need to be pro-active - one of preparedness before an event) it is still not in force, and is unlikely ever to be so.[92] Inevitably, this fact serves to emphasise international apathy in regard to being prepared and coordinated in the event of a cyber-terrorist attack. Ultimately, this may yet have a wider negative effect on adjacent policies and, in essence, to stability and peace.

The world's population increasingly relies on air travel, and airlines are expected to see an increase in travellers over an indefinite period, leading to a doubling of passengers and a forecasted 7 billion passengers taking to the skies by 2034.[93] This equates to a '3.8% average annual growth in demand (2014 baseline year).'[94] With a projected growth in air travel, this will inevitably lead to more aircraft occupying the skies. By 2018 the number of devices connected to Internet Protocol (IP) networks is

[87] Supra. FN. 65.
AIAA Decision Paper, 'A Framework for Aviation Cybersecurity.' August 2013

[88] See the discussions within: S. J. Fox (2015) CONTEST'ing Chicago origins and reflections: *lest we forget! Int. J. Private Law*, Vol. 8, No.1, 2015 pp 73-98.

[89] ICAO Doc. 9960, Signed at Beijing on 10 September 2010 [accessed 15 April 2016].

[90] Ibid - See the discussions within: S. J. Fox (2015) CONTEST'ing Chicago origins and reflections: *lest we forget! Int. J. Private Law*, Vol. 8, No.1, 2015 pp 73-98.

[91] ICAO Doc. 9960, Signed at Beijing on 10 September 2010 [accessed 15 April 2016].

[92] Ibid.

[93] IATA: Total passengers set to double to 7 billion by 2034. Press Release No.: 55. 26 November 2015

[94] Ibid.

expected to be almost twice as high as the global population.[95] Hence, networks will continue to become more connected and electronic data will need to be further shared, thus intensifying risks for cyber-based attacks. All this is technology that aviation will continue to rely heavily on for efficiency and effectiveness on the ground and in the increasingly congested skies.

Perhaps worryingly, likewise, globally, terrorism remains on the rise, with 2015 witnessing the biggest annual rise in deaths caused by terrorism, with more than 32,000 people killed in attacks around the world.[96] Putting this back into an aviation context, this equates to almost a fivefold increase in fatalities since the events of 9/11.[97] Inevitably these factors should be a concern to every State and importantly serve as a stark reminder of the challenges that lay ahead. Disturbingly, it may take a cyber-terrorist atrocity (on the scale of 9/11) against aviation before adequate mechanisms and coordination is ultimately put in place. And at such a time the world will no doubt question why it happened and why it wasn't prepared when the signs and warning were clearly staring it in the face.

References

Abeyratne RIR (2011) 'The Beijing Convention of 2010 on the suppression of unlawful acts relating to international civil aviation – an interpretative study'. *Journal of Transportation Security* 4(2):131–143

Avery Martin (2010) '*Muskoka Terror G8: Activist and Terrorist From Huntsville to Algonquin Park*' Lulu.com.

Blackbourn, J., Davis, F.F. and Taylor, N.C. (2012) 'Academic consensus and legislative definitions of terrorism: applying Schmid and Jongman', *Statute Law Rev.*, 19 November, doi: 10.1093/slr/hms041 [online] http://slr.oxfordjournals.org (accessed 13 April 2016)

COM (2011) 144 (final) '*Roadmap to a Single European Transport Area – Towards a* competitive and resource efficient transport system.' Brussels, 28.3.2011.

Fox S (2014a) 'The evolution of aviation in times of war and peace: blood, tears, and salvation.' *International Journal on World Peace* 31(4):49–79

Fox S J (2014b) To practice justice and right' international aviation liability: have lessons been learnt? *International Journal of Public Law and Policy* 4(4):162–

[95] Cisco, 'The Zettabyte Era—Trends and Analysis'. [Online]. Available: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual- networking-index-vni/VNI_Hyperconnectivity_WP.html. [Accessed 24 April 2014].

[96] ABC News (Melissa Clarke) 'Globally, terrorism is on the rise - but little of it occurs in Western countries.'17 Nov 2015. http://www.abc.net.au/news/2015-11-17/global-terrorism-index-increase/6947200 [Accessed 20 May, 2016].

[97] Guardian Newspaper report by Ewan MacAskill. 18 November, 2014. http://www.theguardian.com/uk-news/2014/nov/18/fivefold-increase-terrorism-fatalities-global-index [Accessed 20 May, 2016].

182

Fox S J (2015) CONTEST'ing Chicago origins and reflections: *lest we forget! Int. J. Private Law* 8(1):73–98

Fox S (2016) Single European Skies: Functional Airspace Blocks – Delays and Responses. *Air & Space Law* 41(3):201–228

Neumann, Peter G. (1997) Computer security in aviation: *Vulnerabilities, Threats, and Risks* international conference on aviation safety and security in the twenty-first Century, 13–15 January 1997; White House Commission on safety and security, and George Washington University

Saul B (2005) Definition of 'terrorism' in the UN Security Council: 1985– 2004. Chinese Journal of International Law 4(1):141–166

Weinberg L, Pedahzur A, Hirsch-Hoefler S (2004) The challenges of conceptualizing terrorism. Terrorism and Political Violence 16(4):777–794. doi: 10.1080/095465590899768 (accessed 1 April 2016)