For EALA Prize 2015

# Cyber Security in Civil Aviation

July 2015

Deepika Jeyakodi
Adv.LL.M in Air and Space Law, Leiden University

# TABLE OF CONTENTS

***'Absence of Evidence is not the Evidence of Absence'***

## A. INTRODUCTION

Scenes from the movie Die Hard, where the safety and security of aircraft are compromised using computers, and even eventually turning the aircraft into weapons, can no more be dismissed off as mere fiction. Even as the aviation industry grows in leaps and bounds, with improvement and innovation in design, technology, and efficiency, its fragility can be witnessed in the sphere of cyber security.

Cyber attacks are a global issue and there are unlimited ways to attack an aircraft's integrity considering its increased dependence on information and communication technology. Such dependence, directed towards reducing human interference and errors, may jeopardize safety, security, and efficiency. Perpetrators use the cyberspace as a new tactic and weapon against their targets. The anonymity, difficulty in assigning responsibility, inexpensiveness, quick attack time, and limited counter-attack mechanisms are few of the contributing factors that make cyber-attacks an effortless opportunity for miscreants, and a potentially catastrophic threat for aviation industry stake-holders as well as beneficiaries.

In general, a legal and regulatory framework for cyber standards, security and enforcement is still in its nascent stages. While so, the situation demands that cyber security issues, in a critical infrastructure[1] such as aviation, need to be resolved.

---

[1] The loss or compromise of which would have a major detrimental impact on the availability or integrity of essential services, leading to severe economic or social consequences or to loss of life,
http://www.cpni.gov.uk/about/cni/#sthash.up2EiCNN.dpuf

## B. CYBER VULNERABILITY OF AVIATION

In aviation, there are multiple points of attack for cyber terrorists/hackers; from the manufacture of aircraft and its equipment, to any stage of their operation. 'Cyber terrorism, whether conducted by individuals, corporations or States, could target the electronic systems of companies, which design and develop hardware and software used in airports, air traffic control systems; It could target industries involved in the construction of aircraft and components whether they be used for civil or military purposes'.[2]

Airplanes are sophisticated systems of engineering. It comprises of a complex network of components that essentially comprise of, but are not limited to a base system, communication links, sensors, and avionics. Ground control systems, air navigation service providers, and more communication links complement this. Just as any other computer, these components and communication links are prone to cyber-attacks that include but are not limited to hacking, jamming[3], and spoofing[4]. 'This interconnectedness can potentially provide unauthorized remote access to aircraft avionics systems;'[5] and this is particularly applicable to newer planes such as the Boeing 787 Dreamliner and long-haul Airbus models such as the A350 and A380.[6] An attack may be on the entire system

---

[2] Abeyratne Ruwantissa,'*Cyber Terrorism and Aviation—National and International Responses*', Journal of Transportation Security, 2011, Vol.4 (4), at pp.342.

[3] 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.

[4] Faking the sending address of a transmission to gain illegal unauthorized entry into a secure system, Cyber Security Glossary, http://niccs.us-cert.gov/

[5] *'FAA Needs a More Comprehensive Approach to Address Cybersecurity As Agency Transitions to NextGen,'* Report of the U.S.Government Accoutability Office, GAO-15-370, http://www.gao.gov/assets/670/669627.pdf

[6] *Id.*

or targeted at individual components, or it could be a manipulation of systems to carry out physical attacks.

Earlier, in 2015, United Airlines had grounded all its flights in the US, reportedly after bogus flight plans appeared in its system.[7] A few weeks later, Polish airline LOT encountered a cyber-attack that affected their ground operation systems. As a result they were not able to create flight plans and outbound flights from Warsaw are not able to depart.[8]

At the DerbyCon 2013, a white-hat[9] demonstrated that with equipment worth $2000, ghost planes could be introduced into the Air Traffic Controller's screen to cause chaos, since there was no verification process to determine where messages were relayed from and no authentication process is involved. In the same year, another hacker, Hugo Teso, demonstrated[10] how to gain remote access into the cockpit system, gain control and remotely programme flights from the ground using a simple application and off-the-shelf electronic equipment. [11] This demonstration urged not only governmental organizations but also several IT Security Analysts to investigate the vulnerability of aircraft to cyber-attacks.

