Chapter 3
Security Issues

Cyber Terrorism, attacks on the integrity of travel documents, the use of full body scanners and issues flowing therefrom, civil unrest as they threaten the security of airports and unlawful interference with civil aviation are issues that draw the attention of the aviation community in general and the air transport industry in particular.

3.1 Cyber Terrorism

Cyber crimes and cyber terrorism are becoming increasingly menacing and the latter has been identified as a distinct threat requiring attention. At the 21st Aviation Security Panel Meeting of ICAO (AVSECP/21, 22 to 26 March 2010) a new Recommended Practice related to cyber threats was proposed for adoption by the Council as part of amendment 12 to Annex 17 (Security) to the Convention on International Civil Aviation (Chicago Convention). It was adopted on 17 November 2010, will become effective on 26 March 2011 and applicable on 1 July 2011. This Recommended Practice suggests that each Contracting State 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. At the 22nd Meeting of the Panel, conducted by ICAO from 21 to 25 March 2011, the Panel noted the value of vulnerability assessments pertaining to cyber security in aviation whose objectives are to evaluate the efficiency of existing mitigation measures and identify any vulnerabilities from a threat-based perspective and further noted that better understanding of residual risks.

Cyber terrorism is an inescapable facet of today's world, and has led to substantial changes in the way we respond to terrorism. The international and national reliance placed on cyberspace for the development and maintenance of human interaction will further increase in the coming years and, in connection with this ongoing growth, dire threats and daunting challenges will proliferate from cyber terrorists. An advantage of cyber terrorism is its anonymous nature, permitting

R. Abeyratne, *Strategic Issues in Air Transport*,
DOI 10.1007/978-3-642-21960-3_3,

hackers to prevent any trace of their movements through checkpoints or physical evidence to be linked to them. Such terrorism can also be run on low budgets, as the only costs incurred are those related to interference with the computer programs of a State, through the purchase of the necessary computer equipment.[1] The unavoidable challenge posed by cyber terrorism is that our digital world, which allows us to create and share knowledge, also provides ample opportunity for terrorists to commit cyber crimes. The digital environment nurtures motivated offenders who are able to explore covert capabilities for exploiting vulnerabilities in that environment. Thus, limiting the opportunities for subterfuge is another challenge to be faced in the development of the cyber environment. Currently, the most ominous obstacle to be overcome is the lack of guards to prevent crimes against the digital world.[2]

In considering the above, we must first establish the difference, if any, between cyber crime and cyber terrorism and determine whether there are any common links. Cyber crime was termed "computer[3] crime" in the early stages of its evolution and has also been called "computer related crime" or "crime by computer".[4] At its most basic, cyber terrorism may be defined as "an assault on electronic

[1] Author Michael Hanlon envisions the consequences of a cyber attack as: "at first, it would be no more than a nuisance. No burning skyscrapers, no underground explosions, just a million electronic irritations up and down the land. Thousands of government web pages suddenly vanish... the disruption continues: thousands of popular websites, from eBay to YouTube, start malfunctioning or are replaced by malicious parodies. Tens of millions of pounds are wiped off the share price of companies like Amazon as fears grow that the whole Internet credit card payment network is now vulnerable and insecure... eventually, reports start to flood in that hundreds of thousands of personal bank accounts have been raided overnight". See Michael Hanlon, Attack on the Cyber Terrorists, Mail Online at http://www.dailymail.co.uk/sciencetech/article-457504/Attack-cyber-terrorists.html.

[2] Cohen and Felson (1979). James D. Zirin, writing to the *Washington Times* said: "It is an irony of the digital age that technology has aided the security forces in detecting and thwarting terrorist operations and has helped terrorists do their evil". See http://bit.ly/d41gsV.

[3] Computers have been defined as "systems of machines that process information in the form of letters, numbers, and other symbols, and that are self directing within predetermined limits". *Webster's New International Dictionary* defines a computer as "a mechanical or electronic apparatus capable of carrying out repetitious and highly complex mathematical operations at high speeds". Computers are used in business for the maintenance of inventories, the calculation and preparation of payrolls, etc.; in industry for the automatic operation of machinery, the control of refinery operations, etc.; and in research for the determination of flight characteristics of missiles and spacecraft, the prediction of the behaviour of substances acted upon by a number of variables, etc. These definitions were cited by the Canadian Supreme Court in *R.* v. *McLaughlin* [1980] 2 SCR 331 at 339.

[4] See House of Commons Standing Committee on Justice and Legal Affairs, Computer Crime, Final Report (1983), at 12. The *Oxford English Dictionary* defines cyber crime as: "crime or a crime committed using computers or the Internet". It is significant that, in 1998 an 18-year-old Israeli hacker Ehud Tenenbaum, popularly known as the "Analyzer," penetrated the computer systems of the Pentagon, National Aeronautics and Space Administration, Massachusetts Institute of Technology, Naval Undersea Warfare Center, and other highly protected computer systems in the United States. A United States Defense Department official called it "the most organized and

communication networks".[5] The Federal Bureau of Investigation provides a fuller definition: "the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against non-combatant targets by sub-national groups or clandestine agents".[6] A commentator declares that cyber terrorism is terrorism in cyberspace, carried out through the use of computers, the Internet and technology-based networks or systems against infrastructures also supported by computers and such networks.[7] A further interpretation is that cyber terrorism involves employing computer networks in order to harm human life or sabotage critical States infrastructures in ways that may cause harm to human life.[8] Consideration of these definitions demonstrates that the activities related to both cyber crime and cyber terrorism are intended to sabotage infrastructure and disrupt computer systems. As can be seen, though the activities involved may be the same or similar in both categories, the motive behind cyber crime may differ to that in cyber terrorism. A 1999 report by the Centre for the Study of Terrorism and Irregular Warfare determined that the probability of significant cyber attacks in the future are in addition to the traditional physical attacks carried out by terrorists.[9]

Cyberspace, comprised of millions of fibre optic cables enabling servers, computers and routers, is the nervous system of any State's critically important infrastructures, significant among which is transportation. Attacks on cyberspace can cause immeasurable harm, particularly by disrupting education centres and religious places of worship, and essential services such as government, banking and finance, telecommunications, transportation, infrastructures, health and health care,

systematic attack the Pentagon has seen to date". See *Master hacker 'Analyzer' held in Israel*, 18 March 1998, at http://www.cnn.com/TECH/computing/9803/18/analyzer/index.html.

[5] http://wordnetweb.princeton.edu/perl/webwn.

[6] http://www.crime-research.org/Cyber_Terrorism_new_kind_Terrorism. Two other definitions are worth noting: "A criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social or ideological agenda" (United States National Infrastructure Protection Center); and "the use of computer network tools to shut down critical national infrastructure (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population" (Center for Strategic and International Studies, author James Lewis).

[7] Dunnigan (2003). Cyber terrorism brings to the fore two significant modern fears, those of technology and terrorism (see Embar-Seddon 2002).

[8] Definition provided by Shlomo Harnoy, Founder, senior Vice President and Professional manager at SDEMA Group, and Yossi Or, Vice President Information Security at SDEMA Group. The SDEMA Group is an integrated homeland security solutions partnership specializing in risk mitigation. SDEMA also offers information security services including market forward protection against cyber terrorism. This definition is also accepted in academic literature. See Weimann (2006).

[9] Dhanashree Nagre and Priyanka Warade, Cyber Terrorism, Vulnerabilities and Policy Issues "Facts Behind the Myth", at http://www.andrew.cmu.edu/user/dnagre.

power and energy generation and distribution, manufacturing, agriculture and food, electricity and water supply, and military defence. Of these, aerospace activities[10] and air traffic control[11] are prominent targets.

Cyber terrorism may be seen as a corollary to a change in control in manufacturing utilities, banking and communications, moving from secured national control to globally networked computers.[12] The threat of cyber terrorism is all the more real for having already occurred and that future occurrences could be prodigious. Blaise Pascal states in *Ars Cogitandi* that fear of harm ought to be proportional not merely to the gravity of the harm but also to the probability of an event.[13] Fundamentals of risk management define that, given similar conditions, the occurrence of an event in the future will follow the same pattern as in the past.[14] It seems a given, then, that we may face the daunting possibility of a nuclear 9/11 in the future,[15] possibly aided and abetted by cyber terrorism.

The events of 11 September 2001 demonstrated that the three most vulnerable targets for a terrorist attack are people, infrastructure and technology, since they are the foremost components of a successful economy. The incident also emphasised the inextricable interdependencies between physical and cyber infrastructures. Cyber terrorism is thus a "clear and present danger"[16] and the question has even been raised as to whether 9/11 was a result of cyber terrorism.[17]

---

[10] In March 1998, the website of the National Aeronautics and Space Administration NASA received a 'denial of service' attack, calculated to affect Microsoft Windows NT and Windows 95 operating systems. These attacks prevented servers from answering network connections and crashed computers, causing a blue screen to appear. The attacked systems were revived, but this attack was a follow-up to one perpetrated in February of the same year when, the United States Defense Department had unclassified networks penetrated for two weeks, with hackers accessing personnel and payroll information.

[11] On 18 March 1998, federal criminal charges were unsealed against a computer hacker who had disabled a key telephone company computer servicing Worcester airport. As a result of a series of commands sent from the hacker's personal computer, vital services to the Federal Aviation Administration control tower were disabled for six hours in March of 1997, see http://www.justice.gov/criminal/cybercrime/juvenilepld.htm. In April 2002, it was reported that hackers were able to penetrate a Federal Aviation Administration system and download unpublished information on airport passenger screening activities. See Poulsen (2002).

[12] *The White House, The National Strategy to Secure Cyberspace* (2003), at 5, at http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf.

[13] Ferguson (2008).

[14] *Ibid.*

[15] Bobbitt (2008).

[16] In the 1919 decision of *Schenk* v. *US* [249 US 47 (1919)], Justice Oliver Wendell Holmes used the words *clear and present danger* when the United States Supreme Court adjudicated the case of Charles Schenk, who had distributed leaflets allegedly calculated to incite and cause insubordination and obstruction in recruits of the American Socialist Party. The actions of Schenk were considered to constitute an offence under the *Espionage Act* of 1917. See also Stohl (2006).

[17] James Corbett, *The Corbett Report*, 9/11 and Cyberterrorism: Did the real "cyber 9/11" happen on 9/11? 17 July 2009, see http://www.corbettreport.com/articles/20090717_cyber_911.htm. For an informative discussion on cyber terrorism post-9/11 see Cortes (2004).

In taking action against cyber crimes, then President Bill Clinton, in a 1999 speech to the National Academy of Sciences said: "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... we must be ready... ready if our adversaries try to use computers to disable power grids, banking, communications and transportation networks, police, fire, and health services – or military assets.[18] In order to achieve this objective", President Clinton outlined a strategy based on a new programme "Cyber Corps" that would be in addition to and augment government efforts already in place to counter cyber terrorism, at the same time initiating new strategies calculated to strengthen the protection of critical systems. The President stated that he would seek the support of Congress to allocate $1.46 billion in the next federal budget for this strategy,[19] involving a 40% increase from previous spending on related efforts. This proposed measure was opportune as, according to a 2002 survey conducted by the Federal Bureau of Investigation and a San Francisco-based computer security institute, 90% of large corporations and government agencies in the United States had experienced unauthorized computer breaches in 2001.[20]

Under then President George Bush, the United States adopted, in 2003, a *National Strategy to Secure Cyberspace*, aimed at preventing cyber attacks against critical American infrastructures, reducing national vulnerability to cyber attacks and minimizing damage and recovery time from actual cyber attacks.[21] The Strategy defines the national priority as securing the government's cyberspace and national security and initiating international cooperation on cyberspace security. The strategy would be supported by a response system, threat and vulnerability reduction programme, and awareness and training programme, for national cyberspace security. A significant principle of this strategy was its recognition that efforts to counter cyber terrorism should involve strong, proactive collaboration between those providing essential services in the United States, since the federal government could not—and should not—secure nor interfere with the computer networks of banks, energy companies, transportation firms, and other activities of the private sector. Similarly, the federal government should not intrude into the computer networks of homes and small businesses, universities, and State and local agencies and departments. The *Strategy* therefore exhorted each American who depends on cyberspace and information networks to secure the part that they own or for which they are responsible.

[18] http://news.cnet.com/2100-1023-220532.html.

[19] http://news.cnet.com/2100-1023-220532.html#ixzz1HWoNI8fW.

[20] Misra (2003).

[21] *The National Strategy to Secure Cyberspace*, February 2003, Washington DC, Executive Summary, see http://www.dhs.gov/files/publications/editorial_0329.shtm. The Cyberspace Strategy is an implementing component of the *National Strategy for Homeland Security* and is complemented by a *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*.

The annual *Threat Assessment of the United States Intelligence Community for the Senate Select Committee on Intelligence*[22] of 2010 shows the extent of the cyber terrorism threat in its statement that the agility and technological innovation demonstrated by the cyber criminal sector far exceeds the response capability of network defenders. The *Threat Assessment* identified two components as particularly vulnerable to cyber attack: *Network Convergence*, the merging of distinct voice and data technologies to the point where all communications are relayed over a common network structure; and *Channel Consolidation*, the concentration of data on individual users captured by service providers through e-mails or instant messages. The *Threat Assessmen*t drew an implicit parallel between cyber terrorism and international organized crime, extrapolating the theory that international criminal organizations will increasingly hinder the ability of legitimate businesses to compete and may even push legitimate players out of the market.[23]

Further, whether conducted by an individual, a corporation or a State, cyber terrorism has the potential to target the electronic systems of companies that design and develop hardware and software used at airports and in air traffic control systems. Such terrorism may also target industries involved in the construction of aircraft and components, whether they are used for civil or military purposes. One commentator says:

> [h]ere, the objective is that of manipulating, in the design phase, software orhardware which will eventually come to be used in critical environments. The eventslinked to the theft of designs relating to the American F-35 project are an exampleof this kind of act.[24]

A review conducted in 2010 by the United States Government reported that the Federal Aviation Administration (FAA) computer systems remained vulnerable to cyber attacks, since most air traffic control facilities had not been enhanced to adequately respond to cyber intrusions.[25] The threat of cyber terrorism was

---

[22] *Threat Assessment of the United States Intelligence Community for the Senate Select Committee on Intelligence,* 2 February 2010, ATA February 2010 – Intelligence Community Statement for the Record, at 3, see http://www.cfr.org/intelligence/annual-threat-assessment-intelligence-community-senate-select-committee-intelligence-2010/p21369.

[23] It is disturbing that a recent study from the Department of Homeland Security highlighted how the information technology systems of the United States Computer Emergency Readiness Team, which are used by the National Cyber Security Division in its mission to be the focal point in terms of cyber security, both at the public and private levels, suffer from numerous and dangerous vulnerabilities linked above all to the problem of a poor information technology security culture amongst its employees, see Department of Homeland Security (DHS) – Office of Inspector General, "*DHS Needs to Improve the Security Posture of Its Cybersecurity Program Systems*", at http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_10-111_Aug10.pdf.

[24] Stefano Male, *Cyber Warfare and its Damaging Effects on Citizens*, September 2010, at https://www.infosecisland.com/download/index/id/30.html.

[25] Lolita C. Baldor, Cyber Security Still Issue for FAA, *Boston Globe*, 13 August 2010, at http://www.boston.com/news/nation/washington/articles/2010/08/13/cyber_security_still_issue_for_faa. A Department of Energy report released in May 2009 documented successful attacks that have affected FAA networks. In 2006, the FAA shut down a "portion of its air traffic control systems in

considered with regard to the Boeing *Dreamliner* 787, whereby the FAA reportedly claimed that "the plane may be at risk for hacking on to its on-board computer system, with disastrous consequences".[26]

In an aviation context, therefore, cyber terrorism has multiple facets that can disrupt air transport in many ways. Acts of cyber terrorism could be used to spread disinformation or engage in psychological warfare, with media attention being manipulated regarding possible threats, leading to disruptions in airport and aircraft operations. The end result would be a "fear factor", such as was seen in the immediate aftermath of 9/11, where individuals displayed increased reluctance to travel. This could, in turn, result in economic losses, particularly in States that are dependent on the tourism industry to boost their Gross National Products. At the most serious level, cyber terrorism could lead to fatalities, injuries and major damage at airports and to aircraft in flight.[27]

3.1.1 International Efforts

Offences against civil aviation, particularly with regard to unlawful interference with civil aviation related to aircraft have been addressed on three major occasions, though the *Tokyo Convention* of 1963, *The Hague Convention* of 1970 and the *Montréal Convention* of 1971.[28] Yet none of these conventions referred, whether directly or indirectly, to cyber terrorism.

The first such convention to do so, the 2010 *Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation* adopted in Beijing,[29] states in Article 1d) that an offence is committed when a person destroys or damages air navigation facilities or interferes with their operation, if any such act is likely to endanger the safety of aircraft in flight. This clearly refers, inter alia, to cyber terrorism, yet links the offence exclusively to the safety of aircraft in flight. Article 2a) of the Convention provides that an aircraft is considered to be in flight at any time from the moment when all its external doors are closed following embarkation until the moment when any such door is opened for disembarkation. In the event of

Alaska" due to a "viral attack", and in 2008, FAA computers, again in Alaska, were compromised and 40,000 usernames and passwords were stolen. In 2009, an FAA "public-facing web application computer" was compromised, leading to the theft of "PII on 48,000 current and former FAA employees", see Nart Villeneuve, Thoughts on "Critical Infrastructure" 13 December 2009, at http://www.nartv.org/2009/12/13/thoughts-on-critical-infrastructure-protection/.

[26] Kim Zetter, FAA: New Boeing 787 Dreamliner may be Vulnerable to Hacker Attack, http://www.wired.com/politics/security/news/2008/01/dreamliner_security.

[27] See Guill (2000).

[28] See generally, Abeyratne (1998), which extensively discusses the treaties. See also, Abeyratne (2010a).

[29] *Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation,* done at Beijing on 10 September 2010.

a forced landing, the flight would be deemed to continue until the competent authorities take over responsibility for the aircraft and for persons and property on board. For instance if, as a result of an act of cyber terrorism, a taxiing aircraft collided with an aircraft that had opened its doors for disembarkation, but passengers were still on board, such an act would not be considered an offence in terms of the passengers in the process of disembarkation. That is, the offender(s) would not be committing an offence under the convention either against the second aircraft or its disembarking passengers. Nonetheless, the Beijing Convention of 2010 is an initial step toward countering the threat of cyber terrorism, a threat directed often toward the target of air transport.

More generally, yet with relevance to the field of aviation, are the activities conducted since the 1980s by international organizations such as the United Nations, Council of Europe, INTERPOL, and the Organization for Economic Co-operation and Development[30] in response to the challenges posed by cyber crime. A significant result of such collective efforts was the publication of the *United Nations Manual on Cybercrime*[31] and 2001 United Nations Resolution[32] exhorting States, in the context of an earlier United Nations Resolution on Millennium Goals,[33] which recognized that the benefits of new technologies, especially information and communication-related technologies, are available to all, to ensure that their laws and practices eliminate safe havens for those who criminally misuse information technology. The Resolution also urged States to ensure the cooperation of law enforcement authorities in the investigation and prosecution of international cases of the criminal misuse of information technology, and that this should be coordinated among all concerned States. The Resolution further required information to be exchanged between States regarding the challenges faced in combating such criminal misuse and stated that law enforcement personnel should be trained and equipped to address any criminal misuse of information technology.

Further, the Resolution recognized that legal systems should protect the confidentiality, integrity and availability of data and computer systems from unauthorized impairment, ensure that criminal abuse is penalized, and that such systems should permit preservation of and quick access to electronic data pertaining to specific criminal investigations. The Resolution called upon mutual assistance regimes to ensure the timely investigation of the criminal misuse of information

[30] The mission of the Organization for Economic Co-operation and Development is to promote policies that will improve the economic and social well being of people around the world. The Organization provides a forum in which governments can work together to share experiences and seek solutions to common problems, and works with governments to understand what drives economic, social and environmental change.

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

[32] *United Nations Resolution on Combating the Criminal Misuse of Information Technologies* General Assembly Resolution 55/63, United Nations General Assembly 55th Session, 81st Plenary Meeting, UN Doc A/RES/55/63 (2001).

[33] A/RES/55/2.

technology and the timely gathering and exchange of evidence in such cases. States were requested to make the public aware of the need to prevent and combat such criminal misuse. Finally, the Resolution called for information technology to be designed to help prevent and detect criminal misuse, trace criminals and collect evidence to the extent practicable, recognizing that countering the criminal misuse of information technology requires the development of solutions that take into account the protection of individual freedoms at the same time as their privacy and the preservation of the capacity of governments to fight such misuse.

A second significant activity borne of international collaborative responses to cyber crime was the adoption of the *Cybercrime Convention*[34] of the Council of Europe, opened for signature in November 2001, and which came into force on 1 July 2004. In the United States, this Convention was ratified by then President Bush on 22 September 2006 and entered into force on 1 January 2007. The main focus of this Convention is the risk that computer networks and electronic information might be used for committing criminal offences and that evidence relating to such offences may be stored in and transferred over these networks. States Parties to the Convention therefore expressed their view in a Preambular Clause that cooperation between States and private industry in combating cyber crime was necessary and that there was a need to protect legitimate interests in the use and development of information technology. The intent of the Convention falls under three goals:

a) Harmonizing domestic criminal substantive law elements of offences and connected provisions in the area of cyber crime;
b) Providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form; and
c) Setting up a fast and effective regime of international cooperation.