Several incidents have also demonstrated that Global Positioning System (GPS) has been subject to intentional and unintentional targeting and disruption by both state and non-state actors. The 2011 capture of a drone by Iran is still one of the most controversial cyber incidents, wherein it was alleged that an RQ 170

---

[7] *'Security Experts Warn Airlines Face Threat of Cyber Attacks'*, Sydney Morning Herald, July 6, 2015.

[8] *'Polish Airline, Hit By Cyber Attack, Says All Carriers Are At Risk'*, Reuters, June 22, 2015, Warsaw/Frankfurt.

[9] Ethical hacker

[10] Black Box Security Conference, 2013, Amsterdam.

[11] Flight Management System and Simon App,

Sentinel was brought down by the Iranian Armed Forces' electronic warfare unit.[12] Following this incident there were several estimations on the possibility of cyber hijack of aircraft. Subsequently, in July 2012, Todd Humphreys, demonstrated in his 'Statement on the Vulnerability of Civil Unmanned Aerial Vehicles and Other Systems to Civil GPS Spoofing',[13] the ability to hijack an Unmanned Aerial Vehicle (UAV) by GPS Spoofing. This was established remotely tricking[14] the aircraft, from a distance of a half mile away, into a commanded dive that was only aborted 10 feet above the ground to prevent it from crashing. Much earlier, in 2009, Newark Liberty International Airport experienced sporadic outages of the GPS Ground-based Augmentation System used for precision approach landing. The ground station 300 feet away experienced signal interference every day at about the same time. The Federal Aviation Authority (FAA), discovered the cause of the outage was a GPS jammer being used by a truck driver to avoid being tracked by his employer.[15] Reliance on open civilian GPS is a matter for concern, as the aviation industry is seeing a marked shift from the use of traditional radar based identification and guidance systems, to one that is based on satellite navigation and automation.[16]

---

[12] *'Iran shows off captured US drone'*, The Telegraph (UK), Dec 8, 2011, *'Obama says U.S. has asked Iran to return drone aircraft'*, CNN Wire Staff, 2011, *'Iran says it built copy of captured U.S. drone'*, CNN International, May 12, 2014.

[13] Submitted to the Subcommittee on Oversight, Investigations, and Management of the House Committee on Homeland Security.

[14] Using equipment that costed less than US $2000, http://www.bbc.com/future/story/20140206-can-drones-be-hacked.

[15] Emilio Iasiello, *'Aviation and Cyber Security: Getting Ahead of the Threat'*, Aerospace America, July-August 2013 at pp. 24.

[16] Example., U.S's NextGen Automatic Dependent Surveillance–Broadcast (ADS-B)

By 2020, ADS-B[17], a surveillance technology will be replacing radar as the primary means of tracking aircraft and will be a compulsory requirement on the majority of aircraft. Being a data infrastructure, it will provide traffic and weather information, offering better communication between the aircraft and air traffic control. However, till date, the ADS-B system remains unprotected and vulnerable to cyber-attacks. Communications between aircraft and air traffic controllers remain unencrypted and unsecured, making it open for attacks that can disrupt air traffic. It remains vulnerable to jamming and spoofing of information.

The disappearance of the MH370 flight had also raised questions on the possibility of cyber-jacking[18] as the possibility of all transponders being switched off to relay location signals despite having state-of the-art communication and reporting system was doubted by several cyber experts. This was triggered by Boeing's request earlier in 2014 to the FAA to incorporate changes to its aircraft designs citing security reasons, as there was a possibility of its in-flight entertainment systems being connected to other critical systems of the aircraft.[19]

The above examples are merely the tip of the iceberg. At every stage, with every new information and communication technology innovation in this industry, the other side would be waiting to test the vulnerabilities and possibly launch attacks. Apart from potential damage to property and life, the chaos and resulting economic losses, there also exists an angle of psychological threat, whereby such cyber interference may play havoc on the integrity of air transport as it did post the 9/11 attacks, instilling some sort of reluctance to air travel.

---

[17] Automatic Dependent Surveillance Broadcast.

[18] A hijack using unconventional cyber weapons.

[19] Dr.Sally Leivesley, British anti-terrorist expert and former Home Office Scientific Adviser, News Report to The Express, March 14, 2014.

## C. LEGAL AND REGULATORY FRAMEWORK

Aviation is a unique critical national infrastructure that requires the application of higher standards of security to fortify their systems from cyber-attacks, than those that are applied to general electronic infrastructure. Having said that, it should be acknowledged, that laws in relation to cyber-security, have not matured yet. Nevertheless, it is not a lawless 'Wild West' scenario. Efforts have already been initiated and are evolving at the international, regional and national levels to address concerns.

Firstly, of particular relevance are the efforts taken by the International Civil Aviation Organization (ICAO). In the early 1970s, ICAO published a Security Manual to assist its Member States to take measures for the prevention of unlawful interference, minimize its effects, and established standards by adopting Annex 17 of the Chicago Convention, thereby establishing a security culture. However, the threat posed by cyber security was left unaddressed until recent times.

The Universal Security Audit Programme[20] recently commenced the auditing of access controls and related security lapses in ICT systems. This was the first step forward in identifying the potential risks in cyber security. Over the years, the ICAO has effectively strengthened existing 'Standards and Recommended Practices' (SARPs) and evolved new recommended practices in respect of Air Traffic Network Security too.[21] The Internet Engineering Task Force (IETF)[22], Internet Corporation for Assigned Names and Numbers (ICANN) [23] , FAA and EUROCONTROL

---

[20] ICAO Assembly Resolution A33-1, October 2001, adopted as a part of the Aviation Security Plan of Action, http://www.icao.int/Meetings/FAL12/Documents/Biernacki.pdf

[21] Amendments made in respect of Annexes 6 and 11 of the Chicago Convention as regards to use of standardized equipment, message handling etc,.

[22] Responsible for aircraft mobile standards routing.

[23] Responsible for internet infrastructure.

collaborated in 2008 with ICAO to discuss about the impact of Boeing's 'Connexion'[24] on global internet routing. Discussions left it clear that aircraft internet service, including the new next generation air traffic management networks, could be highly disruptive to the global Internet. No formal agreements resulted, though, it was suggested that aviation needed to isolate the Internet from disruptions caused by their global aircraft network movements.[25]

It is projected that in a decade over 30,000 aircrafts will occupy our skies and each of these aircraft would be using its own internet bases with each nation owning and controlling their network operations instead of the ideal single network operator. ICAO seems to assume that since telecommunication is a national subject, each State determines what passes through its territory and the responsibility for any default in security will vest with that State. In a world where traffic, data, voice, video, etc. is transmitted via internet, this attitude is untenable in the long term[26]. Ideally ICAO could define a "closed/isolated" network architecture that would both make their aviation network operation easier to manage and isolate the Internet, although for now this seems like a long shot.

In 2009, at the behest of the European Civil Aviation Conference, the Aviation Security Panel along with the Working Group on New and Emerging Threats, looked into the challenges posed by cyber security; It came out with

---

[24] An in-flight online internet connectivity service.

[25] Terry L. Davis, about '*Aviation Network*' at http://www.ietf.org/mail-archive/web/cin/current/msg00005.html

[26] Centre for Protection of National Infrastructure, UK, Report on Cyber Security in Civil Aviation, August 2012, at http://www.cpni.gov.uk/documents/publications/2012/2012020-cyber_security_in_civil_aviation.pdf

several recommendations[27], which includes but not limited to the evaluation of cyber-risks and incorporation of 'unpredictability' into SARPs. Based on the proposals of the Committee on Unlawful Interference[28], the 12th Amendment, and based on the Aviation Security Panel's recommendations, the 14th Amendment, to Annex 17 were made applicable from July 2011 and November 2014 respectively. Chapter 4 of Annex 17 now deals with cyber threats. It recommends 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.'*

Although this provision is in the nature of a recommendation, the imperative need to address the concerns relating to cyber security may compel the States to take efforts in this direction. The ICAO is working on new safety standards for 2018 on large unmanned aircraft that can fly across borders; Early 2015, saw the agency mulling whether to take the unusual step of helping countries draft domestic rules for integrating drones into regular airspace.[29] As UAVs are more prone to cyber-attacks, it is widely expected that cyber security issues would be considered in depth. If so, general aviation would also benefit from such developments.