Article 2 of the Convention requires each Party to adopt the legislative and other measures that may be necessary to establish access to the whole or any part of a computer system, when committed intentionally, without right, as a criminal offence under domestic law.[35] Additionally, a Party may require that the offence

[34] European Treaty Series no. 185. Forty-two European States, the United States, Canada and many other States were signatories to the Convention.

[35] A computer system under the Convention is a device consisting of hardware and software developed for the automatic processing of digital data and may include input, output, and storage facilities. It may stand alone or be connected in a network with other similar devices. "Automatic" means without direct human intervention, "processing of data" means that data in the computer system is operated by executing a computer programme, which is a set of instructions that can be executed by the computer to achieve an intended result. A computer can run different programmes and a computer system usually consists of different devices, such as a processor, central processing unit, and peripherals, which are devices that perform specific functions in interaction with the processing unit, such as printers, video screens, compact disc readers and writers, or other storage devices. See *Cybercrime Convention*, Explanatory Report, paragraph 23.

be committed by infringing security measures, with the intent of obtaining computer data or with other dishonest intent, or in relation to a computer system that is connected to another computer system. Other provisions call for States Parties to adopt legislative or other measures to counter illegal inception of transmission of computer data, data interception and exchange interception.[36] Of particular significance to aviation is Article 7 on the alteration of data and forgery, which requires each Party to adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data, with the intent that such data be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is directly readable and intelligible. The Provision concludes that a Party may require an intent to defraud, or similar dishonest intent, before criminal liability may be imposed.

Article 7 also calls for the protection of certain measures adopted by the aviation community to ensure the integrity of passports and other machine readable travel documents using technology such as the Public Key Directory (PKD). The PKD has been developed using the quantum cryptography technique, intended to eradicate vulnerabilities to fraud in the use of digitally stored data. Quantum cryptography transmits information along cables by polarized photons rather than electronic signals. These photons are tiny particles of light sensitive enough that they immediately become corrupted when intercepted, thus rendering their message unintelligible and alerting both sender and recipient to the attempt at fraud or spying. The use of the PKD technique in passports provides a good example. In this case, the PKD is designed and proposed for use by customs and immigration authorities who verify biometric details in an electronic passport. The PKD is based on cryptography, an already viable tool that is now considered by the aviation community as a fail-safe method for ensuring the accuracy and integrity of passport information.

Biometric information in the identification of persons is another method that counters cyber terrorism and unlawful interference with computer imagery. Biometrics involve measuring the distinguishing physiological or behavioural traits of individuals and storing them in an automated database such as machine-encoded representations created by computer software algorithms, which compare these with the actual features. Biometrics that have been successfully used and are the most appropriate for this scientific process are facial recognition, fingerprinting and iris-recognition. Identification through biometrics involves four steps: first, the capture or acquisition of a biometric sample; second, the extraction or conversion of the sample into an intermediate form; and third, the creation of templates of this data for storage; and fourth, the comparison of the information offered in a travel document with that which is stored in the template.

[36] *Cybercrime Convention*, Articles 3, 4 and 5 respectively.

3.1.2 National Efforts

Interception of data is a significant offense that is a precursor to cyber crime and cyber terrorism. The *Cybercrime Convention* defines interception as:

> Listening to, monitoring or surveillance of the content of communications, to theprocuring of the content of data either directly, through access and use of thecomputer system, or indirectly, through the use of electronic eavesdropping ortapping devices.[37]

Australia adopted the *Telecommunications (Interception and Access) Act* in 1979. Section 7(1) provides that a person must not intercept, authorize, suffer or permit another person to intercept or do any act or thing that will enable him or her or another person to intercept a communication passing over a telecommunications system.[38] An important provision is Section 108 (1), which provides that an offence is committed if a person, with intent and knowledge, accesses a stored communication or authorizes, suffers or permits another person to access a stored communication or does any act or thing that will enable them or another person to access a stored communication, where the intended recipient of the stored communication or the person who sent the stored communication had no knowledge of the offender's act.

In Canada, a Bill[39] was introduced in Parliament in 2005 aimed at introducing reforms to the legislative structure concerned with the unlawful interception of documents and communications. In the absence of specific legislation, parallels may be found in Canada's criminal legislation. For example, Section 184(1) of the *Canadian Criminal Code* provides that an agent of the State[40] may intercept, by means of any electromagnetic, acoustic, mechanical or other device, a private communication if either the originator of the private communication or the person intended by the originator to receive it has consented to the interception, or the agent of the State believes on reasonable grounds that there is a risk of bodily harm

[37] *Cybercrimes Convention* Explanatory Report, paragraph 53.

[38] The Act defines a telecommunications system as a service for carrying communications, by means of guided or unguided electromagnetic energy or both, the use of which enables communications to be carried over a telecommunications system operated by a carrier but not being a service for carrying communications solely by means of radio communication.

[39] Bill C-74. This Bill was introduced in the House of Commons by the Minister of Public Safety and Emergency Preparedness on 15 November 2005. The Bill refers to specific aspects of the rules governing lawful access, an investigative technique used by law enforcement agencies and national security agencies. The Bill was aimed at protecting victims against new technologies such as wireless data networks and voice over Internet protocol, which often present obstacles to the lawful interception of communications. Since such technologies can create "intercept safe havens" where criminal groups are able to operate without being detected, and in light of factors such as the deregulation of the telecommunications market, the Bill was intended to respond to the growing complexity of telephone networks that makes investigators' work more difficult and may result in delays in identifying suspects.

[40] An agent of the State is defined as a peace officer, and a person acting under the authority of, or in cooperation with, a peace officer.

to the person who consented to the interception and the purpose of the interception is to prevent such bodily harm. The provision goes on to require the agent of the State who intercepts a private communication to, as soon as practicable in the circumstances, destroy any recording of the private communication obtained during an interception, any full or partial transcript of the recording and any corresponding notes, if nothing in the private communication suggests that bodily harm, attempted bodily harm or threatened bodily harm has occurred or is likely to occur. Further, Section 287(1)(b) provides that anyone commits theft who fraudulently, maliciously, or without colour of right uses any telecommunications facility or obtains any telecommunications service.[41]

In the United Kingdom, the 2000 *Regulation of Investigatory Powers Act* was a legislative attempt by Parliament to unify in a single legal framework provisions countering the interception of information and communications. This Act does not discriminate between types of communications or the location at which communications are intercepted. Section 1.1. of the Act states that it is an offence to intercept, intentionally and without lawful authority, at any place in the United Kingdom, any communication in the course of its transmission by means of a public postal service or a public telecommunications system. Further, the Act prescribes it an offence to intercept, intentionally and without lawful authority, at any location in the United Kingdom, any communication while it is being transmitted via a public or private telecommunications system. Significantly, Section 4.1 deems conduct by an interceptor lawful if the interception of a communication in the course of its transmission by means of a telecommunications system constitutes interception carried out for the purpose of obtaining information about the communications of a person who is, or whom the interceptor has reasonable grounds for believing may be, in a State or territory outside of the United Kingdom. Such interception would relate to the use of a telecommunications service provided to persons in that State or territory, which is either a public telecommunications service or a telecommunications service that would be a public service if the persons to whom it was offered or provided were members of the public in a part of the United Kingdom.

In the United States, surveillance laws against interception were not fully defined until they were reformed in the 1986 *Electronic Communications Privacy Act*, adopted prior to the widespread introduction of the Internet and World Wide Web. Courts have referred to such laws as convoluted,[42] confusing and uncertain. In the decision of *Konop* v *Hawaiian Airlines*,[43] handed down by the United States Court of Appeal 9th Circuit in 2002, the court noted inter alia that the Act defines "electronic communication" as a "transfer" of signals, and that "unlike the definition of 'wire communication,' the definition of 'electronic communication' does

[41] Section 287 defines telecommunication as "any transmission, emission or reception of signs, signals, writing, images, sounds or intelligence of any nature by radio, visual, electronic or other electromagnetic system".

[42] *US*. v. *Smith* 155 F 3d 1051, at 1055 (9th Cir. 1998).

[43] 302 F 3d 868.

not include electronic storage of such communications", which led the Court to conclude that the Act was not equipped to handle modern forms of electronic communication.[44]

A particular feature of cyber terrorism is that the threat is enhanced by globalization and the ubiquity of the Internet. Given such a global problem, requiring a global solution, the one forum that can provide a global framework against cyber terrorism is the International Civil Aviation Organization (ICAO). A sustained global process of security risk assessment[45] is the first necessary step.

At the 21st Meeting of the ICAO Aviation Security Panel, conducted in Montréal, from 22 to 26 March 2010, a new Recommended Practice related to cyber threats was proposed for adoption by the Council as part of Amendment 12 to Annex 17 – *Security* to the *Convention on International Civil Aviation* (Chicago Convention). This Amendment was adopted on 17 November 2010, and will become effective on 26 March 2011 and applicable on 1 July 2011. The new Recommended Practice suggests that each Contracting State 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. The 22nd Meeting of the ICAO Aviation Security Panel, held in Montréal from 21 to 25 March 2011, noted the value of vulnerability assessments pertaining to cyber security in aviation, whose objectives are to evaluate the efficiency of existing mitigation measures and identify any vulnerabilities from a threat-based perspective. The Panel further noted that better understanding of residual risks will support a State's efforts to refine its risk response.

In pursuance of these objectives, ICAO, in collaboration with its Member States, could undertake a study to identify critical aviation information systems; review the effectiveness of existing mitigation measures established for such systems; identify any vulnerabilities in current security arrangements; analyse best practices on how to address these vulnerabilities; and determine how to better manage identified residual risks.

3.2 Attacks on the Integrity of Travel Documents

A passport is the property of the State which issues it. As such no State or other legal entity has a right to alter an existing passport of a holder or forge false documentation purporting to have been issued by a State. The fundamental issue

[44] *Id.*, 461.

[45] One definition of security risk assessment considered by the ICAO Aviation Security Panel at its Twenty-second Meeting: "an outcome based process, coordinated by the Appropriate Authority utilising all appropriate resources, consisting of an analysis of prevailing threat factors compared against current mitigation measures, with a view to determining levels of risk that result in the application of appropriate mitigation measures".

therefore, is whether a State or instrumentality of that State can use a forged passport with impunity, particularly in the course of criminal activity. On 19 January 2010, Mahmoud al-Mabhouh, considered to be a senior commander of Hamas, a radical Palestinian group, was assassinated at a hotel in Dubai in a manner usually employed by professionally trained military and secret service agencies. The killing was attributed to Mossad, the Israeli secret service. Quite apart from the criminality of the assassination, the issue of the use of forged passport was brought to bear by some countries which alleged that the perpetrators of the crime had allegedly forged passports that seemingly belonged to those countries. This international incident sparked off a legal and diplomatic discussion in the media as to the responsibility and liability of States – which condone or allow the use of these forged documents – towards those States that are affected.

The passport is a basic document in the transport by air of persons. Its use therefore is of fundamental importance as a travel document, not only because it reflects the importance of the sovereignty of a State and the nationality of its citizens but also because it stands for the inviolability of relations between States that are linked through air transport. The assassination of a leader of Hamas on 19 January 2010 by a group of individuals in Dubai who used forged passports belonging to various nations, raised a diplomatic outcry and brought to bear an important facet of air transport that is vulnerable to abuse and contention among States.

The fundamental issue that emerges is one that is critical to air law in the context of the integrity and ownership of the passport and its abuse in the course of criminal activity. There is also the issue, from a legal and diplomatic perspective as to whether a State or instrumentality of State, can, with impunity, use forged passports for travel of its staff on missions of espionage or assassination. A fortiori, an additional issue is whether a State could be complicit or condone or be seen to condone (in the absence of any action taken by the State to punish the miscreants) such abuse of travel documents belonging to other nations. In order to determine these issues, this article addresses two basic discussions: the first on complicity and condonation of a State and the second on the nature and integrity of the passport. Finally, it discusses issues of State responsibility, diplomacy and criminality.

On 19 January 2010, Mahmoud al-Mabhouh, considered to be a senior commander of Hamas, a radical Palestinian group, was assassinated at a hotel in Dubai in a manner usually employed by professionally trained military and secret service agencies. The killing was attributed to Mossad[46] The European Union, which considers Hamas a terrorist organization, nonetheless condemned the assassination of the Hamas leader and showed particular concern over the fact that the killers had used passports from Ireland, France, Germany and the UK – to coordinate their travel into Dubai from various parts of the world, synchronizing their arrival time

[46] Mossad is responsible for the collection of intelligence and other covert activities including military operations. It is one of the most integral parts of the Israeli intelligence community and reports directly to the Prime Minister of Israel. See http://en.wikipedia.org/wiki/Mossad.

from various flights into Dubai International Airport and checking into the hotel of the victim contemporaneously. The EU strongly condemned the fact that those involved in this action used fraudulent EU member states' passports and credit cards acquired through the theft of EU citizens' identities.[47]

Australia was another complainant who warned Israel that its friendly relations with Israel would be jeopardised if it were found to have condoned the suspected theft of three Australian citizens' identities which Mossad used to carry out its political assassination. The diplomatic impasse occurred when three Australians from Victoria living in Israel at the time were confirmed among 26 people from four nations whose tampered passports were allegedly used by a team of suspected Israeli Mossad agents who assassinated al-Mabhouh. Australian Prime Minister Kevin Rudd is reported to have stated that Australia would be vocal in its contempt of any State if it were found that it "... has been complicit in the use or abuse of the Australian passport system, let alone for the conduct of an assassination, and has treated Australia with contempt and there will therefore be action by the Australian government in response".[48] Dubai authorities are reported to have said that they were virtually certain Israeli agents carried out the killing and had released the identities of 11 people who travelled on forged British, Irish, French and German passports to kill al-Mabhouh in a hotel.[49]

There is seemingly a history behind alleged Mossad involvement in the use of fake foreign passports in its activities. Reportedly, in 2004 New Zealand's prime minister imposed diplomatic sanctions – restricting visas and cancelling high level visits – after two Mossad agents were caught trying to acquire passports fraudulently – one in the name of a tetraplegic man. Seven years earlier, Mossad assassins carrying Canadian passports with assumed names attempted to murder the Hamas leader Khaled Meshaal by spraying nerve agent into his ear as he entered his office in Amman.[50]

---

[47] Toby Vogel, EU Condemns Use of False Passports inn Hamas Killing, http://www.europeanvoice.com/article/2010/02/eu-condemns-use-of-false-passports-in-hamas-killing/67225.aspx.

[48] http://www.theaustralian.com.au/news/world/australians-caught-in-hit-on-hamas/story-e6frg6so-1225834538825 It is reported that in 1997, Mossad bungled the assassination of top Hamas leader Khalid Mishal, who was injected while in Jordan with a poison by Israeli agents travelling on Canadian documents. He survived after his assailants were captured by his bodyguards and Israel provided the antidote. In 2004, two Mossad agents were jailed in New Zealand after trying to obtain fake passports, one in the name of a cerebral palsy sufferer. *Ibid*.

[49] http://www.euractiv.com/en/foreign-affairs/eu-unhappy-israel-over-fake-passports-james-bond-killings-news-278602.

[50] David Sapsted, and Loveday Morris, Israel in the Dock Over Fake Passports, http://www.thenational.ae/apps/pbcs.dll/article?AID=/20100218/NATIONAL/702179796/1133/sport.
Hamas, which won 2006 legislative elections in the Palestinian territories, is shunned by the West for rejecting its calls to recognise Israel and renounce violence. Hit squads dispatched by Mossad have used foreign passports in the past, notably in 1997 when agents entered Jordan on Canadian passports and bungled an attempt to kill Meshaal with poison. In 1987, Britain protested to Israel about what London called the misuse by Israeli authorities of forged British passports and said it

The fundamental issue that emerges is one that is critical to air law in the context of the integrity and ownership of the passport and its abuse in criminal activity. There is also the issue, from a legal and diplomatic perspective is whether a State or instrumentality of State such as Mossad, can, with impunity, use forged passports for travel of its staff on missions of espionage or assassination. A fortiori, an additional issue is whether a State could be complicit or condone or be seen to condone (in the absence of any action taken by the State to punish the miscreants) such abuse of travel documents belonging to other nations.

3.2.1 Complicity

The fundamental issue in the context of State responsibility for the purposes of this article is to consider whether a State should be considered responsible for its own failure or non-feasance to prevent a private act that is a violation of its international responsibility towards a third State or whether the conduct of the State itself can be impugned by identifying a nexus between the perpetrator's conduct and the State. One view is that an agency paradigm, which may in some circumstances impute to a state reprehensibility on the ground that a principal–agent relationship between the State and the perpetrator existed, can obfuscate the issue and preclude one from conducting a meaningful legal study of the State's conduct.[51]

At the core of the principal–agent dilemma is the theory of complicity, which attributes liability to a State that was complicit in a private act. Hugo Grotius (1583–1645), founder of the modern natural law theory, first formulated this theory based on State responsibility that was not absolute. Grotius' theory was that although a State did not have absolute responsibility for a private offence, it could be considered complicit through the notion of *patienta* or *receptus*.[52] While the concept of *patienta* refers to a State's inability to prevent a wrongdoing, *receptus* pertains to the refusal to punish the offender.

The eighteenth Century philosopher Emerich de Vattel was of similar view as Grotius, holding that responsibility could only be attributed to the State if a sovereign refuses to repair the evil done by its subjects or punish an offender or deliver him to justice whether by subjecting him to local justice or by extraditing him.[53] This view was to be followed and extended by the British jurist Blackstone a

received assurances steps had been taken to prevent future occurrences. In 2003, the offices of several EU member countries in the Council's Justus Lipsius building, including France, Germany and the UK, were found to be bugged. Although the Union has been discrete over the incident, many consider Mossad to have been responsible for the wiretapping. *Ibid.*

[51] Caron (1998) cited in Becker (2006a).

[52] Grotius and Scott (1646).

[53] De Vattel and Fenwick (1916).

few years later who went on to say that a sovereign who failed to punish an offender could be considered as abetting the offence or of being an accomplice.[54]

A different view was put forward in an instance of adjudication involving a seminal instance where the Theory of Complicity and the responsibility of states for private acts of violence was tested in 1925. The case[55] involved the Mexico-United States General Claims Commission which considered the claim of the United States on behalf of the family of a United States national who was killed in a Mexican mining company where the deceased was working. The United States argued that the Mexican authorities had failed to exercise due care and diligence in apprehending and prosecuting the offender. The decision handed down by the Commission distinguished between complicity and the responsibility to punish and the Commission was of the view that Mexico could not be considered an accomplice in this case.

The Complicity Theory, particularly from a Vattellian and Blackstonian point of view is merely assumptive unless put to the test through a judicial process of extradition. In this Context it becomes relevant to address the issue through a discussion of the remedy.

3.2.2 Condonation

The emergence of the Condonation Theory was almost concurrent with the *Jane* case[56] decided in 1925 which emerged through the opinions of scholars who belonged to a school of thought that believed that States became responsible for private acts of violence not through complicity as such but more so because their refusal or failure to bring offenders to justice, which was tantamount to ratification of the acts in question or their condonation.[57] The theory was based on the fact that it is not illogical or arbitrary to suggest that a State must be held liable for its failure to take appropriate steps to punish persons who cause injury or harm to others for the reason that such States can be considered guilty of condoning the criminal acts and therefore become responsible for them.[58] Another reason attributed by scholars in support of the theory is that during that time, arbitral tribunals were ordering States to award pecuniary damages to claimants harmed by private offenders, on the basis that the States were being considered responsible for the offences.[59]

---

[54] Blackstone and Morrison (2001).

[55] *Laura M.B. Janes (USA)* v. *United Mexican States* (1925) 4 R Intl Arb Awards 82.

[56] *Ibid.*

[57] *Black's Law Dictionary* defines condonation as "pardon of offense, voluntary overlooking implied forgiveness by treating offender as if offense had not been committed."

[58] Jane's case, *Supra*, note 11, at 92.

[59] Hyde (1928).

The responsibility of governments in acting against offences committed by private individuals may sometimes involve condonation or ineptitude in taking effective action against terrorist acts, in particular with regard to the financing of terrorist acts. The United Nations General Assembly, on 9 December 1999, adopted the International Convention for the Suppression of the Financing of Terrorism,[60] aimed at enhancing international co-operation among States in devising and adopting effective measures for the prevention of the financing of terrorism, as well as for its suppression through the prosecution and punishment of its perpetrators.

The Convention, in its Article 2 recognizes that any person who by any means directly or indirectly, unlawfully or willfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out any act which constitutes an offence under certain named treaties, commits an offence. One of the treaties cited by the Convention is the International Convention for the Suppression of Terrorist Bombings, adopted by the General Assembly of the United Nations on 15 December 1997.[61]

The Convention for the Suppression of the Financing of Terrorism also provides that, over and above the acts mentioned, providing or collecting funds toward any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in the situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act, would be deemed an offence under the Convention.