Further, the Beijing Convention[30], 2010, which is yet to come into force, is hailed by cyber security experts as the first step forward in securing the aviation industry. The treaties adopted in Beijing further criminalize the act of using civil

---

[27] Report of the Aviation Security (AVSEC) Panel, Twentieth Meeting, AVSECP/20 at 2.1, April 2009.

[28] Followed by the ICAO Assembly Resolution A36-20, 17th November 2010.

[29] *'U.N. Aviation Agency Mulls Advising On Domestic Drone Rules'*, Reuters Montreal, Mar 24, 2015.

[30] The Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation, ICAO Doc. 9960.

aircraft as a weapon, and of using dangerous materials to attack aircraft or other targets on the ground.[31] It is in this Convention that the problem of cyber threats is implicitly addressed. It provides that an offence is committed when a person destroys or damages air navigation facilities or interferes with their operation, if any such act is likely to endanger the safety of aircraft in flight.[32] This undoubtedly refers, inter alia to cyber terrorism, but strangely links the offence exclusively to the safety of aircraft in flight. If therefore as a result of an act of cyber terrorism, a taxing aircraft collides with an aircraft, which has opened its doors for disembarkation, but the passengers are still on board awaiting disembarkation, that act would not be considered an offence in terms of the passengers in the process of disembarkation. In other words, the offender would not be committing an offence either against the second aircraft or its disembarking passengers.[33] An offence is also said to be committed where a person communicates information, which that person knows to be false, thereby endangering the safety of an aircraft in flight.[34] This can be applied to situations where personas are engaged in interrupting air navigation services. However, the term "safety in flight" may restrict the scope of this provision if such communication is made when the doors are open or when the aircraft is not actually in flight. Moreover, the limited scope of this Convention to attacks on air navigation facilities, an interference with their operations, and/or communicating false information, excludes a wide variety of attacks. The above notwithstanding, the Beijing Treaty of 2010 is a step forward in

---

[31] Abeyratne Ruwantissa, *'The Beijing Convention of 2010 On The Suppression of Unlawful Acts Relating To International Civil Aviation—An Interpretative Study'*, Journal of Transportation Security, 2011, Vol.4 (2), at pp.132.

[32] *Supra*, note 30, Article 1(d).

[33] *Supra*, note 31 at pp.137.

[34] *Supra*, note 30, Article 1(e).

the right direction with the threat of cyber terrorism looming, affecting the peace of nations.[35]

Secondly, the efforts of various international and regional organizations, which contain elements that would apply to aviation, may be used as building blocks for the development of laws and regulations to address cyber-security issues in aviation. The United Nations Manual on Cybercrime[36] and United Nations Resolution of 2001 [37] which stress on the establishment of a law enforcement mechanism to tackle the problems that may arise from technology, are a culmination of the efforts taken by various international and regional organizations such as the United Nations, Council of Europe, Interpol, the OAS[38], the ECAC[39] and OECD[40]. The 2001 Cybercrime Convention[41] was formulated in anticipation of situations where cyber technology may be used to commit criminal acts. It recommends States Parties to adopt legislative or other measures to counter illegal inception of transmission of computer data, data interception and exchange

---

[35] *Supra*, note 31 at pp.138.

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

[37] 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).

[38] Organization of American States.

[39] European Civil Aviation Conference.

[40] Organization for Economic Co-operation and Development. In 2002, OECD announced the completion of "*Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*".

[41] European Treaty Series no. 185 or *the Budapest Convention of the Council of Europe* was opened for signature in November 2001 and came into force on 1 July 2004. As of October 2014, 44 states have ratified the convention, while a further nine states had signed the convention but not ratified it.

interception.[42] This along with Article 7 on alteration of data and forgery[43], require States to establish interceptions and alterations as criminal offences under its domestic law. Following this, various strategies, co-operative agreements and frameworks have been developed and adopted by the EU, ASEAN, the Asia-Pacific Economic Cooperation, the International Telecommunications Union, the Economic Community of West African States etc,. A recent development in regulating cyber activities in the international arena is the Draft United Nations Treaty on an International Criminal Court or Tribunal for Cyberspace[44], which could pave the way for a strong and unified law enforcement mechanism for cybercrimes. These laws would principally deal with the after-math of a cyber-attack on aviation. Although it would be appropriate to harden the aviation infrastructure from attacks, this second level measure will be paramount in acting as a deterrent to potential perpetrators.