The United Nations has given effect to this principle in 1970 when it proclaimed that:

> Every State has the duty to refrain from organizing or encouraging the organization of irregular forces or armed bands, including mercenaries, for incursion into the territory of another State. Every State has the duty to refrain from organizing, instigating, assisting or participating in acts of civil strife or terrorist acts in another State or acquiescing in organized activities within its territory directed towards the commission of such acts, when the acts referred to in the present paragraph involve a threat or use of force.[62]

Here, the words *encouraging* and *acquiescing in organized activities within its territory directed towards the commission of such acts* have a direct bearing on the concept of condonation and would call for a discussion about how States could

[60] International Convention for the Suppression of the Financing of Terrorism, adopted by the General Assembly of the United Nations in resolution 54/109 of 9 December 1999.

[61] A/52/653, 25 November 1997.

[62] Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations, UN General Assembly Resolution 2625 (XXV) 24 October 1970.

overtly or covertly encourage the commission of such acts. One commentator[63] identifies three categories of such support: *Category I* support entails protection, logistics, training, intelligence, or equipment provided terrorists as a part of national policy or strategy; *Category II* support is not backing terrorism as an element of national policy but is the toleration of it; *Category III* support provides some terrorists a hospitable environment, growing from the presence of legal protections on privacy and freedom of movement, limits on internal surveillance and security organizations, well-developed infrastructure, and émigré communities.

Another commentator[64] discusses what he calls the '*separate delict theory*' in State responsibility, whereby the only direct responsibility of the State is when it is responsible for its own wrongful conduct in the context of private acts, and not for the private acts themselves. He also contends that indirect State responsibility is occasioned by the State's own wrongdoing in reference to the private terrorist conduct. The State is not held responsible for the act of terrorism itself, but rather for its failure to prevent and/or punish such acts, or for its active support for or acquiescence in terrorism.[65] Arguably the most provocative and plausible feature in this approach is the introduction by the commentator of the desirability of determining State liability on the theory of causation. He emphasizes that:

> The principal benefit of the causality based approach is that it avoids the automatic rejection of direct State responsibility merely because of the absence of an agency relationship. As a result, it potentially exposes the wrongdoing State to a greater range and intensity of remedies, as well as a higher degree of international attention and opprobrium for its contribution to the private terrorist activity.[66]

The causality principle is tied in with the rules of State Responsibility enunciated by the International Law Commission and Article 51 of the United Nations Charter which states that nothing in the Charter will impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. The provision goes on to say that measures taken by Members in the exercise of this right of self-defense will be immediately reported to the Security Council and will not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.

The International Law Commission has established that a crime against the peace and security of mankind entails individual responsibility, and is a crime of

[63] Steven Metz, State Support for Terrorism, Defeating Terrorism, Strategic Issue Analysis, at http://www.911investigations.net/IMG/pdf/doc-140.pdf.

[64] Becker (2006b).

[65] *Id.* Chapter 2, 67.

[66] Becker, *supra*, note 64 at 335.

aggression.[67] A further link drawing civil aviation to the realm of international peace and security lies in the Rome Statute of the International Criminal court, which defines a war crime, inter alia, as intentionally directing attacks against civilian objects; attacking or bombarding, by whatever means, towns, villages, dwellings or buildings which are undefended and which are not military objects; employing weapons, projectiles, and material and methods of warfare that cause injury.[68] The Statute also defines as a war crime, any act which is intentionally directed at buildings, material, medical units and transport, and personnel using the distinctive emblems of the Geneva Conventions in conformity with international law.[69]

3.2.3 Knowledge

Another method of determining State responsibility lies in the determination whether a State had actual or presumed knowledge of acts of its instrumentalities, agents or private parties which could have alerted the State to take preventive action. International responsibility of a State cannot be denied merely on the strength of the claim of that State to sovereignty. Although the Chicago Convention in Article 1 stipulates that the contracting States recognize that every State has complete and exclusive sovereignty over the airspace above its territory, the effect of this provision cannot be extended to apply to State immunity from responsibility to other States. Professor Huber in the *Island of Palmas* case[70] was of the view:

> Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State. . .Territorial sovereignty. . .involves the exclusive right to display the activities of a State.[71]

Professor Huber's definition, which is a simple statement of a State's rights, has been qualified by Starke as the residuum of power which a State possesses within the confines of international law.[72] Responsibility would devolve upon a State in whose territory an act of unlawful interference against civil aviation might occur, to other States that are threatened by such acts. The International Court of Justice (ICJ) recognised in the *Corfu Channel* Case:

---

[67] Draft Code of Crimes Against the Peace and Security of Mankind, International Law Commission Report, 1996, Chapter II Article 2.

[68] Rome Statute of the International Criminal Court, Article 8.2 (b) (ii), (V) and (XX).

[69] Id. Article 8.2 (b) (XXIV).

[70] The *Island of Palmas* Case (1928) 11 U.N.R. I.A.A. at 829.

[71] Ibid.

[72] Starke (1989).

> every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States.[73]

In the famous *Corfu Channel* case, the International Court of Justice applied the subjective test and applied the fault theory. The Court was of the view that:

> It cannot be concluded from the mere fact of the control exercised by a State over its territory and waters that the State necessarily knew, or ought to have known, of any unlawful act perpetrated therein, nor yet that it necessarily knew, or should have known the authors. This fact, by itself and apart from other circumstances, neither involves prima facie responsibility nor shifts the burden of proof.[74]

The Court, however, pointed out that exclusive control of its territory by a State had a bearing upon the methods of proof available to establish the involvement or knowledge of that State as to the events in question.

Apart from the direct attribution of responsibility to a State, particularly in instances where a State might be guilty of a breach of treaty provisions, or violate the territorial sovereignty of another State, there are instances where an act could be imputed to a State.[75] Imputability or attribution depends upon the link that exists between the State and the legal person or persons actually responsible for the act in question. The legal possibility of imposing liability upon a State wherever an official could be linked to that State encourages a State to be more cautious of its responsibility in controlling those responsible for carrying out tasks for which the State could be ultimately held responsible. In the same context, the responsibility of placing mines was attributed to Albania in the *Corfu Channel* case where the court attributed to Albania the responsibility, since Albania was known to have knowledge of the placement of mines although it did not know who exactly carried out the act. It is arguable that, in view of the responsibility imposed upon a State by the Chicago Convention on the provision of air navigation services, the principles of immutability in State responsibility could be applied to an instance of an act or omission of a public or private official providing air navigation services.

The sense of international responsibility that the United Nations ascribed to itself had reached a heady stage at this point, where the role of international law in

---

[73] (1949) *I.C.J.R.*1, 22.

[74] The *Corfu Channel* Case, ICJ Reports, 1949, p. 4.

[75] There are some examples of imputability, for example the incident in 1955 when an Israeli civil aircraft belonging to the national carrier El Al was shot down by Bulgarian fighter planes, and the consequent acceptance of liability by the USSR for death and injury caused which resulted in the payment of compensation to the victims and their families. See 91 *ILR* 287. Another example concerns the finding of the International Court of Justice that responsibility could have been be imputed to the United States in the *Nicaragua* case, where mines were laid in Nicaraguan waters and attacks were perpetrated on Nicaraguan ports, oil installations and a naval base by persons identified as agents of the United States. See *Nicaragua* v. *the United States*, ICJ Reports 1986, 14. Also, 76 *ILR* 349. There was also the instance when the Secretary General of the United Nations mediated a settlement in which a sum of $ 7 million was awarded to New Zealand for the violation of its sovereignty when a New Zealand vessel was destroyed by French agents in New Zealand. See the *Rainbow Warrior* case, 81 *AJIL*, 1987 at 325. Als in 74 *ILR* at 241.

international human conduct was perceived to be primary and above the authority of States. In its Report to the General Assembly, the International Law Commission recommended a draft provision which required:

> Every State has the duty to conduct its relations with other States in accordance with international law and with the principle that the sovereignty of each State is subject to the supremacy of international law.[76]

This principle, which forms a cornerstone of international conduct by States, provides the basis for strengthening international comity and regulating the conduct of States both internally – within their territories – and externally, towards other States. States are effectively precluded by this principle of pursuing their own interests untrammelled and with disregard to principles established by international law.

The United Nations General Assembly, in its Resolution 56/83,[77] adopted as its Annex the International Law Commission's *Responsibility of States for Internationally Wrongful Acts* which recognizes that every internationally wrongful act of a State entails the international responsibility of that State[78] and that there is an internationally wrongful act of a State when conduct consisting of an action or omission is attributable to the State under international law and constitutes a breach of an international obligation of the State.[79] Article 5 of the ILC document provides that the conduct of a person or entity which is not an organ of State but which is empowered by the law of that State to exercise elements of the governmental authority shall be considered an act of State under international law, provided the person or entity is acting in that capacity in the particular instance.

In the *Pan Am* case,[80] where an aircraft was destroyed over Lockerbie the British allegation against Libya's involvement in the act of terrorism was that the accused individuals (Libyan nationals) had acted as part of a conspiracy to further the purposes of the Libyan Intelligence Services using criminal means that amounted to terrorism. The United Kingdom appeared to stress the point in the UN Security Council that Libya had failed to respond to the request for extradition of the implicated Libyan nationals, and arguably as a consequence, the Security Council adopted Resolution 731 on 21 January 1992 which expressed concerns over certain investigations which imputed reprehensibility to officials of the Libyan Government.[81]

ICAO has been working on the development of passports since 1968. The Seventh Session of the ICAO Facilitation Division in 1968 recommended that a

[76] Report of the International Law Commission to the General Assembly on the Work of the 1st Session, A/CN.4/13, June 9 1949, at 21.

[77] A/RES/56/83 56th Session, 28 January 2002

[78] *Id.* Article 1

[79] Id. Article 2.

[80] *Infra*, note 130.

[81] For a discussion on this point see Jorgensen (2000).

small panel of qualified experts including representatives of the passports and/or other border control authorities, be established: to determine the establishment of an appropriate document such as a passport card, a normal passport or an identity document with electronically or mechanically readable inscriptions that meet the requirements of document control; the best type of procedures, systems (electronic or mechanical) and equipment for use with the above documents that are within the resources and ability of Member States; the feasibility of standardizing the requisite control information and methods of providing this information through automated processes, provided that these processes would meet the requirements of security, speed of handling and economy of operation.[82]

A passport asserts that the person holding the passport is a citizen of the issuing State while a visa confirms that the State issuing the visa has granted the visa holder the non-citizen privilege of entering and remaining in the territory of the issuing State for a specified time and purpose. An ePassport is a type of Machine Readable Passport (MRP)[83] with an embedded microchip that contains data printed on the data page of the passport, including biographic and biometric information of the holder, and passport data. The chip also contains security features for preventing passport fraud and forgery and misuse of data stored on the chip. ePassports are easily recognised by the international ePassport symbol on the front cover.[84]

The techniques of biometrics employed in a machine readable travel document (MRTD), be it a visa or passport,[85] enable the user to uniquely encode a particular physical characteristic of a person into a biometric identifier or biometric template which can be verified by machine to confirm or deny a claim regarding a person's identity. Accordingly, biometric identification of a person either correctly establishes his identity as being consistent with what is claimed in the passport he is holding or brings to bear the possibility that the person carrying a particular passport is an imposter. A biometric is a measurable, physical characteristic or

[82] See Facilitation Division, Report of the Seventh Session, 14–30 May 1968, ICAO Doc 8750-FAL/564, Agenda Item 2.3, at 2.3-4. See also *AT-WP/1079, 1/12/70*, Attachment A, which sets out the Terms of Reference of the Panel.

[83] The machine readable passport (MRP) is a passport that has both a machine readable zone and a visual zone in the page that has descriptive details of the owner. The machine readable zone enables rapid machine clearance, quick verification and instantaneous recording of personal data. Besides these advantages, the MRP also has decided security benefits, such as the possibility of matching very quickly the identity of the MRP owner against the identities of undesirable persons, whilst at the same time offering strong safeguards against alteration, counterfeit or forgery. See Abeyratne (1992).

[84] http://www.dhs.gov/xtrvlsec/programs/content_multi_image_0021.shtm.

[85] The machine readable passport (MRP) is a passport that has both a machine readable zone and a visual zone in the page that has descriptive details of the owner. The machine readable zone enables rapid machine clearance, quick verification and instantaneous recording of personal data. Besides these advantages, the MRP also has decided security benefits, such as the possibility of matching very quickly the identity of the MRP owner against the identities of undesirable persons, whilst at the same time offering strong safeguards against alteration, counterfeit or forgery (Abeyratne 1992).

personal behavioral trait used to recognize the identity, or verify[86] the claimed identity of a person. In the modern context, biometrics are usually incorporated in an MRTD with a view to achieving five goals, the first of which is global interoperability[87] enabling the specifications of biometrics deployed in travel documents across the world to be applied and used in a universally operable manner. This is a critical need if the smooth application of biometric technology were to be ensured across borders. The second goal is to ensure uniformity within States in specific standard setting by States authorities who deploy biometrics in travel documents issued by them. The third is technical reliability, where States are required to ensure that technologies used in deploying biometrics are largely failure-proof and of sufficient quality and standard to ensure a State immigration authority reading documents issued by other States can determine that the details in the document do provide accurate verification of facts. Fourthly, the technology used has to be practical and not give rise to the need for applying disparate types of support technology at unnecessary cost and inconvenience to the user. The final goal is to ensure that the technology used will be sufficiently up to date for at least 10 years and also be backwardly compatible with new techniques to be introduced in the future.

Biometrics target the distinguishing physiological or behavioral traits of the individual by measuring them and placing them in an automated repository such as machine encoded representations created by computer software algorithms that could make comparisons with the actual features. Physiological biometrics that have been found to successfully accommodate this scientific process are facial recognition, fingerprinting and iris-recognition which have been selected by ICAO as being the most appropriate. The biometric identification process is fourfold: firstly involving the capture or acquisition of the biometric sample; secondly extracting or converting the raw biometric sample obtained into an intermediate form; and thirdly creating templates of the intermediate data that is converted into a template for storage; and finally the comparison stage where the information offered by the travel document is compared with that which is stored in the reference template.

Biometric identification gets into gear each time an MRTD holder (traveler) enters or exists the territory[88] of a State and when the State verifies his identity

[86] To "verify" means to perform a one-to-one match between proffered biometric data obtained from the holder of the travel document at the time of inquiry with the details of a biometric template created when the holder enrolled in the system.

[87] "Global interoperability" means the capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective states. Global interoperability is a major objective of the standardized specifications for placement of both eye-readable and machine-readable data in all MRTDs.

[88] The Chicago Convention, *supra*, note3, defines, in Article 2, "territory of a State" as the land areas and territorial waters adjacent to the State under the sovereignty, suzerainty, protection and mandate of such State.

against the images or templates created at the time his travel document was issued. This measure not only ensures that the holder of the document is the legitimate claimant to that document and to whom it was issued, but also enhances the efficacy of any advance passenger information (API)[89] system used by the State to predetermine the arrivals to its territory. Furthermore, matching biometric data presented in the form of the traveler with the data contained in the template accurately ascertains as to whether the travel document has been tampered with or not. A three way check, which matches the traveler's biometrics with those stored in the template carried in the document and a central database, is an even more efficacious way of determining the genuineness of a travel document. The final and most efficient biometric check is when a four way determine is effected, were the digitized photograph is visually matched (non electronically) with the three way check described above.[90] In this context, it is always recommended that the traveler's facial image (conventional photograph) should be incorporated in the travel document along with the biometric templates in order to ensure that his identity could be verified at locations where there is no direct access to a central database or where the biometric identification process has not entered into the legal process of that location.

3.2.4 Security of the Passport

Production of passport books and travel documents, including the personalization processes, should be undertaken in a secure, controlled environment with appropriate security measures in place to protect the premises against unauthorized access. If the personalization process is decentralized, or if personalization is carried out in a location geographically separated from where the travel document blanks are made, appropriate precautions should be taken when transporting the blank

[89] API involves exchange of data information between airlines and customs authorities, where an incoming passenger's essential details are notified electronically by the airline carrying that passenger prior to his arrival. The data for API would be stored in the passenger's machine readable passport, in its machine readable zone. This process enables customs authorities to process passengers quickly, thus ensuring a smoother and faster clearance at the customs barriers at airports. One of the drawbacks of this system, which generally works well and has proven to be effective, is that it is quite demanding in terms of the high level of accuracy required. One of the major advantages, on the other hand, is the potential carried by the API process in enhancing aviation security at airports and during flight. See Abeyratne (2002a).

[90] Issuing States must ensure the accuracy of the biometric matching technology used and functions of the systems employed if the integrity of the conducted checks are to be maintained. They must also have realistic and efficient criteria regarding the number of travel documents checked per minute in a border control situation and follow a regular biometric identification approach such as facial recognition, fingerprint examination or iris identification system.

documents and any associated security materials to safeguard their security in transit.

There should be full accountability over all the security materials used in the production of good and spoiled travel documents and a full reconciliation at each stage of the production process with records maintained to account for all material usage. The audit trail should be to a sufficient level of detail to account for every unit of material used in the production and should be independently audited by persons who are not directly involved in the production. Certified records should be kept of the destruction of all security waste material and spoiled documents.

Materials used in the production of travel documents should be of controlled varieties and obtained only from bona fide security materials suppliers. Materials whose use is restricted to high security applications should be used, and materials that are available to the public on the open market should be avoided.

Sole dependence upon the use of publicly available graphics design software packages for originating the security backgrounds should be avoided. These software packages may however be used in conjunction with specialist security design software.

Security features and/or techniques should be included in travel documents to protect against unauthorized reproduction, alteration and other forms of tampering, including the removal and substitution of pages in the passport book, especially the biographical data page. In addition to those features included to protect blank documents from counterfeiting and forgery, special attention must be given to protect the biographical data from removal or alteration. A travel document should include adequate security features and/or techniques to make evident any attempt to tamper with it.

The combination of security features, materials and techniques must be well chosen to ensure full compatibility and protection for the lifetime of the document. There is another class of security features comprised of covert (secret) features, designed to be authenticated either by forensic examination or by specialist verification equipment. It is evident that knowledge of the precise substance and structure of such features should be restricted to very few people on a "need to know" basis. The purpose of these features is not to prevent counterfeiting but to enable authentication of documents where unequivocal proof of authenticity is a requirement (e.g. in a court of law). All travel documents should contain at least one covert security feature as a basic feature.

3.2.4.1 Threats to the Security of Passports

There are many threats to the security of passports such as: counterfeiting a complete travel document; photo-substitution; deletion/alteration of text in the visual or machine readable zone of the MRP data page; construction of a fraudulent document, or parts thereof, using materials from legitimate documents; removal and substitution of entire page(s) or visas; deletion of entries on visa pages and the

observations page; theft of genuine document blanks; and impostors (assumed identity; altered appearance).

To provide protection against these threats and others, a travel document requires a range of security features and techniques combined in an appropriate way within the document. Although some features can offer protection against more than one type of threat, no single feature can offer protection against them all. Likewise, no security feature is 100% effective in eliminating any one category of threat. The best protection is obtained from a balanced set of features and techniques providing multiple layers of security in the document that combine to deter or defeat fraudulent attack.[91]

Annex 9[92] to the Convention on International Civil Aviation, in Standard 3.7 requires ICAO member States to regularly update security features in new versions of their travel documents, to guard against their misuse and to facilitate detection of cases where such documents have been unlawfully altered, replicated or issued. Recommended Practice 3.9 suggests that member States incorporate biometric data in their machine readable passports, visas and other official travel documents, using one or more optional data storage technologies to supplement the machine readable zone, as specified in Doc 9303, Machine Readable Travel Documents. The required data stored on the integrated circuit chip is the same as that printed on the data page, that is, the data contained in the machine-readable zone plus the digitized photographic image. Fingerprint image(s) and/or iris image(s) are optional biometrics for member States wishing to supplement the facial image with another biometric in the passport. Member States incorporating biometric data in their Machine Readable Passports are to store the data in a contactless integrated circuit chip complying with ISO/IEC 14443 and programmed according to the Logical Data Structure as specified by ICAO.

3.2.4.2 The Diplomatic Fallout

Any diplomatic action in the context of the issues raised in this article must primarily be based on State responsibility. In turn, and as already discussed, the issue of responsibility hinges on knowledge, complicity and condonation of a State. The responsibility of a State is determined by the quantum of proof available that could establish intent or negligence of the State, which in turn would establish complicity or condonation on the part of the State concerned. One way to determine complicity or condonation is to establish the extent to which the State adhered to the obligation imposed upon it by international law and whether it breached its duty to others. In order to exculpate itself, the State concerned will have to demonstrate that either it did not tolerate the offence or that it ensured the punishment of the

[91] Machine Readable Travel Documents, ICAO Doc 9303 Part 1, Machine Readable Passports, Sixth Edition, 2006, III-4.