Thirdly, of considerable importance are the national laws that some countries have adopted in line with the Cybercrime Convention; although their effectiveness is questionable. While there are many provisions that address jurisdiction, economic activity, privacy, content etc., those relating to cyber security and its breach are either inadequate or non-existent at best. Additionally, the enforcement provisions are often poorly designed and the punishment is far disproportionate to the resultant economic loss. This can be attributed to the lack of understanding and consequent poverty in defining cybercrimes specifically

---

[42] *Cybercrimes Convention*, Articles 3, 4 and 5 respectively.

[43] When committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible.

[44] 9th Edition, June 2014.

regarding to hacking, unlawful interference, data alteration etc. For example, in Brazil[45] the law addresses only manipulation of data by authorized public servants, consequently, there is no mention about external actors; In India[46] the term 'hacking' is defined, yet, the punishment for the same is 3 years imprisonment and/or a fine equivalent to 1000 Euros; In China[47] the punishment for interference with computer systems is punishable with imprisonment for 7 years; Korea[48] is comparatively, the country with the strongest cyber laws, wherein any damage to Critical Information Infrastructure, would attract a 10 year imprisonment and a fine of 100 million Korean currency. Similar provisions can be found in the national legislations of USA[49] and UK[50]. Increasing reports on cyber incidents may probably force or at least urge these States to revisit their national cyber laws, in order to acclimatise them to changing demands.

Fourthly, apart from the above mentioned laws, there exist guidelines and 'good practices' that are frequently prescribed by various bodies within the aviation industry. In a way, these efforts from within the industry can be termed as self-regulation mechanisms. IATA's[51] Aviation Cyber Security Toolkit[52], ECAC's

---

[45] *Law no. 9983 of July 7, 2000*, Insertion of fake data into systems of information Article 313-A / Non-authorized modification or alteration of systems of information Article 313-B.

[46] *Information Technology Act, 2000*.

[47] '*Regulations on Safeguarding Computer Information Systems'*, Feb. 1996 / Criminal Law of the People's Republic of China Articles 285, 286, 287.

[48] *Act On Promotion of Information and Communications Network Utilization and Information Protection*, etc. Chapter VI *Stability of the Information and Communications Network/ Information Infrastructure Protection Act*.

[49] *Homeland Security Act of 2002*, *USAPATRIOT Act of 2001* etc.,

[50] *Regulation of Investigatory Powers Act (RIPA) of 2000*, *Computer Misuse Act of 1990*, The *Anti-Terrorism, Crime and Security Act of 2001* etc,.

[51] International Air Transport Association

guidance material for member states on cyber security control measures, studies by the EUROCONTROL[53] at the various stages of Single European Sky ATM Research[54] programme, are a few examples. The U.K's Centre for Protection of National Infrastructure, the U.S.' National Institute of Standards and Technology, and several other national and regional organizations are drawing attention to the issue and calling for a coordinated response. The organization that is leading its way into cyber-security research is the Federal Aviation Authority. In February 2015, a notice of assignment was made to the Aviation Rule making and Advisory committee to make recommendations on Aircraft Systems Information Security/ Protection (ASISP). Moreover, it is also advancing on Airborne Radio Standards Development and prescription of airworthiness standards for ICT components in aviation. Besides, it is also collaborating with the U.S. Homeland Security in applying the Cyber Security Assessment and Risk Management Approach 'CARMA' to Aviation Sector. The initiatives taken by the FAA may act as an archetype for future laws and regulations governing aviation cyber-security.

Finally, several independent cyber security analysts, University IT labs,[55] manufacturers, and ethical hackers are actively involved in conducting research, identifying exploits and vulnerabilities, and recommending guidelines to various

---

[52] Launched in October 2014 to identify, assess and mitigate, cyber risks in aviation IT infrastructure, '*Aviation Cyber Security Toolkit North American Premiere at AVSEC World*', IATA Press Release, 28/10/2014.

[53] International organization with 39 member states, supporting its members to achieve safe, efficient and environmentally friendly air traffic operations across the whole of the European region.

[54] Hereinafter referred to as SESAR.

[55] System-Aware Secure Sentinel developed by Georgia Institute of Technology and Virginia Tech, in which the new system detects "illogical behavior" compared to how the aircraft normally operates before initiating warnings, *'Watching The Watchmen: US Shield To Protect Drones From 'Spoofing' Cyber-Attacks'*, Russia Today, December 6, 2014.

stakeholders in the industry. Aforesaid practices will go a long way in testing the waters, subsequently resulting in the establishment of unified aviation cyber security architecture.

Overall, there is promise for the future, nonetheless, the law needs to catch up with the rise of the cyber-dependent systems to efficiently regulate and protect various stakeholders and beneficiaries.

### D. SUGGESTIONS

It is clear that terrorizations to aviation infrastructure from cyber-attacks are real and imminent. It is required to develop a hybrid system that amalgamates elements of the aviation and IT industry to create a suitable environment for safe and secure operation.

The first step in this direction would be to see the complete picture by understanding, identifying and accepting the existence of cyber threats and risks. The full implications of the increased connectivity and dependency on ICT need to be understood in light of evolving cyber threats.[56] The States need to foresee that even a single incident of cyber-attacks may cause enormous damage. Keeping in mind the unique nature of cyberspace and the activities therein, even if separate laws to address cyber-attacks are not made, incorporation of corresponding provisions must be made into their local criminal laws so that they are well-equipped to deal with such circumstances if and when they arise. A separate 'Cyber Security Architecture' for aviation can be devised by establishing common standards in order to keep the structure closed and thereby subject to strict regulation and control. Further, a cyber security culture must be established

[56] *'A Framework for Aviation Cyber Security'*, AIAA Decision Paper, August 2013.

through formulation and strong implementation of SARPs; This could be effectively carried out by encouraging co-ordination and co-operation between States as well as industry players and establishing a cyber-security incident reporting and response system. Components, data communication systems, especially COTS, have to be hardened against cyber-attacks. Manufacturers should ensure that a minimum standard in security is applied. Adopting a prescriptive approach, as suggested by Stefan Kaiser,[57] airworthiness standards may be applied to the aviation IT components for their reliable and stable use. Not prescribing such a standard fearing an adverse economy would have dangerous consequences as '…the quality standards commonly practiced in the information technology industry do not suffice airworthiness standards'.[58] Automatic re-programming, kill switches etc., should be incorporated in systems as a fall back measure when it is under said attack. A cyber-attack can be intercepted only in a manner that is similar to the one employed by hackers; by blocking signals, or hacking to assume control. Training of personnel at various levels in various capacities to meet the challenges posed by cyber threats is necessary, in order to launch response attacks to secure networks, the aircraft, and/or third parties. This can be achieved by taking inputs from cyber experts including those who test vulnerabilities as third party actors. A certification examination for operators must also test the operators' cyber-security knowledge.

---

[57] '*RPAS/UAS: A Challenge For International, European And National Air Law*', Workshop of EASA and Institute of Air and Space Law, University of Cologne, 23-24 May 2013.

[58] Stefan Kaiser, *'UAVs and Their Integration into Non-segregated Airspace'* (2011) 36 Air and Space Law, Issue 2, pp. 161–172.

The need of the hour is an assessment of the 'spectrum of threats, not simply the worst one imaginable, in order to properly understand and coherently deal with the risks to people, institutions, and the economy'.[59]

## E. CONCLUSION

'As a key critical infrastructure and an essential link to commerce and passenger transportation, the global aviation industry will remain a target for adversaries seeking to make a statement or cause substantial loss to life and financial bearing. Like many emerging threats, cyber attacks still loom in the periphery, bordering on the 'not yet realized,' and are seen more as a stylized fiction than an actual possibility'.[60] Technological advancement, dependence thereon, current economic pressures to reduce labour, increase automation etc,. should not act as an impediment to the security of the aviation industry. The development of a cyber-security framework is urgent. The only way forward to tackle this new and emerging threat is to find a global solution. Every day, in the field of aviation, some innovation is made, more so when it comes to the part of information and communication technology. The key to ensuring its security would be to keep up with the developments thereby being in a position to confront the threats rather than evoking responsive action after its occurrence.