[92] Annex 9 to the Convention on International Civil Aviation, 12th Edition, 2006.

offender. *Brownlie* is of the view that proof of such breach would lie in the causal connection between the offender and the State.[93] In this context, the act or omission on the part of a State is a critical determinant particularly if there is no specific intent.[94] Generally, it is not the intent of the offender that is the determinant but the failure of a State to perform its legal duty in either preventing the offence (if such was within the purview of the State) or in taking necessary action with regard to punitive action or redress.[95]

There are a few principles that have to be taken into account when determining State responsibility. Firstly, there has to be either intent on the part of the State towards complicit or negligence reflected by act or omission. Secondly, where condonation is concerned, there has to be evidence of inaction on the part of the State in prosecuting the offender. Thirdly, since the State as an abstract entity cannot perform an act in itself, the imputability or attribution of State responsibility for acts of its agents has to be established through a causal nexus that points the finger at the State as being responsible. For example, The International Law Commission, in Article 4 of its Articles of State Responsibility states that the conduct of any State organ which exercises judicial, legislative or executive functions could be considered an act of State and as such the acts of such organ or instrumentality can be construed as being imputable to the State. This principle was endorsed in 1999 by the ICJ which said that according to well established principles of international law, the conduct of any organ of a state must be regarded as an act of State.[96]

The law of State responsibility has evolved through the years, from being a straightforward determination of liability of the State and its agents to a rapidly widening gap between the State and non State parties. In today's world private entities and persons could wield power similar to that of a State, bringing to bear the compelling significance and modern relevance of the agency nexus between the State and such parties. This must indeed make States more aware of their own susceptibility.

The United Nations General Assembly, in 2002 adopted Resolution A 56/83[97] on the subject of Responsibility of States for internationally wrongful acts. The Resolution, which was the result of work of the International Law Commission on the subject, provides that every internationally wrongful act of a State entails the international responsibility of that State[98] and that such an act is attributable to that State under international law and constitutes a breach of an international obligation of that State. Article 5 to the Annex to the Resolution states that the conduct of a

[93] Brownlie (1983).

[94] Report of the International Law Commission to the United Nations General Assembly, UNGOAR 56th Session, Supp. No. 10, *UN DOC A/56/10*, 2001 at 73.

[95] de Arechaga (1968).

[96] Differences Relating to Immunity from Legal Process of a Special Rapporteur, ICJ Reports 1999, 62 at 87.

[97] A/RES/56/83 Fifty sixty Session 28 January 2002.

[98] *Id.* Annex, Article 1.

person or entity which is not an organ of a State but which is empowered by the law of that State to exercise elements of the governmental authority shall be considered an act of the State under international law, provided the person or entity is acting in that capacity in the particular instance. If, as alleged, the assassination of Mahmoud al-Mabhouh was carried out by Mossad, which reports to the Isreali Prime Minister, Article 8 of the Annex to the Resolution is particularly relevant as it provides that the conduct of a person or group of persons would be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of that State in carrying out the conduct. The Resolution also recognizes that there is a breach of an international obligation by a State when an act of that State is not in conformity with what is required of it by that obligation, regardless of its origin or character.[99]

Diplomatic relations between States are intrinsically linked to State responsibility and are based on relations between States dependent on comity.[100] The fundamental fact in this context is that international society is not an unchanging entity, but is subject to the ebb and flow of political life and activity.[101] Analogies to diplomatic relations between States arise often in the context of terrorism as in the 1985 *Rainbow Warrior* case. The sinking of the ship *Rainbow Warrior* in Auckland Harbour in New Zealand as a result of an officially organized undercover French military operation calculated to obstruct Greenpeace protests against French nuclear operations in the South Pacific is a good example. The destruction of the ship, which resulted in the death of a Dutch seaman, was directly attributable to the placing of explosives by an agency reporting to the French Ministry of Defence. This was construed by the Government of New Zealand and by the High Court of New Zealand as a violation of the principles of international law against the sovereignty of the country.[102] The Secretary General of the United Nations ruled that France should offer New Zealand an apology and that compensation should follow to the amount of $ 7,000,000. The *Rainbow Warrior* incident goes down in the annals of diplomatic relations as an act of international delinquency resulting in the criminal responsibility of a State.

Another analogous diplomatic incident occurred in 1981 when, on May 6, the US Department of State announced at a special press briefing that the United States Government had decided to require the Socialist People's Libyan Arab Jamahiriya

[99] *Id*, Article 12.

[100] In law, comity specifically refers to legal reciprocity - the principle that one jurisdiction will extend certain courtesies to other nations (or other jurisdictions within the same nation), particularly by recognizing the validity and effect of their executive, legislative, and judicial acts. The term refers to the idea that courts should not act in a way that demeans the jurisdiction, laws, or judicial decisions of another jurisdiction. Part of the presumption of comity is that other jurisdictions will reciprocate the courtesy shown to them.

[101] See generally Jennings and Watts (1992), Lauterpacht (1947), Chen (1951), Shaw (2003).

[102] *R*. v. *Mafart and Prieur*, New Zealand High Court, Auckland Registry, 22 November 1985, Per Davison CJ reported in 74 *ILR* 241.

to close its People's Bureau at Washington immediately and to withdraw all personnel within five working days. The Department's official statement was that from the first days of the Administration, both the President and the Secretary of State had made known their very real concern about a wide range of Libyan provocations and misconduct, including support for international terrorism. The United States made it officially clear that it had been concerned by a general pattern of unacceptable conduct by the People's Bureau in Washington, which was contrary to internationally accepted standards of diplomatic behaviour. The United States therefore asked the Libyans to close their People's Bureau in Washington and have given them five working days starting today to withdraw their personnel. This action reduced US relations with Libya to the lowest level consistent with maintenance of diplomatic relations and was followed with a travel advisory which stated that due to unsettled relations between the United States and the Government of Libya, the Department of State warned American citizens against any travel to or residence in Libya. Travellers were also informed that the US Embassy in Tripoli was closed and the US was not in a position to provide consular protection and assistance to Americans presently in Libya.[103]

In 1999, the Clinton administration warned Russia to voluntarily reduce the large number of intelligence officers operating in the United States or face cutbacks in diplomatic positions or expulsions. U.S. Ambassador James Collins delivered the message in Moscow during a meeting with Vladimir Putin, the former KGB domestic spying chief and currently Russia's top Security Council adviser, according to administration officials familiar with the issue. The warning followed two expulsions of Russian intelligence officers from the United States and the ouster of a U.S. Army attaché from Moscow a month earlier.[104]

The international treaty regulating diplomatic relations is the *Vienna Convention on Diplomatic Relations* of 1961.[105] The Convention does not explicitly make provision for the right to break diplomatic relations. It follows by implication from Article 2 which provides that the establishment of diplomatic relations takes place by mutual consent that if either State withdraws that consent diplomatic relations are broken. Breach therefore takes place normally in consequence of a unilateral act – even though it frequently follows a sequence of reciprocal or retaliatory moves between two States to downgrade their relations or a collective political decision by a number of States directed against another State whose conduct is regarded as unacceptable. Relations are broken from the moment of the initial action.[106] The other State has no option in the matter. There are no legal

[103] Dept. of State File No. P81 0101–1084.

[104] Bill Gertz, *The Washington Times*, 26 July 1999.

[105] Done at Vienna on 18 April 1961 and entered into force on 24 April 1964. United Nations Treaty Series, Vol. 5000 at p. 95.

[106] For an account of the series of incidents and complaints between France and Iran which led France to break diplomatic relations in July 1987, see *1987 AFDI 1000*. See also do Nascimento e Silva, *Diplomacy in International Law* p. 173–4.

limitations on the right of a State to break diplomatic relations with another, but the action is now invariably taken for political reasons. Practical considerations will almost always favour the continuation of relations, though not necessarily the retention of a permanent mission. This has become more obvious in the light of some recent cases where diplomatic relations subsisted even while armed conflict was taking place between sending and receiving States – as between India and Pakistan in 1965 and 1971.

A breach of diplomatic relations generally precludes direct contact between sending and receiving States other than what is needed to effect orderly departure and some form of interim regime. It does not, however, preclude the sending and receiving of special missions (which may later herald a resumption of normal diplomatic relations), meetings between diplomatic representatives of the two States in a third State (for example the regular meetings in Warsaw over many years of representatives of the United States and of the People's Republic of China) or contacts between representatives of the two States to an international organization. Detailed rules on permissible contacts are usually provided in the internal diplomatic service regulations of each State. It is often a feature of modern diplomacy that those on occasion a much-advertised breach of relations may turn out to be only partially real. This occurs when two States, having broken off diplomatic relations, usually on the initiative of one of them, continue an active, if quiet, direct relationship despite the appointment of third States to protect the interests of each in the territory of the other State.[107]

Whatever unilateral diplomatic action an aggrieved State might take, be it on grounds of sovereignty or the violation of its national property (passports) and the rights of its citizens who held the passports, there are certain legal nuances in the Mahmoud al-Mabhouh case which are incontrovertible. Falsification of passports and identity theft are serious criminal offences under most national laws. It could well be that these are also offences under the laws of Israel. Falsification of a national passport, whatever its country or nationality might be, by a member of the Israeli intelligence services brings to bear issues that are much more serious than mere breaches of diplomatic courtesy or relations. Under the theory of condonation any government involved would be seriously implicated, were it to turn out that it was aware that falsified travel documents were being used by its security agency as has been suggested by some.

The international community should therefore condemn the extra judicial killing of Mahmoud al-Mabhouh as a breach of international law and those involved must unequivocally declare as to whether they were aware that falsified travel documents were being used by Mossad in relation to this operation and/or any other. If there is cogent evidence implicating the Israeli Government, the international community must also require the former to confirm whether its intelligence services were involved in the murder of Mahmoud al-Mabhouh and demand that the Israeli

[107] D. James, "Diplomatic Relations and Contacts", *1991 BYIL 375*.

government confirm whether or not their intelligence services used falsified passports for this or any other operation or whether they have done since any assurance that they would not do so. Furthermore the international community should seek an assurance from the Israeli government that their intelligence operatives will never falsify passports for use in operations and require the Israeli government to condemn the killing of Mahmoud al-Mabhouh as a breach of international law. Finally an assurance must be sought from the Israeli government that they will extradite to Dubai any of those identified by the Dubai authorities as having been involved in the killing to face trial for murder and to Ireland, Britain, France and/or Germany to face trial for offences arising out of the abuse of passports issued by those countries.

At present, the issue of extradition could be settled through the United Nations and its Organs such as the Security Council[108] and the International Court of Justice (ICJ).[109] Of noteworthy practical relevance with regard to the complicity theory, particularly on the issue of extradition and whether one State can demand the extradition of offenders harbored in another State is the opinion given by the ICJ[110] on the explosion over Lockerbie, Scotland on 21 December 1988 of PAN AM Flight 103. The explosion is believed to have been caused by the detonation of a plastic explosive concealed in a portable cassette player/radio. The ICJ noted that it was a general principle of international law that no State could be compelled to extradite its nationals and that the State concerned held the prerogative of trying the accused of a crime in its own territory. The ICJ was encumbered with the discussion as to whether the Court had jurisdiction over a United Nations Security Council Resolution on the issue. The essence of the views of the learned judges of the ICJ was that the complimentary roles played by the United Nations Security Council and the ICJ would devolve responsibility on States to respect both these organs on the subject of extradition of private offenders.

It appears that the question in The ICJ's was whether the Security Council, by its Resolution 748 (1992) which required Libya to extradite its nationals either to the United States or to the United Kingdom, had the authority to override an established

[108] The Security Council is the branch of the United Nations charged with the maintenance of international peace and security. Its powers, outlined in the Charter of the United Nations, include the establishment of peacekeeping operations, the establishment of international sanctions, and the authorization for military action. The Security Council's power are exercised through its Resolutions. The Permanent members of the Security Council are the United States of America, United Kingdom, France, the Russian Federation and the Republic of China.

[109] The International Court of Justice (ICJ) is the principal judicial organ of the United Nations (UN). It was established in June 1945 by the Charter of the United Nations and began work in April 1946.The Court's role is to settle, in accordance with international law, legal disputes submitted to it by States and to give advisory opinions on legal questions referred to it by authorized United Nations organs and specialized agencies. The Court is composed of 15 judges, who are elected for terms of office of 9 years by the United Nations General Assembly and the Security Council. It is assisted by a Registry, its administrative organ. Its official languages are English and French.

[110] I.C.J. Reports 1980, 116.

principle of international law. The answer to this question was, in the view of one judge, in the affirmative.

If a State found reprehensible is unable or unwilling to make reparations as requested, there is nothing to prevent a State from unilaterally terminating diplomatic relations with any that State if the former wishes to do so.

3.3 Full Body Scanners and Emergent Issues

Aviation is an important global business and a significant driver of the global economy. It is vital, therefore, that stringent measures are taken to counter acts of unlawful interference with civil aviation. The *Convention on International Civil Aviation* signed at Chicago on 7 December 1944, states in its *Preamble* that whereas the development of civil aviation may help preserve friendship and understanding among the people of the world, yet, its abuse could become a threat to general security.

The genealogy of the term "*Terrorism*" lies in Latin terminology meaning "to cause to tremble"(*terrere*). Since the catastrophic events of 11 September 2012, we have seen stringent legal measures taken by the United States to attack terrorism, not just curb it. The famous phrase "war on terror" denotes pre-emptive and preventive strikes carried out through applicable provisions of legitimately adopted provisions of legislation. The earliest example is the *Air Transportation Safety and System Stabilization Act* (ATSAA) enacted by President Bush less than 2 months after the 9/11 attacks. Then, 2 months after the attacks, in November 2001, Congress passed the *Aviation and Transportation Security Act* (ATSA) with a view to improving security and closing the security loopholes which existed on that fateful day in September 2001. The legislation paved the way for a huge federal body called the Transportation Security Administration (TSA) which was established within the Department of Transportation. The Homeland Security Act of 2002 which followed effected a significant reorganization of the Federal Government.

Since the events of 11 September 2001, there have been several attempts against the security of aircraft in flight. These threats have ranged from shoe bombs to dirty bombs to explosives that can be assembled in flight with liquids, aerosols and gels. In every instance the global community has reacted with pre emptive and preventive measures which prohibit any material on board which might seemingly endanger the safety of flight. Some jurisdictions have even gone to extremes in prohibiting human breast milk and prescriptive medications on board.

New and emerging threats to civil aviation are a constant cause for concern to the aviation community. Grave threats such as those posed by the carriage of dangerous pathogens on board, the use of cyber technology calculated to interfere with air navigation systems, and the misuse of man portable air defence systems are real and have to be addressed with vigour and regularity. The International Civil Aviation

Organization has been addressing these threats for some time and continues to do so on a global basis.

It is a platitude to say that aviation security is a largely reactive process. It will be recalled that after the spate of hijackings in the late 1960s and 1970s, States rushed to install detectors with X-Ray capability at the entrance to the aircraft gate. Then, as the *displacement theory*[111] demonstrated, terrorists moved their attention towards attacking airports, which prompted States to install screening equipment at centralized points in the terminal itself. In similar vein, in the aftermath of the attempted bombing of an aircraft on 25 December 2009 by a person who is alleged to have carried explosives in his undergarments, some States began to look seriously into tightening airport security, particularly through a more stringent body scanning process. While the United States toughened screening measures on US bound flights, particularly with regard to passengers arriving from 14 targeted nations,[112] airports in the United Kingdom began the use of full body scanners at both Heathrow and Manchester airports.[113] In Canada, Rob Merrifield, Minister of State for Transport is reported to have stated that 44 scanners have been ordered to be used on passengers selected for secondary screening at Canadian airports. The machines, which can scan through clothing, will be installed in Vancouver, Calgary, Edmonton, Winnipeg, Toronto, Ottawa, Montreal and Halifax.[114] This measure is partly due to the fact that the Christmas day incident was later classified as having occurred due to a serious lapse in security.

Full body scanners, costing about $ 250,000 each and claimed by some security experts as an effective tool in detecting hidden explosives, show the contours of the human body as well as body parts in some detail, prompting some to question the legality and ethical justification of their use. In the United States, passengers handpicked for a full-body scan can opt out of the screening, but if they do, they must submit to full-body pat-downs by an officer of the Transport Security

[111] The Displacement Theory suggests that removing opportunity for crime or seeking to prevent a crime by changing the situation in which it occurs (see Situational Crime Prevention) does not actually prevent crime but merely moves it around. There are five main ways in which this theory suggests crime is moved around: crime can be moved from one location to another (geographical displacement); crime can be moved from one time to another (temporal displacement); crime can be directed away from one target to another (target displacement); one method of committing crime can be substituted for another (tactical displacement); and one kind of crime can be substituted for another (crime type displacement).

[112] Afghanistan, Algeria, Cuba, Iran, Iraq, Lebanon, Libya, Nigeria, Pakistan, Saudi Arabia, Somalia, Sudan, Syria and Yemen. See US Toughens Screening for US- Bound Flights, *Air Letter*, No. 16,896, Monday 04 January 2010, at 1.

[113] UK Airports Commence Use of Full Body Scanners, *Air Letter*, No. 16,918, Wednesday 03 February 2010 at 2. According to this report, scanning equipment were scheduled to be installed in Birmingham in late February 2010. *Ibid.*

[114] CBC News, January 5 2010. See: http://www.cbc.ca/canada/story/2010/01/05/security-canada-us-airport.html#ixzz0eVT3wBNY.

Administration (TSA).[115] The technology was introduced a couple of years ago, but U.S. airports have been slow to install the machines, partly because of privacy concerns raised by some members of Congress and civil liberties groups.

It must be noted that in the United States, the Fourth Amendments states:

> The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[116]

The significance of this provision lies in the fact that the prohibition is against unreasonable searches, and that too by agents of the governments, the latter fact being borne out by a strong *cursus curiae* in the United States.[117] It can therefore be assumed that the Fourth Amendment may not be applicable in instances where scanning is carried out by airport security officers who are not government agents.[118] If, however, the scanning at the airport is conducted by officers of the government, by law, the consent of the passenger has to be obtained before such scanning is carried out.[119]

States which are installing full body scanners are fully aware that their use could bring to bear issues of privacy. However, it should be noted that this is just one more reactive step – to ensure that no person enters an aircraft with explosives hidden in his underwear – and the only known way to respond to this new threat is to use full body scanner. The question then arises as to whether the responsibility of the State toward its constituents and those using aircraft for transport from and to their territory, to prevent private acts of terrorism overrides the right of privacy of the individual. This article will address the balance between the two interests.

3.3.1 The Right of Privacy of the Passenger

The *Convention on International Civil Aviation* of 1944 (Chicago Convention),[120] which established the regulatory framework for international civil aviation, underscores the fundamental aim of States in the context of civil aviation to exchange privileges which friendly nations have a right to expect from each other. In his message to the Conference in Chicago, President Roosevelt said:

---

[115] Philip Rucker, TSA Tries to Assuage Concerns About Full Body Scans, *Washington Post*, Monday January 4 2010 at 1.

[116] *Us Constitution*, Article 1 Sec. 4 Clause 6.

[117] See Kathleen Sweet, Aviation Security and Passenger Rights, *Aviation Security Management*, Volume Two, Andrew R. Thomas ed, Praeger Security International: Westport Connecticut, 2008, at 45.

[118] *Ibid.*

[119] See *US* v. *Favela* 247 F.3d.838, 2001 and *U.S* v. *Eustaquio* 198 R.3d 1068 (8th Cir.1999).

[120] Convention on International Civil Aviation, signed at Chicago on 7 December 1944. See ICAO Doc 7300/9 Ninth Edition, 2008.

"the Conference is a great attempt to build enduring institutions of peace, which cannot be endangered by petty considerations or weakened by groundless fears".[121]

The Chicago Convention embodies in its *Preamble* the need to create and preserve friendship and understanding among the nations and peoples of the world, and cautions Contracting States that the abuse of this friendship and understanding can become a threat to general security. Article 13 of the Convention provides that the laws and regulations of a Contracting State as to the admission to and departure from its territory of passengers, crew or cargo of aircraft, such as regulations relating to entry, clearance, immigration, passports, customs and quarantine shall be complied with by or on behalf of such passengers, crew or cargo upon entrance into or departure from, or while within the territory of that State. This provision ensures that a Contracting State has the right to prescribe its own internal laws with regard to passenger clearance and leaves room for a State to enact laws, rules and regulations to ensure the security of that State and its people at the airport. However, this absolute right is qualified so as to preclude unfettered and arbitrary power of a State, by Article 22 which makes each Contracting State agree to adopt all practicable measures, through the issuance of special regulations or otherwise, to facilitate and expedite navigation of aircraft between the countries.

The above notwithstanding, there are three rights of privacy relating to the display and storage and use of personal data:

1. The right of an individual to determine what information about oneself to share with others, and to control the disclosure of personal data;
2. The right of an individual to know what data is disclosed, and what data is collected and where such is stored when the data in question pertains to that individual; the right to dispute incomplete or inaccurate data; and
3. The right of people who have a legitimate right to know in order to maintain the health and safety of society and to monitor and evaluate the activities of government.[122]

It is incontrovertible that the data subject has a right to decide what information about oneself to share with others and more importantly, to know what data is collected about him. This right is balanced by the right of a society to collect data about individuals that belong to it so that the orderly running of government is ensured.