[59]John Mueller, Mark G. Stewart *'Terror, Security, and Money'*, Oxford, 2011, pg.16.

[60] *Supra*, note 15 at pg.25.

**LIST OF SOURCES**


International Law / Treaties /Resolutions

- Cybercrime Convention, 2001
- United Nations Manual on the Prevention and Control of Computer Related Crime, International Review of Criminal Policy nos. 43 and 44 (1999).
- 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).
- European Treaty Series No. 185
- The Tokyo Convention On Offences And Certain Other Acts Committed On Board Aircraft, 1963
- The Hague Convention For The Suppression Of Unlawful Seizure Of Aircraft, 1970
- Montreal Convention For The Suppression Of Unlawful Acts Against The Safety Of Civil Aviation, 1971.

Articles/Reports

- Abeyratne Ruwantissa, *'Cyber terrorism and aviation—national and international responses'*, Journal of Transportation Security, 2011, Vol.4, Issue 4.
- Emilio Iasiello, *'Aviation and Cyber Security: Getting Ahead of the Threat'*, Aerospace America, July-August 2013.
- Abeyratne Ruwantissa, *'The Beijing Convention Of 2010 On The Suppression Of Unlawful Acts Relating To International Civil Aviation—An Interpretative Study'*, Journal of Transportation Security, 2011, Vol.4, Issue 2.
- Dr. Marco Gercke, *'Regional and International Trends in Information Society Issues'*, Cybercrime Research Institute, 2010
- '*We Need To Talk About Cyber Security'*, Aviation Business, 26/06/2014.
- *'A Framework for Aviation Cyber Security'*, AIAA Decision Paper, August 2013.
- '*Advances in Intelligent Systems and Computing International Joint Conference*', SOCO'13-CISIS'13-ICEUTE'13, Springer, 2014.
- *'FAA Needs a More Comprehensive Approach to Address Cybersecurity As Agency Transitions to NextGen,'* Report of the U.S.Government Accoutability Office, GAO-15-370.

- Stefan Kaiser, '*RPAS/UAS: A Challenge For International, European And National Air Law'*, Workshop of EASA and Institute of Air and Space Law, University of Cologne, 23-24 May 2013.
- Stefan Kaiser, *'UAVs and Their Integration into Non-segregated Airspace'* (2011) 36 Air and Space Law, Issue 2.
- John Mueller, Mark G. Stewart '*Terror, Security, and Money'*, Oxford, 2011.
- Todd Humphreys *'Statement on the Vulnerability of Civil Unmanned Aerial Vehicles and Other Systems to Civil GPS Spoofing'*, 2012.

Websites

- http://www.icao.int/Meetings/FAL12/Documents/Biernacki.pdf
- http://www.ietf.org/mail-archive/web/cin/current/msg00005.html
- http://www.cpni.gov.uk/documents/publications/2012/2012020-cyber_security_in_civil_aviation.pdf
- http://niccs.us-cert.gov/
- http://www.gao.gov/assets/670/669627.pdf
- http://www.bbc.com/future/story/20140206-can-drones-be-hacked.

Other

- Cyber Security Glossary
- *'Security Experts Warn Airlines Face Threat of Cyber Attacks'*, Sydney Morning Herald, July 6,2015.
- *'Polish Airline, Hit By Cyber Attack, Says All Carriers Are At Risk'*, Reuters, June 22, 2015,
- Warsaw/Frankfurt.
- *'Iran shows off captured US drone'*, The Telegraph (UK), Dec 8,2011, *'Obama says U.S. has asked Iran to return drone aircraft'*, CNN Wire Staff, 2011, *'Iran says it built copy of captured U.S. drone'*, CNN International, May 12, 2014.
- '*U.N. Aviation Agency Mulls Advising On Domestic Drone Rules'*, Reuters Montreal, Mar 24, 2015.
- '*Aviation Cyber Security Toolkit North American Premiere at AVSEC World*', IATA Press Release, 28/10/2014.
- *'Watching The Watchmen: US Shield To Protect Drones From 'Spoofing' Cyber-Attacks'*, Russia Today, December 6, 2014.


***National Laws were cited for reference only, hence they are not included in the bibliography.**

***The websites listed were last accessed on July 15th, 2015.**