The data subject, like any other person, has an inherent right to his privacy.[123] The subject of privacy has been identified as an intriguing and emotive one.[124] The right to privacy is inherent in the right to liberty, and is the most comprehensive of rights and the right most valued by civilized man.[125] This right is susceptible to

[121] Proceedings of the International Civil Aviation Conference, Chicago, Ikllinois, November 1–December 7 1944 The Department of State, Vol. 1 at p. 43.

[122] Hoffman (1980).

[123] Abeyratne (2001, 2002b).

[124] Young (1978).

[125] Warren and Brandies (1890–1891).

being eroded, as modern technology is capable of easily recording and storing dossiers on every man, woman and child in the world.[126] The data subject's right to privacy, when applied to the context of the full body scanner is brought into focus by Alan Westin who says:

> Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information is communicated to others.[127]

The role played by technology in modern day commercial transactions has affected a large number of activities pertaining to human interaction. The emergence of the information superhighway and the concomitant evolution of automation have inevitably transformed the social and personal life styles and value systems of individuals, created unexpected business opportunities, reduced operating costs, accelerated transaction times, facilitated accessibility to communications, shortened distances, and removed bureaucratic formalities.[128] Progress notwithstanding, technology has bestowed on humanity its corollaries in the nature of automated mechanisms, devices, features, and procedures which intrude into personal lives of individuals. For instance, when a credit card is used, it is possible to track purchases, discovering numerous aspects about that particular individual, including, food inclination, leisure activities, and consumer credit behaviour.[129] In similar vein, computer records of an air carrier's reservation system may give out details of the passenger's travel preferences, inter alia, seat selection, destination fondness, ticket purchasing dossier, lodging keenness, temporary address and telephone contacts, attendance at theatres and sport activities, and whether the passenger travels alone or with someone else.[130] In similar vein, does it follow that a full body scanning exercise would reveal imperfections of the human body which person would desire to keep private? This scheme of things may well give the outward perception of surveillance attributable to computer devices

[126] As far back as in 1973 it was claimed that ten reels, each containing 1,500 m of tape 2.5 cm wide, could store a 20 page dossier on every man, woman, and child in the world. See Jones (1973).

[127] Westin (1970).

[128] Orwell (1978).

[129] For a detailed analysis of the implications of credit cards with respect to the right of privacy see Nock (1993).

[130] The paramount importance of airline computer reservation system records is reflected in the world-renowned cases *Libyan Arab Jamahiriya* v. *United Kingdom* and *Libyan Arab Jamahiriya* v. *United States of America* regarding the PANAM 103 accident at Lockerbie, Scotland in 1988, where the International Court of Justice requested air carriers to submit to the Court the defendants' flight information and reservation details. See International Court of Justice. News Release 99/36, "Questions of Interpretation and Application of the 1971 Montreal Convention arising from the Aerial Incident at Lockerbie" (1 July 1999), online: http://www.icj-cij.org/icjwww/idocket/iluk/iluk2frame.html (date accessed: 14 July 2000). In a similar vein, Arthur R. Miller describes the significance of airline computer reservation system records when dealing with federal, state, local, and other types of investigations where these dossiers could provide valuable information. See also Miller(1971).

monitoring individuals' most intimate activities, preferences and physical attributes, leading to the formation of a genuine "traceable society".[131]

The main feature of this complex web of technological activity is that an enormous amount of personal information handled by such varied players from the public and private sector, may bring about concerns of possible "data leaks" in the system, a risk that could have drastic legal consequences affecting an individual's rights to privacy.

At the international level, privacy was first recognized as a fundamental freedom in the *Universal Declaration of Human Rights*.[132] Thereafter, several other human rights conventions followed the same trend, granting to individuals the fundamental right of privacy.[133] The pre-eminent concern of these international instruments was to establish a necessary legal framework to protect the individual and his rights inherent to the enjoyment of a private life.

Privacy represents different things for different people.[134] The concept per se has evolved throughout the history of mankind, from the original non-intrusion approach, which defended an individual's property and physical body against unwanted invasions and intrusions, then manifesting in whom to associate with, later enlarging its scope to include privacy as the individual's decision-making right,[135] and culminating in the control over one's personal information.[136] Thus, the conceptual evolution of privacy is directly related to the technological advancement of each particular period in history.

---

[131] See Scott (1995), Burnham (1983). *A contrario* to the argument supported in this thesis that the advancement of technology directly affects the intimacy of individuals. U.S. Circuit Judge Richard Posner favours the idea that other factors, such as urbanisation, income, and mobility development have particularly weakened the information control that, for instance, the government has over individuals: this denotes that individuals' privacy has increased. See Posner (1978).

[132] The text reads: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks". See *Universal Declaration of Human Rights*. GA Res. 217(III), 10 December 1948, Art. 12.

[133] See International Covenant on Civil and Political Rights, GA Res. 2200 (XXI), 16 December 1966, Art. 17; American Declaration on the Rights and Duties of the Man (1948), Art. 5; American Convention on Human Rights, 22 November 1969, San Jose, Costa Rica, Art. 11; Convention for the Protection of Human Nations Convention on Migrant Workers, A/RES/45/158, 25 February 1991, Art. 14; United Nations Convention on Protection of the Child, GA Res. 44/25, 12 December 1989, Art. 16.

[134] See Regan (1995), Freund (1971).

[135] In this case, the US Supreme Court acknowledged the right of women to have abortions based on the grounds that the federal government could not interfere within her "decisional privacy" sphere. See *Roe* v. *Wade*, 410 U.S. 113 (1973). See also Cate (1997), Zelermyer (1959).

[136] In a remarkable case concerning the legality of a national census scheduled by the authorities, the German Constitutional court connected the individual's liberty and the personal data processing of the intended census, to rule that if the individuals do not know for what purposes and who is collecting the data, that situation will eventually create an abdication of the individual's rights to the processor's command, "which cannot be tolerated in a democratic society". See Simitis (1995). See also Hoffer (2000), Gavison (1980).

The right of privacy, as enunciated by the United States Judge Thomas M. Cooley, was the right "to be let alone" as a part of a more general right to one's personality. This idea was given further impetus by two prominent young lawyers, Samuel D. Warren and Louis D. Brandeis,[137] in 1890.[138] Before this idea was introduced, the concept of privacy reflected primarily a somewhat physical property or life. The foundations of "information privacy", whereby the individuals would determine when, how, and to what extent information about themselves would be communicated to others, inextricably drawing the right of control of information about oneself,[139] is a cornerstone of privacy. With the development of computer capabilities to handle large amounts of data, privacy has been enlarged to include the collection, storage, use, and disclosure of personal information.[140] The notion of informational privacy protection, a typically American usage, has been particularly popular both in the United States and Europe, where the term "data protection" is used.[141]

Self-determination in the right to protect one's privacy was first judicially embraced by the German Bundesverfassungsgericht in 1983. The US Supreme court followed this trend by adopting the principle of privacy self-determination in *DOJ* v. *Reporters Comm. for Freedom of the Press*.[142]

It must be borne in mind that privacy is not an absolute, unlimited right that operates and applies in isolation.[143] It is not an absolute right, applied unreservedly, to the exclusion of other rights. Hence there is frequently the necessity to balance privacy rights with other conflictive rights, such as the freedom of speech and the right to access information when examining individuals' rights *vis-à-vis* the interest of society.[144] This multiplicity of interests will prompt courts to adopt a balanced approach when adjudicating on a person's rights, particularly whose interests of a State are involved.

---

[137] See Cooley (1888), as cited in Warren and Brandeis (1980).

[138] The definition of privacy as the "Right to be Alone" is often erroneously attributed to Warren and Brandeis. See Warren & Brandeis. See Cooley (1888) as cited in Warren and Brandeis (1980). Additionally the concept of privacy as "the right to be let alone", and "the right most valued by civilized man: was embraced by US courts in the landmark dissenting opinion of Justice Louis D. Brandeis in *Olmsted* v. *United States*. See *Olmsted* v. *United States*, 277 U.S. 438, 478 (1928) [hereinafter *Olmstead*.]

[139] See Westin (1967). For a similar conceptualisation of privacy, see Fried (1978).

[140] See Reidenberg (1995).

[141] The former Privacy Commissioner of British Columbia, Canada, has asserted that privacy was originally a "non-legal concept". See Flaherty (1991). The term "data protection" has been translated from the German word *Datenschutz*, referring to a set of policies seeking to regulate the collection, storage, use, and transfer of personal information. See Bennet (1992).

[142] See DOJ v. Reporters Comm. for Freedom of the Press, 489 U.S. 749 AT 763 (1988).

[143] See Simmel (1971).

[144] See Halpin (1997). See also Foschio (1990). For a comprehensive study on the conflictive interest on privacy and the mass media and the Freedom of Speech, see Pember (1972), Prowda (1995). See also J. Montgomery Curtis Memorial Seminar (1992).

Since the data contained in equipment such as body scanners may be subject to trans-border storage, there is a compelling need to consider the introduction of uniform privacy laws in order that the interests of the data subject and the data seeker are protected. Although complete uniformity in privacy legislation may be a difficult objective to attain[145] (as has been the attempt to make other aspects of legislation uniform), it will be well worth the while of the international community to at least formulate international Standards and Recommend Practices (in the lines of the various ICAO Annexes) to serve as guidelines of State conduct. After all, as Collin Mellors pointed out:

> Under international agreements... privacy is now well established as a universal, natural, moral and human right. Article 12 of the Universal Declaration of Human Rights, Article 17 of the United Nations Covenant on Civil and Political Rights and Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, all specify this basic right to privacy. Man everywhere has occasion to seek temporary "seclusion or withdrawal from society" and such arrangements cannot define the precise area of the right to privacy.[146]

It is such a definition that is now needed so that the two requirements of ensuring respect for information about individuals and their privacy on the one hand, and the encouragement of free and open dissemination of trans-border data flows on the other, are reconciled.

As for the use of information resulting in a full body scan, such information is purely biological and should be used only for purposes of identifying weapons or dangerous objects on the person with an explicit undertaking by the authorities concerned who use the information that it will not be used for any purpose other than for purposes of scanning. Before a process for the collection of such information is formally put into practice, legal issues pertaining to privacy, cultural sensitivity and ethical justification should be carefully thought out, and given foremost consideration.

In the provision of biometric data, the provider of the information and the receiver thereof are both under obligation to ensure that the data is not used for any purpose other than clearance of the owner of the information through customs barriers. This information may not later be used for commercial or other gain for instance for advertising purposes (such as using the physical profile of a prominent actor or actress whose biometric information originally given for customs clearance).[147]

In the body scanning process, there is an implicit link between ownership rights and privacy. Data protection legislation, including data privacy laws have been enacted by many countries throughout the world for two main reasons: protection of privacy; and ensuring of access by the owner to his information stored in a

---

[145] *Computers and Privacy in the Next Decade*, Lance J. Hoffman ed. op. cit at 146.

[146] Collin Mellors, *Governments and the Individual – Their Secrecy and His Privacy, cited in, A Look at Privacy*, John B.Young ed., Supra, note 15, at 94.

[147] See *Gould Estate* v. *Stoddart Publishing Company* (1996) O.J. No. 3288 (Gen. Div)

computer. Although the exact nature can vary from State to State, there is a common thread that weaves itself into the fabric of legislation in general, to ensure that: data is obtained by lawful means and processed in a fair manner; data is stored for the legitimate purpose intended and not used for any purpose incompatible with the original purpose; the collection of data is done in a reasonable manner and not excessively in order to store data over and above what is necessary; the accuracy of the data should be ensured; and the time of preservation of data is limited to the period during which such data is used.

The protection of human rights is the most significant and important task for a modern State, particularly since multi ethnic States are the norm in today's world. Globalization and increased migration across borders is gradually putting an end to the concept of the nation State, although resistance to reality can be still seen in instances where majority or dominant cultures impose their identity and interests on groups with whom they share a territory. In such instances, minorities frequently intensify their efforts to preserve and protect their identity, in order to avoid marginalization. Polarization between the opposite forces of assimilation on the one hand and protection of minority identity on the other inevitably causes increased intolerance and eventual armed ethnic conflict. In such a scenario, the first duty of governance is to ensure that the rights of a minority society are protected.

3.3.2 Security of the State

The foregoing discussion addressed the right of privacy of the individual which is paramount over most legal considerations. The only factor that would override this would be the security of State. Inherent to the concept of security of State is State responsibility to its citizens and others who are in its territory. The fundamental issue in the context of State responsibility for the purposes of this article is to consider whether a State should be considered responsible for its own failure or non-feasance to prevent a private act of terrorism against civil aviation or whether the conduct of the State itself can be impugned by identifying a nexus between the perpetrator's conduct and the State. One view is that an agency paradigm, which may in some circumstances impute to a state reprehensibility on the ground that a principal–agent relationship between the State and the perpetrator existed, can obfuscate the issue and preclude one from conducting a meaningful legal study of the State's conduct.[148]

At the core of the principal–agent dilemma is the theory of complicity, which attributes liability to a State that was complicit in a private act. Hugo Grotius (1583–1645), founder of the modern natural law theory, first formulated this theory

[148] Caron (1998) cited in Becker (2006a).

based on State responsibility that was not absolute. Grotius' theory was that although a State did not have absolute responsibility for a private offence, it could be considered complicit through the notion of *patienta* or *receptus*.[149] While the concept of *patienta* refers to a State's inability to prevent a wrongdoing, *receptus* pertains to the refusal to punish the offender.

The eighteenth Century philosopher Emerich de Vattel was of similar view as Grotius, holding that responsibility could only be attributed to the State if a sovereign refuses to repair the evil done by its subjects or punish an offender or deliver him to justice whether by subjecting him to local justice or by extraditing him.[150] This view was to be followed and extended by the British jurist Blackstone a few years later who went on to say that a sovereign who failed to punish an offender could be considered as abetting the offence or of being an accomplice.[151]

A different view was put forward in an instance of adjudication involving a seminal instance where the Theory of Complicity and the responsibility of states for private acts of violence was tested in 1925. The case[152] involved the Mexico-United States General Claims Commission which considered the claim of the United States on behalf of the family of a United States national who was killed in a Mexican mining company where the deceased was working. The United States argued that the Mexican authorities had failed to exercise due care and diligence in apprehending and prosecuting the offender. The decision handed down by the Commission distinguished between complicity and the responsibility to punish and the Commission was of the view that Mexico could not be considered an accomplice in this case.

The Complicity Theory, particularly from a Vattellian and Blackstonian point of view is merely assumptive unless put to the test through a judicial process of extradition. In this Context it becomes relevant to address the issue through a discussion of the remedy.

The emergence of the Condonation Theory was almost concurrent with the *Jane* case[153] decided in 1925 which emerged through the opinions of scholars who belonged to a school of thought that believed that States became responsible for private acts of violence not through complicity as such but more so because their refusal or failure to bring offenders to justice, which was tantamount to ratification of the acts in question or their condonation.[154] The theory was based on the fact that it is not illogical or arbitrary to suggest that a State must be held liable for its failure to take appropriate steps to punish persons who cause injury or harm to others for the reason that such States can be considered guilty of condoning the criminal acts

[149] Grotius and Scott (1646).

[150] De Vattel and Fenwick (1916).

[151] Blackstone and Morrison (2001).

[152] *Laura M.B. Janes (USA)* v. *United Mexican States* (1925) 4 R Intl Arb Awards 82.

[153] *Ibid.*

[154] *Black's Law Dictionary* defines condonation as "pardon of offense, voluntary overlooking implied forgiveness by treating offender as if offense had not been committed."

and therefore become responsible for them.[155] Another reason attributed by scholars in support of the theory is that during that time, arbitral tribunals were ordering States to award pecuniary damages to claimants harmed by private offenders, on the basis that the States were being considered responsible for the offences.[156]

The responsibility of governments in acting against offences committed by private individuals may sometimes involve condonation or ineptitude in taking effective action against terrorist acts, in particular with regard to the financing of terrorist acts. The United Nations General Assembly, on 9 December 1999, adopted the International Convention for the Suppression of the Financing of Terrorism,[157] aimed at enhancing international co-operation among States in devising and adopting effective measures for the prevention of the financing of terrorism, as well as for its suppression through the prosecution and punishment of its perpetrators.

The Convention, in its Article 2 recognizes that any person who by any means directly or indirectly, unlawfully or willfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out any act which constitutes an offence under certain named treaties, commits an offence. One of the treaties cited by the Convention is the International Convention for the Suppression of Terrorist Bombings, adopted by the General Assembly of the United Nations on 15 December 1997.[158]

The Convention for the Suppression of the Financing of Terrorism also provides that, over and above the acts mentioned, providing or collecting funds toward any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in the situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act, would be deemed an offence under the Convention.

The United Nations has given effect to this principle in 1970 when it proclaimed that:

> Every State has the duty to refrain from organizing or encouraging the organization of irregular forces or armed bands, including mercenaries, for incursion into the territory of another State. Every State has the duty to refrain from organizing, instigating, assisting or participating in acts of civil strife or terrorist acts in another State or acquiescing in organized activities within its territory directed towards the commission of such acts, when the acts referred to in the present paragraph involve a threat or use of force.[159]

---

[155] Jane's case, *Supra*, note 55, at 92.

[156] Hyde (1928).

[157] International Convention for the Suppression of the Financing of Terrorism, adopted by the General Assembly of the United Nations in resolution 54/109 of 9 December 1999.

[158] A/52/653, 25 November 1997.

[159] Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations, UN General Assembly Resolution 2625 (XXV) 24 October 1970.

Here, the words *encouraging* and *acquiescing in organized activities within its territory directed towards the commission of such acts* have a direct bearing on the concept of condonation and would call for a discussion about how States could overtly or covertly encourage the commission of such acts. One commentator[160] identifies three categories of such support: *Category I* support entails protection, logistics, training, intelligence, or equipment provided terrorists as a part of national policy or strategy; *Category II* support is not backing terrorism as an element of national policy but is the toleration of it; *Category III* support provides some terrorists a hospitable environment, growing from the presence of legal protections on privacy and freedom of movement, limits on internal surveillance and security organizations, well-developed infrastructure, and émigré communities.

The Convention, in its Article 2 recognizes that any person who by any means directly or indirectly, unlawfully or wilfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out any act which constitutes an offence under certain named treaties, commits an offence. The treaties listed are those that are already adopted and in force and which address acts of unlawful interference with such activities as deal with air transport and maritime transport. Also cited is the International Convention for the Suppression of Terrorist Bombings, adopted by the General Assembly of the United Nations on 15 December 1997.

The *Convention for the Suppression of the Financing of Terrorism* also provides that, over and above the acts mentioned, providing or collecting funds toward any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in the situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act, would be deemed an offence under the Convention.

The above notwithstanding, one cannot ignore the incontrovertible fact that security is a systemic process. The mere use of full body scanners by no means ensures total security against acts of unlawful interference with civil aviation. As the Christmas day incident showed, intelligence gathering, sharing of information, and more importantly, integration and analysis of such information[161] are critical to the security chain. What is most important is to establish a global security culture that ensures the cooperation of the 190 ICAO member States by working in harmony. A perceived inadequacy of the global framework of aviation security is the lack of an implementation arm. ICAO has taken extensive measures to

[160] Steven Metz, State Support for Terrorism, Defeating Terrorism, Strategic Issue Analysis, at http://www.911investigations.net/IMG/pdf/doc-140.pdf.

[161] As stated by President Obama, "this was not a failure to collect intelligence. . .it was a failure to integrate and understand the intelligence that we already had. . ." Airline Bomber could Have Been Stopped, *The Air Letter*, Tuesday 05 January 2010, No. 16,897, at 1.

introduce relevant international conventions as well as Standards and Recommended Practices (SARPs) in Annex 17 to the Chicago Convention. There is also a highly classified *Aviation Security Manual* developed by ICAO which is provided to States. Additionally, the Organization provides focused security training courses to its member States. However, ICAO's role is largely confined to rule making and the provision of guidance, bringing to bear the need for an aviation security crisis management team on a global scale that could work towards effectively precluding acts of terrorism.

3.3.3 Flight NW 253

The attempted bombing of Northwest Airlines flight 253 on Christmas day of 2009, which was arguably the turning point in the initiative across the globe to use full body scanners, once again issued the ominous reminder that aviation is vulnerable and that there is a compelling need for a global security culture that recognizes and applies uniform global security standards. The first step toward achieving this objective is the realization by the aviation community of new and emerging threats to aviation and the need to share information. Since the event, several countries have imposed stringent security standards at airports and initiated inter-governmental meetings to discuss closer cooperation among States in the hope that such measures will effectively respond to the threat. Both ICAO and IATA took immediate measures after the event in issuing statements and called for a closer look by States at their security measures and a re-assessment of available responses to threats posed to aviation.

It is now abundantly clear that collection and sharing of information, improvement of technology and the strengthening of security standards are critical in addressing the problem of unlawful interference with civil aviation. Other aspects such as curbing the financing of terrorism, taking a closer look at the responsibility of States, and increasing vigilance on a global scale are also significant considerations.

On 25 December 2009, a person on board Northwest Airlines flight 253, flying from Amsterdam to Detroit, attempted to detonate an explosive device[162] which failed to explode, but ignited injuring the offender and two other passengers. The flight crew and some passengers restrained the offender, who was arrested when the A330 airliner landed safely in Detroit. The Summary of the United States White House Review which was issued subsequent to the event reflected preliminary findings which were that several opportunities that might have allowed the counter-terrorism community to take cohesive action by "connecting the dots" of information available prior to the attempted bombing of the airliner, brought to bear

[162] The device used contained the explosive PETN (Pentaerytritol) which was stitched into his underwear.

a need to assist counter-terrorism analysts in their preventive work.[163] The White House Review highlighted human errors which resulted in failure to identify, correlate and piece together an emerging terrorist plot against the United States. Also identified were weak points in assigning responsibility and accountability and shortcomings of the watch-list system that would have enabled the offender to board the flight.

Reportedly, as a result of the event, US officials reacted by tightening security measures for all US bound passengers, advising persons flying from 14 handpicked nations[164] that they would be subject to stringent screening.[165] Dutch authorities are known to have stated that they planned to put full body scanners into use within 3 weeks and British authorities had similar comments.[166]

The International Civil Aviation Organization (ICAO) responded on 30 December 2009 with a communiqué to its points of contacts in member States to the effect inter alia that ICAO Member States were encouraged to conduct a risk assessment, taking into consideration all the relevant factors, and implement appropriate screening measures. Where additional screening measures are considered necessary, these may include the application of explosives trace detection technology, physical searches and randomly-deployed explosives detection canine teams, among others.

The communiqué reminded ICAO Member States of the need for cooperation in all matters related to aviation security, particularly with regard to the requirements of Standard 2.4.1 of Annex 17 – *Security*, which required each member State to ensure that requests from other Contracting States for additional security measures in respect of a specific flight(s) by operators of such other States are met, as far as may be practicable. The requesting State was required to give consideration to alternative measures of the other State that are equivalent to those requested.

Finally ICAO stated that it was committed to provide all possible assistance in this matter, and will seek to establish the necessary communication and

[163] The *Aviation Safety Journal* records that there was a similar finding five years before the flight 253 incident where "Information was not shared . . . analysis was not pooled . . . often the handoffs of information were lost across the divide separating the foreign and domestic agencies of the government. The finding recommended that "improved use of 'no-fly' and 'automatic selectee' lists should not be delayed . . .. This screening function should be performed by the TSA [Transportation Security Administration], and it should utilize the larger set of watch-lists maintained by the federal government". . . the TSA . . . must give priority attention to improving the ability of screening checkpoints to detect explosives on passengers". See *http://asj.nolan-law.com/2009/12/red-flags-ignored-in-underpants-bomber-caper-same-as-in-911/*.

[164] Afghanistan, Algeria, Cuba, Iran, Iraq, Lebanon, Libya, Nigeria, Pakistan, Saudi Arabia, Somalia, Sudan, Syria and Yemen.

[165] US Toughens Screening for US Bound Fights, The Air Letter, Monday 4 January 2010, No. 10,896, at 1. According to the same report the Transportation Security Administration advised all passengers flying into the United States from abroad that they will be subject to random screening or so called "threat based screens".

[166] *Ibid.*

coordination mechanisms to ensure that any response to this latest threat is provided with the greatest possible degree of harmonization. In this respect, States were reminded of the need to register and provide up-to-date information to ICAO for the Aviation Security Point of Contact Network. Giovanni Bisignani, Director General of the International Air Transport Association (IATA), in a letter to the Secretary of the US Department of Homeland Security, noted inter alia that security was a government responsibility which was a shared priority with industry, urging that a comprehensive review of security systems followed.[167]

While it is quite true that, as stated by President Obama, "this was not a failure to collect intelligence. . .it was a failure to integrate and understand the intelligence that we already had. . ."[168] the event resurfaces three fundamental truths about aviation security: it is a global issue and there are new and emergent threats to civil aviation; there needs to be a global security culture; and information sharing between parties is essential. This article will address these issues.

At its 33rd session held in Montreal from 25 September – 5 October 2001, the ICAO Assembly adopted Resolution A33-1[169] which was a direct response to the terrorist acts of 9/11. The Resolution recognized that a new type of threat was posed to civil aviation which required new concerted efforts and policies of cooperation on the part of States. The Resolution also urges all ICAO member States to ensure, in accordance with Article 4 of the Chicago Convention,[170] that civil aviation is not used for any purpose inconsistent with the aims of the Convention, and to hold accountable and punish severely those who misuse civil aircraft as weapons of destruction, including those responsible for planning and organizing such acts or for aiding, supporting or harbouring perpetrators. It also called upon States to cooperate with each other in this endeavour and to ensure that ICAO Standards and Recommended Practices (SARPs) relating to aviation security are adhered to. Finally the Resolution directed the Council of ICAO and the Secretary General to act urgently to address new and emerging threats to civil aviation, in particular to review the adequacy of existing aviation conventions on security.

A Special Sub Committee of the Legal Committee of ICAO met in Montreal from 3 to 6 July 2007 to discuss the preparation of one or more instruments addressing new and emerging threats. One of the issues addressed at this meeting was the unlawful transport of biological, chemical, nuclear weapons and other dangerous substances on board aircraft.

Earlier, the Secretary General of ICAO, Dr. Taieb Cherif, addressing the China Civil Aviation Development Forum on 9 May 2007, stated that although the global

[167] *http://iata.org/pressroom/pr/2009-12-30-02.htm*.

[168] Airline Bomber could Have Been Stopped, *The Air Letter*, Tuesday 05 January 2010, No. 16,897, at 1.

[169] Resolution A33-1, Declaration on misuse of civil aircraft as weapons of destruction and other terrorist acts involving civil aviation, Assembly Resolutions in Force (as of 8 October 2004) ICAO Doc. 9848. at VII-1.

[170] Supra n. 3

air transport system remains as secure as ever, yet events such as the illegal terrorist plot in the United Kingdom in the Summer of 2006, potentially involving liquids used as explosives, reminds us how vulnerable the system is. On another aviation platform, Giovanni Bisignani, Director General of IATA stressed at its Annual General Meeting held in Vancouver from 3 to 5 June 2007 that the industry had changed tremendously in 5 years since 9/11. Bisignani stated that, 6 years after the tragic events of 2001, air travel was much more secure but there were unlimited ways to attack the aircraft integrity. He added that there was no perfect security system and terrorists change tactics and weapons. Bisignani rightly pointed out that terrorists are studying what measures the industry is adopting; and that all the air industry can do is make the system strong enough to constitute sufficient deterrent and make aircraft a harder target to hit.

3.3.4 The AVSEC Panel

The Aviation Security Panel of ICAO met at its 20th Meeting in Montreal from 30 March to 3 April 2009. One of the key areas of discussion at this meeting concerned new and emerging threats to civil aviation. The Panel worked through the Working Group on New and Emerging Threats and noted that significant progress in efforts to proactively identify vulnerabilities and potential gaps in existing measures had been made, that would strengthen *Annex 17* (Aviation Security)to the Convention on International Civil Aviation (Chicago Convention).[171] At this meeting, the European Civil Aviation Conference (ECAC) stressed the importance of the challenge posed by cyber threats in light of the current lack of related provisions in Annex 17.

Consequently, the Panel considered the threat of cyber attacks, and some members stressed that this threat is significant. With reference to a proposal to include a Recommended Practice in Annex 17 to ensure that information and communication technology systems used for civil aviation purposes be protected from cyber attacks, the Panel agreed that, given the complexity of this issue, which involves air traffic management systems, aircraft design and operations, the matter requires further analysis by the Working Group on New and Emerging Threats prior to inclusion in Annex 17 or any guidance material. This analysis will be disseminated over the secure website by the end of June 2009 and, depending on the results of the analysis, the Working Group on Amendment 12 to Annex 17 will develop a proposal for amending the Annex, to be presented to the Panel at its 21st meeting.

The Panel also considered the merits of building unpredictability into the aviation security regime. While concern was expressed regarding the impact of

[171] Supra n 3

unpredictable security measures on passenger confidence in aviation security, many Panel members supported implementation of the concept because of its value as a deterrent. It was suggested that States adopt an approach providing for a baseline regime, but with the addition of unpredictable measures, thus achieving a balance between certainty and unpredictability. With regard to an amendment to Annex 17 in this regard, the need for introducing unpredictability into the aviation security regime was considered, and it was agreed that unpredictability should be promoted in principle but not prescribed. The Panel suggested that if an Annex 17 specification related to unpredictability were to be developed, it would be necessary to ensure that the introduction of this concept by States does not diminish the level of security or result in delays for passengers. Further, the Panel noted that appropriate guidance material may be required to address the potential negative impact of introducing the concept of unpredictability, and proposed the development of guidance material related to unpredictability prior to the introduction of an amendment to Annex 17.

A Conclusion of the Panel was, inter alia, that the threat of cyber attacks is real and cannot be ignored, and that further analysis by the Working Group on New and Emerging Threats would be appropriate. Another Conclusion was that the ICAO focal point of contact (PoC) Network is an important tool for sharing critical threat information and should be used more effectively, and that the Secretariat should consider the establishment of a web-based community page. Yet another was that the concept of building unpredictability into the aviation security regime is in principle a useful tool, however, concerns expressed regarding the possible impact on the level of security and the impact on passenger confidence should be resolved before its inclusion as a Recommended Practice in Annex 17.

The Recommendations of the Panel were that:

a) The Working Group on New and Emerging Threats propose its new name, terms of reference and composition, including suggestions on how observers might participate in the Working Group, as well as details of its evolving collaboration with the G8 Group, at the 21st Panel meeting;
b) The Working Group evaluate the threat of cyber attacks and disseminate the results of its analysis on the secure website by the end of June 2009 and that, depending on the results of this analysis, the Working Group on Amendment 12 to Annex 17 consider developing an amendment to Annex 17 for presentation at the 21st Panel meeting;
c) The ICAO Secretariat issue an electronic bulletin reminding States of the importance of subscribing to the PoC Network and providing information on its usage; and
d) the concept of building unpredictability into the aviation security regime be further considered.[172]

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

3.3.4.1 The Need for a Security Culture

Since the events of 11 September 2001, there have been several attempts against the security of aircraft in flight. These threats have ranged from shoe bombs to dirty bombs to explosives that can be assembled in flight with liquids, aerosols and gels. In every instance the global community has reacted with pre emptive and preventive measures which prohibit any material on board which might seemingly endanger the safety of flight. Some jurisdictions have even gone to extremes in prohibiting human breast milk and prescriptive medications on board.

New and emerging threats to civil aviation are a constant cause for concern to the aviation community. Grave threats such as those posed by the carriage of dangerous pathogens on board, the use of cyber technology calculated to interfere with air navigation systems, and the misuse of man portable air defence systems are real and have to be addressed with vigour and regularity. The International Civil Aviation Organization has been addressing these threats for some time and continues to do so on a global basis.

Since the events of 11 September 2001 took place, the most critical challenge facing international civil aviation remains to be the compelling need to ensure that the air transport industry remains continuous and its consumer is assured of sustained regular, safe and secure air transport services. The Air Transport Association (ATA), in its 2002 State of the United States Airline Industry Statement, advised that, in the United States, the combined impact of the 2001 economic downturn and the precipitous decline in air travel following the 11 September 2001 attacks on the United States resulted in devastating losses for the airline industry which are likely to exceed $7 billion and continue through 2002.[173] Of course, the overall picture, which portended a certain inevitable gloom for the air transport industry, was not the exclusive legacy of United States' carriers. It applied worldwide, as was seen in the abrupt downfall of air traffic globally during 2001. The retaliation by the world community against terrorism, which is an ongoing feature in world affairs, increased the airline passenger's fear and reluctance to use air transport. In most instances in commercial aircraft purchasing, air carriers cancelled or postponed their new aircraft requisition orders. Many carriers, particularly in developing countries, were seen revisiting their cost structures and downsizing their human resource bases. It is incontrovertible that another similar event or series of events will inevitably plunge the aviation industry into similar despair and destitution.

ICAO has a security oversight programme called the Universal Security Audit Programme (UASP). The ICAO Universal Security Audit Programme (USAP), launched in June 2002, represents an important initiative in ICAO's strategy for

[173] State of the United States Airline Industry, *A Report on Recent Trends for United States Carriers*, Air Transport Association: 2002, Statement by Carol B. Hallett, President and CEO, ATA.

strengthening aviation security worldwide and for attaining commitment from States in a collaborative effort to establish a global aviation security system.

The programme, which is part of the Aviation Security Plan of Action, provides for the conduct of universal, mandatory and regular audits of the aviation security systems in all ICAO member States. The objective of the USAP is to promote global aviation security through the auditing of States on a regular basis to assist States in their efforts to fulfil their aviation security responsibilities. The audits identify deficiencies in each State's aviation security system, and provide recommendations for their mitigation or resolution.

Implementation of the programme commenced with the first aviation security audit taking place in November 2002 and between three and four audits continue to be conducted around the world each month. The 35th Session of the Assembly held from 28 September to 8 October 2004 mandated ICAO to maintain strict confidentiality of all State-specific information derived from audits conducted under the Universal Security Audit Programme (USAP). However, in order to promote mutual confidence in the level of aviation security between States, the Assembly urged all Contracting States to "share, as appropriate and consistent with their sovereignty, the results of the audit carried out by ICAO and the corrective actions taken by the audited State, if requested by another State".[174]

While noting the importance of continuing bilateral exchanges of information between States, the 36th Session of the Assembly, held from 18 to 28 September 2007, also recognized the value of proposals presented by the Council and Contracting States for the introduction of a limited level of transparency with respect to ICAO aviation security audit results[175] The Assembly directed the Council to consider such an introduction of a limited level of transparency, balancing the need for States to be aware of unresolved security concerns with the need to keep sensitive security information out of the public realm. In doing so, the Assembly emphasized that it was essential that any methodology developed to provide for increased transparency also ensure the appropriate safeguarding of a State's security information in order to prevent specific information that could be used to exploit existing vulnerabilities from being divulged.

The 36th Session of the ICAO Assembly adopted Resolution A 36–20,[176] *Appendix E* of which addresses the USAP. As mentioned earlier, it must be emphasized that the Resolution inter alia directs the Council to consider the introduction of a limited level of transparency with respect to ICAO aviation security audits, balancing the need for States to be aware of unresolved security

[174] A35-9, Appendix E, Resolving Clause 4; and Recommended Practice 2.4.5 of Annex 17 — *Security*).

[175] Resolution A36-20, A36-WP/336 and Plenary Action Sheet No. 3.

[176] Resolution A 36–20, Consolidated statement on the continuing CA policies related to the safeguarding of international civil aviation against acts of unlawful interference, Report of the Executive Committee (Report Folder) Assembly, Thirty –sixth Session, A36 – WP/336, p/46, at 16–2.

concerns with the need to keep sensitive security information out of the public realm and requests the Council to report to the next ordinary session of the Assembly (in 2010) on the overall implementation of the USAP.

Since the launch of the USAP in 2002, 169 aviation security audits and 77 follow-up missions have been conducted.[177] The audits have proven to be instrumental in the ongoing identification and resolution of aviation security concerns, and analysis reveals that the average implementation rate of Annex 17 Standards in most States has increased markedly between the period of the initial audit and the follow-up mission.

A critical part of the audit process is the requirement that all audited States submit a corrective action plan to address deficiencies identified during an audit. As directed by the Council, all States are notified (by State letter and on the USAP secure website) of those states that are more than 60 days late in submitting a corrective action plan. As of 31 July 2007, there were seven States that were more than 60 days late. In the case of late corrective action plans, repeated reminders are sent to States, including at the level of the Secretary General and with the involvement of the applicable Regional Office, and ICAO assistance is offered should the State require advice or support in the preparation of its action plan. Extensive feedback is provided to each audited State on the adequacy of its corrective action plan, and an ongoing dialogue is maintained where necessary to provide support in the implementation of proposed actions.

ICAO performs comprehensive analyses of audit results on levels of compliance with Annex 17 – *Security* Standards on an ongoing basis (globally, by region and by subject matter). This statistical data is made available to authorized users on the USAP secure website and is shared with other relevant ICAO offices as a basis for prioritizing training and remedial assistance projects. As of 31 July 2007, 77 follow-up missions had been conducted. These missions take place 2 years after the initial audit with the purpose of validating the implementation of State corrective action plans and providing support to States in remedying deficiencies. These missions are normally conducted by the applicable Regional Office, with close coordination through Headquarters. The results of the follow-up visits indicate that the majority of States have made significant progress in the implementation of their corrective action plans.

A high-level ICAO Secretariat Audit Results Review Board (ARRB) has been established as part of an overall coordinated strategy for working with States that are found to have significant compliance shortcomings with respect to ICAO Standards and Recommended Practices (SARPs). The ARRB examines both the

[177] The 36th Session of the ICAO Assembly was informed that there are some 150 certified auditors on the USAP roster, from 59 States in all ICAO regions. The participation of certified national experts in the audits under the guidance of an ICAO team leader has permitted the programme to be implemented in a cost-effective manner while allowing for a valuable interchange of expertise.

safety and security histories of specific States and provides an internal advisory forum for coordination among ICAO's safety, security and assistance programmes.

A security culture, if such were to exist among ICAO's member States, would mean that the States would be aware of their rights and duties, and, more importantly, assert them. Those who belong to a security culture also know which conduct would compromises security and they are quick to educate and caution those who, out of ignorance, forgetfulness, or personal weakness, partake in insecure conduct. This security consciousness becomes a "culture" when all the 190 member States as a whole makes security violations socially and morally unacceptable within the group.

A significant issue pertaining to the infusion of a security culture in States is the compelling need to globally curb the financing of terrorism. The United Nations General Assembly, on 9 December 1999, adopted the International Convention for the Suppression of the Financing of Terrorism, aimed at enhancing international co-operation among States in devising and adopting effective measures for the prevention of the financing of terrorism, as well as for its suppression through the prosecution and punishment of its perpetrators.

The Convention, in its Article 2 recognizes that any person who by any means directly or indirectly, unlawfully or wilfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out any act which constitutes an offence under certain named treaties, commits an offence. The treaties listed are those that are already adopted and in force and which address acts of unlawful interference with such activities as deal with air transport and maritime transport. Also cited is the International Convention for the Suppression of Terrorist Bombings, adopted by the General Assembly of the United Nations on 15 December 1997.

The *Convention for the Suppression of the Financing of Terrorism* also provides that, over and above the acts mentioned, providing or collecting funds toward any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in the situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act, would be deemed an offence under the Convention.

Acts of international terrorism that have been committed over the past two decades are too numerous to mention. Suffice it to say, that the most deleterious effect of the offense is that it exacerbates international relations and endangers international security. From the isolated incidents of the 1960s, international terrorism has progressed to becoming a concentrated assault on nations and organizations that are usually susceptible to political conflict, although politics is not always the motivation of the international terrorist. International terrorism has been recognized to engulf acts of aggression by one State on another as well as by an individual or a group of individuals of one State on another State. The former typifies such acts as invasion, while the latter relates to such individual acts of violence as hijacking and the murder of civilians in isolated instances. In both

instances, the duties of the offender-State have been emphatically recognized. Such duties are to condemn such acts and take necessary action.

The United Nations has given effect to this principle in 1970 when it proclaimed that:

> Every State has the duty to refrain from organizing or encouraging the organization of irregular forces or armed bands, including mercenaries, for incursion into the territory of another State. Every State has the duty to refrain from organizing, instigating, assisting or participating in acts of civil strife or terrorist acts in another State or acquiescing in organized activities within its territory directed towards the commission of such acts, when the acts referred to in the present paragraph involve a threat or use of force.

The most pragmatic approach to the problem lies in identifying the parameters of the offense of international terrorism and seeking a solution to the various categories of the offense. To obtain a precise definition would be unwise, if not impossible. Once the offense and its parasitic qualities are clearly identified, it would become necessary to discuss briefly its harmful effects on the international community. It is only then that a solution can be discussed that would obviate the fear and apprehension we suffer in the face of this threat.

Finally on this subject, it must be said that in building a security culture within ICAO member States it is imperative that consideration should also be given to the development of a process for ensuring that all Member States are notified when deficiencies identified during the course of a USAP audit remain unaddressed for a sustained period of time. A notification process could involve the use of information which does not divulge specific vulnerabilities but enables States to initiate consultations with the State of interest to ensure the continued protection of aviation assets on a bilateral basis. Such a notification process may result in a strengthened ability on the part of ICAO to ensure that States unwilling to meet basic security standards will be held accountable and allow for a limited amount of transparency in the security audit programme without divulging specific potential security vulnerabilities.

3.3.4.2 Sharing Information

Assembly Resolution A 35–1 (adopted at the 35th Session of the ICAO Assembly in Montreal in September/October 2004),[178] calls upon ICAO member States to study the ways and means to reinforce the prevention of terrorist attacks by means of explosives, in particular by enhancing international cooperation and information exchange in developing technical means of detection of explosives, giving increased attention to the detection of explosive devices on the human body.

[178] Resolving Clause 4. See Assembly Resolutions in Force (as of 28 September 2007), Doc 9902, at 1–44.

The Passenger Name Record

One category of information in this regard is the Passenger Name Record (PNR).[179] The Passenger Name Record (PNR) is a subject that has been under intense scrutiny by the Council of ICAO, which has developed PNR Data Guidelines that have been transmitted to Contracting States for their comments[180] This exercise was carried out on the understanding that, in the present context of the compelling need for the enhancement of aviation security, the global aviation community has shown an increased interest[181] in adding the PNR data as a security measure in addition to the already existing Advanced Passenger Information (API)[182] and the Machine Readable Travel Document (MRTD), which, although primarily are facilitation tools, greatly assist States authorities in ensuring border security.

A new Recommended Practice concerning the PNR data was included in Annex 9 to the Chicago Convention (Facilitation) after being adopted by the ICAO Council in March 2005.[183] This Recommended Practice, which supplements an already existing Recommended Practice[184] provides that Contracting States requiring

[179] The air transport industry regards a *Passenger Name Record* (PNR), as a generic term applicable to records created by aircraft operators or their authorized agents for each journey booked by or on behalf of any passenger. The data is used by operators for their own commercial and operational purposes in providing air transportation services. The definition applicable in the United States identifies a PNR as a repository of information that air carriers would need to make available upon request under existing regulations and refers to reservation information contained in a carrier's electronic computer reservation system.

[180] See Attachment to State Letter EC 6/2-05/70, Passenger Name Record (PNR) data, 9 June 2005.

[181] The advantage of collection by States of PNR Data was first discussed by the global aviation community at the Twelfth Session of the ICAO Facilitation Division that was held in Cairo, Egypt from 22 March to 1 April 2004. Consequently, the Division adopted Recommendation B/5, that reads as follows:

"It is recommended that ICAO develop guidance material for those States that may require access to Passenger Name Record (PNR) data to supplement identification data received through an API system, including guidelines for distribution, use and storage of data and a composite list of data elements [that] may be transferred between the operator and the receiving State."

Pursuant to this recommendation, In June 2004, the Air Transport Committee of the ICAO Council requested the Secretary General to establish a Secretariat Study Group to develop Guidelines on PNR data transfer. The Council, in endorsing Recommendation B/5, directed that these Guidelines were to be submitted early in 2005.

[182] See, Abeyratne (2002a). Also by the same author, Abeyratne (2001), and also by Abeyratne (2003).

[183] Recommended Practice 3.48 which provides: "Contracting States requiring Passenger Name Record (PNR) access should conform their data requirements and their handling of such data to guidelines developed by ICAO".

[184] Recommended Practice 3.47, which provides inter alia that Contracting States should, where appropriate, should introduce a system of advance passenger information which capture certain passport and visa information prior to departure, for onward transmission to relevant public authorities by electronic means.

Passenger Name Record (PNR) access should conform their data requirements and their handling of such data to guidelines developed by ICAO. It is worthy of note that Article 13 of the Chicago Convention provides that the laws and regulations of a Contracting State as to the admission to or departure from its territory of passengers, crew or cargo of aircraft, such as regulations relating to entry, clearance, immigration, passports, customs, and quarantine shall be complied with, by or on behalf of such passengers, crew or cargo upon entrance into or departure from, or while within the territory of that State. This provision gives a State the discretion to specify the information it requires relating to persons wishing to gain entry into its territory. Accordingly, a State may require aircraft operators operating flights to, from or in transit through airports within its territory to provide its public authorities, upon request, with information on passengers such as PNR data.

The philosophy underlying the importance of PNR data and their efficient use by States for enhanced expediency in border crossing by persons is embodied in the General Principles set out in Chapter 1 of Annex 9 which require Contracting States to take necessary measures to ensure that: the time required for the accomplishment of border controls in respect of persons is kept to the minimum[185]; the application of administrative and control requirements causes minimum inconvenience; exchange of relevant information between Contracting States, operators and airports is fostered and promoted to the greatest extent possible; and, optimal levels of security, and compliance with the law, are attained.

Contracting States are also required to develop effective information technology to increase the efficiency and effectiveness of their procedures at airports.[186]

Advance Passenger Information (API)

The API process requires the carrier to capture passport details prior to departure and the transmit the details by electronic means to the authorities at destination. By this process, authorities can screen the passengers through their databases with a view to identifying potentially high-risk individuals. In addition to he security

[185] There is an abiding symbiosis between security and facilitation in the field of air transport. While security is of paramount interest to the global aviation community, it must not unduly disrupt or in any adversely affect the expediency of air transport. To this end, Recommended Practice 2.2 of Annex 9 – Facilitation – to the Chicago Convention suggests that Each Contracting State should whenever possible arrange for security controls and procedures to cause a minimum of interference with, or delay to the activities of civil aviation provided the effectiveness of these controls and procedures is not compromised. See McMunn (1996).

[186] It must be noted that Annex 9 specifies that the provisions of the Annex shall not preclude the application of national legislation with regard to aviation security measures or other necessary controls.

advantage, this process also assists in reducing congestion at airports and consequently decreases delays in border control processing.[187]

Some States consider API to be a compelling information tool that enables public authorities to manage a potential threat of unlawful interference with civil aviation and also to expedite clearance on arrival.[188] The implementation of such a system requires a great deal of regulation as it involves data capturing and processing. It has also to be noted that under the Chicago Convention, a State has the right to request information in order for proper border control to be established.[189] Therefore, this is a matter of national policy which is further buttressed by the concept of sovereignty of nations.[190]

The United States is arguably one of the most active jurisdictions in adopting recent legislation with regard to airline passengers carried into the territory of a State. On 19 November 2001, The President signed into law the *Aviation and Transportation Security Act* which added on a new requirement that each carrier, foreign and domestic, operating a passenger flight involving foreign air transportation into the United States, must transmit to the US Customs electronically and in advance of the arrival of the flight, a related passenger manifest and crew manifest containing certain specifically required information of such persons. Following this law, the Customs authorities of the United States published an interim rule[191] in the Federal Register on 31 December 2001 which requires air carriers, for each flight subject to the *Aviation and Transportation Security Act*, to transmit to Customs, by means of an electronic data interchange system approved by Customs, a passenger manifest and, by way of a separate transmission, using the same system, a crew manifest.

---

[187] "[. . .] This technique is beginning to be used by Border Control Agencies and it has the potential to reduce considerably the inconvenience and delay experienced by some travelers due to border controls." Facilitation Division-Eleventh Session, (1995) ICAO Doc FAL/11-IP/2.

[188] Refer to Recommendation Practice 3.34 of Annex 9: "Where appropriate Contracting States should introduce a system of advanced passenger information which involves the capture of certain passport or visa details prior to departure, the transmission of the details by electronic means to public authorities, and the analysis of such data for risk management purposes prior to arrival in order to expedite clearance. To minimize handling time during check-in, document reading devices should be used to capture the information in machine readable travel documents. When specifying the identifying information on passengers to be transmitted, Contracting States should only require information that is found in the machine readable zones of passports and visas that comply with the specifications contained in Doc 9303 (series), Machine Readable Travel Documents. All information required should conform to specifications for UN/EDIFACT PAXLST message formats.

[189] Chicago Convention-Art. 13: "The laws and regulations of a contracting State as to the admission to or departure from its territory of passengers, crew or cargo of aircraft, such as the regulations relating to entry, clearance, immigration, passports, customs, and quarantine shall be complied with by or on behalf of such passengers, crew or cargo upon entrance into or departure from, or while within the territory of that State."

[190] Chicago Convention-Art. 1: "The contracting States recognize that every State has complete and exclusive sovereignty over the airspace above its territory."

[191] 66 FR 67482.

The Passenger Name Record (PNR) information so required must electronically provide Customs with access to any and all PNR data elements concerning the identity and travel plans of the passenger to any flight in foreign air transportation to and from the United States, to the extent that the carrier in fact possesses the required data elements in its reservation system and/or departure control system.

On Section 402 of The United States *Enhanced Border Security and Visa Entry Reform Act of 2002* amends section 231 of the Immigration and Nationality Act by providing that for each commercial vessel or aircraft transporting any person to any seaport or airport of the United States. . .it shall be the duty of an appropriate official. . .to provide. . .manifest information about each passenger, crew member, and other occupant transported on such vessel or aircraft prior to arrival at that port. This new provision admits of the valid use of advance passenger information (API) to determine the admissibility of a person to the United States as well as the admissibility of a person as a passenger in an aircraft. The provision details the type of information that may be required. Section 231 is amended in (f) which states that no operator of any private or public carrier that is under a duty to provide information shall be granted papers until the requirements of the provision are complied with. Sub section (g) prescribes penalties to be imposed on carriers who do not comply with the requirement of providing information to the authorities.

The significance of these requirements to the carrier's right in refusing a passenger boarding is that such requirements may impose upon the carrier the added responsibility of being doubly vigilant as to the safety of flights performed by the carrier into the United States. It is therefore evident that the above legislation imposes an obligation on air carriers in the United States to be vigilant and aware of persons they have contracted to carry.

The No Fly List

A vexed issue that flight 253 brought to bear is the effectiveness of "no fly" lists which contain names of persons who are considered a threat to aviation should they travel by air. These lists are maintained by individual States (and not by Organizations such as ICAO) where such States effectively preclude the travel of a potentially dangerous passenger. This is a matter purely for the State concerned as the prerogative of admitting a person to its territory lies exclusively on the State. However, the maintenance of a no fly list is not a fool proof measure as there have been occasions (such as when an 8 year old boy who shared the same name with a suspect on a no fly list was patted down by Customs authorities every time he travelled).[192]

[192] http://www.cbsnews.com/stories/2006/10/05/60minutes/main2066624.shtml. A "false positive" occurs when a passenger who is not on the No Fly List has a name that matches or is similar to a name on the list. Such a passenger will not be allowed to board a flight unless they can differentiate themselves from the actual person on the list – usually by showing a middle name or date of birth. In some cases, false positive passengers have been denied boarding or have missed flights because they could not easily prove that they were not the person on the No Fly List.

A potentially dangerous passenger can be identified either by spontaneous offensive conduct at the pre-boarding stage, a name-match or by criminal profiling, which is an investigative technique based on knowledge of the human personality and various psychological disorders that afflict the human being. However, a no fly list in particular may well raise the issue of privacy, particularly in instances of the false positive. The data subject, like any other person, has an inherent right to his privacy. The subject of privacy has been identified as an intriguing and emotive one.[193] The right to privacy is inherent in the right to liberty, and is the most comprehensive of rights and the right most valued by civilized man.[194] This right is susceptible to being eroded, as modern technology is capable of easily recording and storing dossiers on every man, woman and child in the world.[195] The data subject's right to privacy, when applied to the context of the machine readable travel document (MRTD) is brought into focus by Alan Westin who says:

> Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information is communicated to others.[196]

Legally speaking, there are three rights of privacy relating to the storage and use of personal data:

1. The right of an individual to determine what information about oneself to share with others, and to control the disclosure of personal data;
2. The right of an individual to know what data is disclosed, and what data is collected and where such is stored when the data in question pertains to that individual; the right to dispute incomplete or inaccurate data; and
3. The right of people who have a legitimate right to know in order to maintain the health and safety of society and to monitor and evaluate the activities of government.[197]

It is incontrovertible therefore that the data subject has a right to decide what information about oneself to share with others and more importantly, to know what data is collected about him. This right is balanced by the right of a society to collect data about individuals that belong to it so that the orderly running of government is ensured.

The role played by technology in modern day commercial transactions has affected a large number of activities pertaining to human interaction. The emergence of the information superhighway and the concomitant evolution of automation have inevitably transformed the social and personal life styles and value systems of individuals,

---

[193] Young (1978).

[194] Warren and Brandies (1890–1891).

[195] As far back as in 1973 it was claimed that ten reels, each containing 1,500 m of tape 2.5 cm wide, could store a twenty page dossier on every man, woman, and child in the world. See Jones (1973).

[196] Westin (1970).

[197] Hoffman (1980).

created unexpected business opportunities, reduced operating costs, accelerated transaction times, facilitated accessibility to communications, shortened distances, and removed bureaucratic formalities.[198] Progress notwithstanding, technology has bestowed on humanity its corollaries in the nature of automated mechanisms, devices, features, and procedures which intrude into personal lives of individuals. For instance, when a credit card is used, it is possible to track purchases, discovering numerous aspects about that particular individual, including, food inclination, leisure activities, and consumer credit behaviour.[199] In similar vein, computer records of an air carrier's reservation system may give out details of the passenger's travel preferences, inter alia, seat selection, destination fondness, ticket purchasing dossier, lodging keenness, temporary address and telephone contacts, attendance at theatres and sport activities, and whether the passenger travels alone or with someone else.[200] This scheme of things may well give the outward perception of surveillance attributable to computer devices monitoring individuals' most intimate activities and preferences, leading to the formation of a genuine "traceable society".[201]

The above notwithstanding, it must be borne in mind that privacy is not an absolute, unlimited right that operates and applies in isolation.[202] It is not an absolute right, applied unreservedly, to the exclusion of other rights. Hence there is frequently the necessity to balance privacy rights with other conflictive rights, such as the freedom of speech and the right to access information when examining individuals' rights *vis-à-vis* the interest of society.[203] This multiplicity of interests

[198] See generally Orwell (1984).

[199] For a detailed analysis of the implications of credit cards with respect to the right of privacy see Nock (1993).

[200] The paramount importance of airline computer reservation system records is reflected in the world-renowned cases *Libyan Arab Jamahiriya* v. *United Kingdom* and *Libyan Arab Jamahiriya* v. *United States of America* regarding the PANAM 103 accident at Lockerbie, Scotland in 1988, where the International Court of Justice requested air carriers to submit to the Court the defendants' flight information and reservation details. See International Court of Justice. News Release 99/36, "Questions of Interpretation and Application of the 1971 Montreal Convention arising from the Aerial Incident at Lockerbie" (1 July 1999), online: http://www.icj-cij.org/icjwww/idocket/iluk/iluk2frame.html (date accessed: 14 July 2000). In a similar vein, Arthur R. Miller describes the significance of airline computer reservation system records when dealing with federal, state, local, and other types of investigations where these dossiers could provide valuable information. See also Miller (1971).

[201] See Scott (1995), Burnham (1983). *A contrario* to the argument supported in this thesis that the advancement of technology directly affects the intimacy of individuals. U.S. Circuit Judge Richard Posner favours the idea that other factors, such as urbanisation, income, and mobility development have particularly weakened the information control that, for instance, the government has over individuals: this denotes that individuals' privacy has increased. See Posner (1978).

[202] See Simmel (1971).

[203] See Halpin (1997). See also Foschio (1990). For a comprehensive study on the conflictive interest on privacy and the mass media and the Freedom of Speech, see Pember (1972), Prowda (1995). See also J. Montgomery Curtis Memorial Seminar (1992).

will prompt courts to adopt a balanced approach when adjudicating on a person's rights, particularly when the interests of his own State are involved.

A perceived inadequacy of the global framework of aviation security is the lack of an implementation arm. ICAO has taken extensive measures to introduce relevant international conventions as well as Standards and Recommended Practices (SARPs) in Annex 17 to the Chicago Convention. There is also a highly classified *Aviation Security Manual* developed by ICAO which is provided to States. Additionally, the Organization provides focused security training courses to its member States. However, ICAO's role is largely confined to rule making and the provision of guidance, bringing to bear the need for an aviation security crisis management team on a global scale that could work towards effectively precluding acts of terrorism.

3.4 Suppressing the Financing of Terrorism

Suppressing the financing of terrorism is a major measure against terrorism. However it is just one of the many tools in a conglomeration of connected measures that goes toward combating terrorism. Therefore, any study of the financing of terrorism and the fight against it would not be complete with an analysis of the collective counter-terrorism measures to be used in combating the problem. This article discusses the subject of suppressing the financing of terrorism against the backdrop of the offence of terrorism and its related issues.

The United Nations General Assembly, on 9 December 1999, adopted the *International Convention for the Suppression of the Financing of Terrorism*,[204] aimed at enhancing international co-operation among States in devising and adopting effective measures for the prevention of the financing of terrorism, as well as for its suppression through the prosecution and punishment of its perpetrators.

[204] http://www.un.org/law/cod/finterr.htm. On 26 October 2001 President George W. Bush signed the USA Patriot Act (the contrived acronym for "PATRIOT" being *Providing Appropriate Tools Required to Intercept and Obstruct Terrorism*) and the full title being *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*. The Act empowered law enforcement agencies to search telephone, e-mail communications, medical, financial, and other records; eases restrictions on foreign intelligence gathering within the United States. It also extended the powers of the Secretary of State to regulate financial transactions, particularly those involving foreign individuals and entities; and the discretion of law enforcement and immigration authorities in detaining and deporting immigrants suspected of terrorism-related acts. A significant feature of this legislation was its extended coverage that included domestic terrorism.

The Convention, in its Article 2 recognizes that any person who by any means directly or indirectly, unlawfully or wilfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out any act which constitutes an offence under certain named treaties, commits an offence. The treaties[205] listed are those that are already adopted and in force and which address acts of unlawful interference with such activities as deal with air transport and maritime transport. Also cited is the International Convention for the Suppression of Terrorist Bombings,[206] adopted by the General Assembly of the United Nations on 15 December 1997.

The Convention for the Suppression of the Financing of Terrorism also provides that, over and above the acts mentioned, providing or collecting funds toward any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in the situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act, would be deemed an offence under the Convention.[207]

The use of the word "terrorism" in the title of the Convention brings to bear the need to examine in greater detail both the etymology and the connotations of the word in modern parlance. The term "terrorism" is seemingly of French origin and is believed to have been first used in 1798. "Terrorism", which originally had connotations of criminality to one's conduct, is now generally considered a system of coercive intimidation brought about by the infliction of terror or fear. The most frustrating obstacle to the control of unlawful acts against international peace is the paucity of clear definition of the offence itself. Many attempts at defining the offence have often resulted in the offence being shrouded in political or national barriers.

---

[205] Convention for the Suppression of Unlawful Seizure of Aircraft, done at The Hague on 16 December 1970; Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, done at Montreal on 23 September 1971; Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents, adopted by the General Assembly of the United Nations on 14 December 1973; International Convention against the Taking of Hostages, adopted by the General Assembly of the United Nations on 17 December 1979; Convention on the Physical Protection of Nuclear Material, adopted at Vienna on 3 March 1980; 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, done at Montreal on 24 February 1988; Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, done at Rome on 10 March 1988; 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 International Convention for the Suppression of Terrorist Bombings, adopted by the General Assembly of the United Nations on 15 December 1997

[206] United Nations General Assembly A/52/653, 25 November 1997. See http://www.un.org/law/cod/terroris.htm.

[207] Article 2 b).

In 1980 the Central Intelligence Agency of the United States of America adopted a definition of terrorism which read:

> Terrorism is the threat or use of violence for political purposes by individuals or groups, whether acting for or in opposition to established governmental authority, when such actions are intended to shock, stun or intimidate victims. Terrorism, has involved groups seeking to overthrow specific regimes, to rectify perceived national or group grievances, or to undermine international order as an end in itself.[208]

This all embracing definition underscores the misapprehension that certain groups which are etched in history such as the French Resistance of Nazi occupied France during World War 11 and the Contras in Nicaragua would broadly fall within the definitive parameters of terrorism. In fact, this formula labels every act of violence as being "terrorist" engulfing in its broad spectrum such diverse groups as the Seikigunha of Japan and the Mujahedeen of Afghanistan, although their aims, modus operandi and ideologies are different. James Adams prefers a narrower definition which reads:

> a terrorist is an individual or member of a group that wishes to achieve political ends using violent means, often at the cost of casualties to innocent civilians and with the support of only a minority of the people they claim to represent.[209]

Even this definition although narrower than the 1980 definition cited above is not sufficiently comprehensive to cover for instance the terrorist who hijacks an air plane for his own personal gain. The difficulty in defining the term seems to lie in its association with political aims of the terrorist as is found in the definition that terrorism is really:

> terror inspired by violence, containing an international element that is committed by individuals or groups against non-combatants, civilians, States or internationally protected persons or entities in order to achieve political ends.[210]

The offence of terrorism has also been defined as one caused by:

> . . .any serious act of violence or threat thereof by an individual. Whether acting alone or in association with other persons which is directed against internationally protected persons, organizations, places, transportation or communication systems or against members of the general public for the purpose of intimidating such persons, causing injury to or the death of such persons, disrupting the activities of such international organizations, of causing loss,

---

[208] The CIA website states: The Intelligence Community is guided by the definition of terrorism contained in Title 22 of the US Code, Section 2656f(d):

- The term "terrorism" means premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents.
- The term "international terrorism" means terrorism involving the territory or the citizens of more than one country.
- The term "terrorist group" means any group that practices, or has significant subgroups that practice, international terrorism. See https://www.cia.gov/news-information/cia-the-war-on-terrorism/terrorism-faqs.html.

[209] Adams (1989).

[210] Silets (1987); see also Lee (2005).

> detriment or damage to such places or property, or of interfering with such transportation and communications systems in order to undermine friendly relations among States or among the nationals of different States or to extort concessions from States.[211]

It is time that terrorism is recognised as an offence that is *sui generis* and one that is not always international in nature and motivated by the political aims of the perpetrator. For the moment, if terrorism were to be regarded as the use of fear, subjugation and intimidation to disrupt the normal operations of humanity, a more specific and accurate definition could be sought, once more analysis is carried out on the subject. One must always be mindful however, that without a proper and universally acceptable definition, international cooperation in combating terrorism would be impossible.

A terrorist act is one which is *mala in se* or evil by nature and has been associated with the political repression of the French Revolution era where, it is said, the word terrorism was coined. A terrorist is a *hostis humani generis* or common enemy of humanity.

International terrorism has so far not been defined comprehensively largely due to the fact that owing to its diversity of nature the concept itself has defied precise definition. However, this does not preclude the conclusion that international terrorism involves two factors. They are:

1. The commission of a terrorist act by a terrorist or terrorists; and
2. The "international" element involved in the act or acts in question i.e., that the motivation for the commission of such act or acts or the eventual goal of the terrorist should inextricably be linked with a country other than that in which the act or acts are committed.

Perhaps the oldest paradigm of international terrorism is piracy which has been recognized as an offense against the law of nations and which is seen commonly today in the offense of aerial piracy or hijacking.

Acts of international terrorism that have been committed over the past two decades are too numerous to mention. Suffice it to say, that the most deleterious effect of the offense is that it exacerbates international relations and endangers

---

[211] Nechayev, Serge, Revolutionary Catechism, cited in (Rapoport 1971). Another noteworthy definition was the one that was adopted at the Conference of the International Law Association in Belgrade, 1980 which states:

The definition of "international terrorist offence" presented here is more comprehensive than the definitions which appear in the multilateral convention relating to the control of international terrorism which has been concluded in the past two decades. The term comprehends serious criminal acts, such as murder, assault, arson, kidnapping, extortion, sabotage and the use of explosives devices which are directed towards selected targets. These targets include internationally protected persons, places and international civil aircraft which are already protected under the conventional or customary international law. See. Delaney (1979). See also, The Draft Convention of the International Law Association, Belgrade Conference (Committee on International Terrorism), August 1980, at 9, for definitions of "terrorism" proposed by the Haitian and French delegations at the Conference.

international security. From the isolated incidents of the 1960s, international terrorism has progressed to becoming a concentrated assault on nations and organizations that are usually susceptible to political conflict, although politics is not always the motivation of the international terrorist. International terrorism has been recognized to engulf acts of aggression by one State on another as well as by an individual or a group of individuals of one State on another State. The former typifies such acts as invasion, while the latter relates to such individual acts of violence as hijacking and the murder of civilians in isolated instances. In both instances, the duties of the offender-State have been emphatically recognized. Such duties are to condemn such acts and take necessary action.

The United Nations has given effect to this principle in 1970 when it proclaimed that:

> Every State has the duty to refrain from organizing or encouraging the organization of irregular forces or armed bands, including mercenaries, for incursion into the territory of another State. Every State has the duty to refrain from organizing, instigating, assisting or participating in acts of civil strife or terrorist acts in another State or acquiescing in organized activities within its territory directed towards the commission of such acts, when the acts referred to in the present paragraph involve a threat or use of force.[212]

The most pragmatic approach to the problem lies in identifying the parameters of the offense of international terrorism and seeking a solution to the various categories of the offense. To obtain a precise definition would be unwise, if not impossible. Once the offense and its parasitic qualities are clearly identified, it would become necessary to discuss briefly its harmful effects on the international community. It is only then that a solution can be discussed that would obviate the fear and apprehension we suffer in the face of this threat.

3.4.1 Acts of International Terrorism

It is said that terrorism is a selective use of fear, subjugation and intimidation to disrupt the normal operations of society. Beyond this statement which stands both for national and international terrorism any attempt at a working definition of the words "international terrorism" would entail complications. However, in seeking a solution which would lead to the control of international terrorism it is imperative that contemporaneous instances of the infliction of terror be identified in order that they may be classified either as acts of international terrorism or as mere innocuous acts of self defence. Broadly acts of international terrorism may be categorized into two distinct groups. In the first category may be included what are termed as acts of oppression such as the invasion of one state by another. In the second category are acts which are deviously claimed to be acts of defence. While the former is self

[212] A/52/653, 25 November 1997.

explanatory, the latter – by far the more prolific in modern society – can be identified in four separate forms of manifestation. They are:

(a) Acts claimed to be committed in self defence and in pursuance of self-determination to circumvent oppression;
(b) Nonviolent acts committed internationally which are calculated to sabotage and destroy an established regime;
(c) Random acts of violence committed internationally by an individual or groups of individuals to pressurize a State or a group of individuals to succumb to the demands of terrorists; and
(d) Acts committed internationally which aid and abet national terrorism.

With the exception of the first category of invasion, the others are *prima facie* acts of international terrorism which are essentially extensions of national terrorism. That is to say that most acts of international terrorism are a species of the genus national terrorism.

3.4.1.1 Acts of Defence

Some States claim that internal oppression either by foreign invasion or by an internal totalitarian regime necessitates guerrilla warfare for the achievement of freedom. With more emphasis, it has been claimed that one state must not be allowed to exploit and harass another and that the physical manifestation of desire to attain freedom should not be construed as terrorism. Often, such acts of self defence prove to take extreme violent forms and manifest themselves overseas, thus giving rise to international terrorism. Acts of defence, as they are called, are common forms of international terrorism and are categorized as political violence. These acts take the form of acts of disruption, destruction, injury whose purpose, choice of targets or victims, surrounding circumstances, implementation and/or effects have political significance.

Organized political groups plan strikes and acts of violence internally while extensions of these groups carry out brutal assassinations, kidnapping and cause severe damage to property overseas. The retaliatory process which commences as a token of self defence transcends itself to terroristic violence which is totally ruthless and devoid of moral scruples. Usually, a cause which originates as dedicated to self defence and self determination aligns itself to gaining the support of the people, disarming the military strength of the regime against which it rebels and above all seeks to strengthen itself in order that the terrorist movement attains stability. In this instance terrorist acts seek primarily to carry out a massive propaganda campaign in the international community while at the same time concentrating more on individual instances of terrorism in populated urban areas which attract attention more than those committed in isolated areas. Advertising a cause in the international community becomes an integral part of political terrorism of this nature.

Both the international community and the governments concerned should be mindful that acts of defence can be treated as such only in instances where people

defend themselves when they are attacked and not when retaliatory measures are taken in isolation to instil fear in the international community. To that extent, acts of defence can be differentiated from acts of terrorism.

3.4.1.2 Nonviolent Acts

There are instances where terrorism extends to destabilizing an established regime or a group of persons by the use of threats which are often calculated to instil fear in the international community. Typical examples of this kind of terrorism are the spreading of false propaganda and the invocation of threats which unhinge both the nation or a group of persons against whom the threats are carried out and the nations in which such acts are said to be committed. There have been instances in the past where export consumer commodities of a nation such as food items have been claimed to be poisoned in order that foreign trade between nations be precluded. Although such acts are devoid of actual physical violence, they tend to unhinge the economic stability of a nation particularly if such nation depends solely on the export of the item in question. In such instances, international terrorism assumes proportions of great complexity and succeeds at least temporarily to disrupt the infrastructural equilibrium of the nation against which such threat is aimed. The government concerned is immediately placed on the defensive and attempts counter-propaganda. In spreading propaganda of this nature, the media is the terrorist's best friend. He uses the media of television and radio as a symbolic weapon to instil fear in the public and to cripple the persons or government against which his attack has been aimed. The effect of publicity on people is truly tangible, whether it pertains to the statement of facts or whether it relates to the issuance of threats. Primarily, media terrorism creates an emotional state of apprehension and fear in threatened groups and secondly, draws world attention to the existence of the terrorists and their cause. In both instances, the terrorist succeeds in creating a credibility gap between his target and the rest of the world. Psychological terrorism of this nature is perhaps the most insidious of its kind. It is certainly the most devious.

3.4.1.3 Random Acts of Violence

A random act of violence is normally a corollary to a threat though not necessarily so. Often as it happens, the international community is shocked by a despicable act of mass murder and destruction of property which takes the world completely by surprise. Responsibility for the act is acknowledged later though in many instances no responsibility is claimed. In the latter instance when no responsibility is claimed, the offended nation and the world at large are rendered destitute of an immediate remedy against the offense. Even if motive is imputed to a particular terrorist group, the exercise of sanction becomes difficult as the international community would not condone sanction in the absence of concrete and cogent evidence.

The difficulty lies largely on the fact that any terrorist act is usually carefully planned and executed. Often one observes that the terrorist cautiously retracts his steps obscuring all evidence unless he seeks publicity. The average terrorist is a militant who employs tactics aimed at instilling fear in the minds of the international community. His acts are calculated to instil fright and paralyse the infrastructure of a state by totally exhausting the strength of his target. He further disarms his target by introducing the element of surprise to his attack. Perhaps the most outstanding element of a random attack is the psychological element where excessive and sporadic acts of violence instil both fear and psychological disorientation in a society. This in turn contributes to undermining and weakening a government's authority and control. The disruptive influence that terrorism of this kind exercises over society often creates disharmony within the political circles of a nation and unhinges the psychological behavioural pattern of an organized society. Most often the gap between the citizen and the established government both in the State in which the act is committed and in the state against which the act is committed is widened as the average citizen tends to regard his personal security as the most inviolate of rights that has to be protected by his government.

3.4.1.4 Acts Which Aid and Abet National Terrorism

The fourth facet of international terrorism pertains to acts which promote national terrorism and which are committed outside the State against which the terrorist cause exists. These acts manifest themselves in the maintenance of overseas training camps for terrorists where guerilla warfare, techniques of assassination, destruction and sabotage are taught to terrorist groups who, after sustained training, return to their country and practice what they learn overseas. Such training camps are conducted usually by revolutionary groups and mercenaries on the request of terrorist organizations. A natural corollary to this trend is the collection of funds overseas for the financing of such training programmes, the purchase of arms, ammunition and explosives and the collection of monies involved in meeting the costs incurred by foreign propaganda.

Indirect acts of international terrorism such as those which aid and abet national terrorism indicate clearly that although there is no identifiable definition of the word "terrorism", the word itself can no longer be associated only with violent acts of aggression. In fact, recent studies reflect that any organized campaign of international terrorism involves both direct and indirect acts in equal proportion.

Broadly, international terrorism embitters humanity and antagonizes one nation against another, one human being against another. The eventual consequence of the problem is aggression and even war. The main aim of use of the psychological element by the international terrorist which is by far the most obnoxious and objectionable ambition is to polarize humans and society. However, its immediate manifestation and future development are not without features sufficient to cause grave concern to the world.

Acts of international terrorism, whether in the form of violent or non violent acts have clear and immediate international consequences. They are numerous in nature and warrant a separate study. However, in effect they obtain for the miscreant the same result of creating disharmony and disruption in society. The concept has grown in recent times to portend more serious problems to the international community. Those problems are worthy of comment.

Terrorism has so far not reached the proportions of being an international conspiracy although one group identifies its objectives and purpose with another. We have not had the misfortune of seeing all terrorist groups band together to work as a composite element. This has not happened for the reason that diverse ideologies and religions have kept each group separate. Nevertheless, there is a strong identity bond between groups and even evidence that one helps the other with training and military aid, even though their causes are quite different. The link between terrorist groups is an important consideration for the world as close association between groups could strengthen a weak force and nurture it to maturity. In addition, strong and established terrorist organizations, under cover of burgeoning groups, could carry out campaigns which would cover their tracks and make identification difficult. In most instances, this was found to be true and investigation reveals that a small group, not too significant at that time to take account of, has been responsible for an act or acts whereas later it is revealed that a much stronger group had masterminded the offenses for its benefit. Another important feature of the growing incidence of international terrorism is the assistance the terrorists receive from the advancement of technology in communication, the manufacture of sophisticated weaponry and the proliferation of nuclear armament. In today's context, terrorism has blown to unmanageable proportions with the use of advanced weapons of destruction. Arms control plays a vital role in the control of aggression and it naturally follows that terrorism too benefits from the availability of new modes of aggression. The vulnerability of the international community has been mainly brought upon by the paucity of adequate security measures to prevent nuclear theft. With the growth of the nuclear power industry, developed nations exposed themselves to the vulnerability of theft by power groups, in whose hands nuclear weapons act as threats of destruction. The most effective counter measure that can be taken in this instance against the threat of nuclear theft is to take such effective measures as are necessary to protect the stored items and to make known to the terrorist the high risk involved in an attempt to steal such material. Ideally, any hope of theft must be obviated. This can be achieved by strengthening governmental security.

3.4.1.5 Problems of Deterrence

The only deterrence that would be effective against terrorism of any nature is broadly based on the success of convincing the terrorist that the risk he takes outweighs the benefits which may accrue to his cause by his act. The futility of attempting to wipe out terrorism by the use of military force or the threat of general

sanction on an international level is apparent. The terrorist has to be shown that any attempt at terrorist activity would cause him and his cause more harm than good. Deterrence in this context attains fruition when effective punitive sanctions are prescribed and carried out whilst simultaneously denying the terrorist his demands. In both instances the measures taken should be imperatively effective. It is not sufficient if such measures are merely entered into the statute books of a State or incorporated into international treaty. The international community has to be convinced that such measures are forceful and capable of being carried out.

However, deterrence does not stop at the mere imposition of effective sanction nor does it complete its task by the denial of terrorist demands. Perhaps the most effective method of countering terrorism is psychological warfare. The terrorist himself depends heavily on psychology. His main task is to polarize the people and the establishment. He wants popular support and a sympathetic ear. He wants a lot of people listening and watching, not a lot of people dead. Counter measures taken against a terrorist attack, be it hostage taking, kidnapping or a threat of murder, should essentially include an effective campaign to destroy the terrorist's credibility and sincerity in the eyes of the public. Always, the loyalty of the public should be won over by the target and not by the terrorist. It is only then that the terrorist's risk outweighs the benefits he obtains. To achieve this objective it must be ensured that the terrorist receives publicity detrimental to him, showing the public that if the threatened person, group of persons or State comes to harm, the terrorist alone is responsible. Therefore, the most practical measures that could be adopted to deter the spread of terrorism can be accommodated in two chronological stages:

1. Measures taken before the commission of an offense such as the effective imposition and carrying out of sanctions and the refusal to readily comply with the demands of the terrorist;
2. Measures taken after the commission of the act such as the skilful use of the media to destroy the credibility of the terrorist cause and to convince the people that the responsibility for the act devolves at all stages solely upon the terrorist.

One difficulty in exercising deterrence against terrorism in general and international terrorism in particular is that often, the measures taken are not effective enough to convince the terrorist that in the end, more harm would be caused to him than good. Negotiation with the terrorist in particular has to be done by professionals specially trained for the task. A fortiori, the media has to be handled by specialists with experience. Things would be much more difficult for the terrorist if these were done. The greatest problem of deterrence is the pusillanimity of the international community in the face of terrorism and the feeble response offered by States as a composite body. The reasons for this hesitation on the part of the international community to adopt effective measures against international terrorism are by no means inexplicable. When one state supports a revolutionary cause which is aimed against another, it is quite natural that the terrorist is aware of the support he is capable of obtaining from at least one part of the already polarized world. Therein lies the problem.

3.4.1.6 The Practical Solution

The primary objective of international peace and security is the endeavour to preserve the right to life and liberty. This right is entrenched in Article 3 of the Universal Declaration of Human Rights of 1948 and is accepted today as constituting an obligation on all member States to recognize the legally and morally binding nature of the Declaration. Therefore the destruction of human life and the restriction of liberty are acts committed against international law and order. International terrorism destroys both life and liberty. Indeed there need be no doubt in our minds that international terrorism is illegal. To begin with, there should be more awareness in the world today that every human being has the inherent right to life and that the right is protected by law. Any act of terrorism being illegal, becomes subject to law and its punitive sanctions. However, in this instance, unlike in a simple instance of murder where sanction itself may act as a deterrent, the two forces of law and sanction are not sufficient to curb terrorism. The international community should realize that the solution to terrorism lies rather in its prevention than in its cure. Therefore the problem has to be approached solely on the basis that the terrorist on the one hand has to be dissuaded that his act may not succeed while on the other he has to be persuaded that even if he succeeded in committing the act of terrorism, it would not achieve for him the desired results. The philosophy of warfare against terrorism is therefore based on one single fact – that of convincing the terrorist that any attempt at committing a terrorist act would be fruitless and would entail for him unnecessary harm. This simple philosophy should be adopted gradually in stages with the sustained realization that each measure taken is as important as the next and that all measures should be adopted as a composite element and not as those that are mutually exclusive.

A potential terrorist can therefore be attacked in two ways:

1. By the adoption of practical measures to discourage the commission of the act;
2. By the adoption of such effective measures as would impose severe punitive sanctions if the act is committed.

In the first instance measures of self help are imperative. They should be adopted with careful planning and the terrorist should be made aware that the community at large are afforded the full protection of these measures. They are:

a) The establishment of a system of intelligence which would inform the state concerned of an impending terrorist attack;
b) The establishment of counter–terrorism mechanisms which would effectively preclude such catalysts as the collection of arms, ammunition and weaponry;
c) The adoption of such practical measures of self-help and attack as are necessary in an instance of an attack;
d) The existence of the necessary machinery to retain the confidence and sympathy of the public at all times;
e) The persuasion necessary to convince the public that terrorism of any kind is evil and should not be condoned, whatever its cause is.

The second instance is concerned with measures taken in the event a terrorist act is committed. If strongly enforced with unanimity, such measures as the imposition of laws which bind all nations to view terrorist acts as crimes against humanity can be an effective deterrent. A fortiori, sanctions would further discourage the terrorist.

3.4.2 Money Laundering

In theory, the financing of terrorism and money laundering are antithetical in that while the former involves the support of terrorism through the injection of funds the latter involves covering money acquired through acts of criminality in a cloak of legitimacy. In other words money laundering is "the process by which the source and ownership of criminally derived wealth and property is changed to confer on it a perception of legitimacy".[213] From the point of view of the criminal, there seem to be three basic requirements: (a) the need to conceal the true ownership and origin of the proceeds; (b) the need to maintain control of the proceeds; and (c) the need to change the form of the proceeds.[214] However, it is incontrovertible that there is a certain synergy between the two, as one feeds off the other and often the money gained from acts of terrorism are laundered and put back into funding acts of terrorism The enormity and wide-spread nature of money laundering on a global scale is reflected by the fact that the International Monetary Fund has estimated that, during the decade 1999–2009 the aggregate size of money-laundering was anywhere between 2% and 5% of the world's gross domestic product.[215] Just as an example, it is reported that in 2007, the money generated by organized crime in the United Kingdom was 15 billion Pounds Sterling, of which 10 billion was laundered.[216]

The most fundamental measure taken against money laundering is to criminalize it and to adopt legislative and other measures to identify, trace, freeze, seize and confiscate the proceeds of crime. To this the international effort is quite significant, particular concerning concerted action taken by the Financial Action Task Force (FATF), which is an inter-governmental body whose purpose is the development and promotion of national and international policies to combat money laundering

[213] *Money Laundering and the Financing of Terrorism*, Report published by the authority of the House of Lords of England, Volume 1, 22 July 2009. See http://www.coe.int/t/dghl/monitoring/moneyval/activities/UK_Parlrep.pdf.

[214] *Id* at 7. The offences associated with money laundering are: the conversion or transfer of property for the purpose of concealing or disguising its illicit origin or of assisting any person to evade the legal consequences of his actions; the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of criminally derived property; and the acquisition, possession or use of criminally derived property.

[215] Camdessus, Michel, (Managing Director of the IMF), "Money Laundering: the Importance of International Countermeasures", an address to the Plenary Meeting of the Financial Action Task Force on Money Laundering in Paris, 10 February 1998.

[216] Treasury (2007).

and terrorist financing. The FATF is therefore a "policy-making body" created in 1989 that works to generate the necessary political will to bring about legislative and regulatory reforms in these areas.[217] The FATF has recommended that: the 1999 United Nations Convention for the Suppression of the Financing of Terrorism and relevant UN Security Council Resolutions be ratified and implemented; the financing of terrorism, terrorist acts and terrorist organisations be criminalized; terrorist assets be frozen and confiscated; the widest possible assistance be extended to other countries' law enforcement and regulatory authorities for terrorist financing investigations; suspicious transactions related to terrorism be reported; anti-money laundering requirements on alternative remittance systems be imposed; ensure that entities, in particular non-profit organisations, cannot be misused to finance terrorism; and customer identification measures in international and domestic wire transfers be strengthened.

The Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism,[218] signed at Warsaw in December 2005 provides, in Article 2 that each Party shall adopt such legislative and other measures as may be necessary to enable it to confiscate instrumentalities and proceeds or property the value of which corresponds to such proceeds and laundered property. The Convention goes on to say that Parties may provide for mandatory confiscation in respect of offences which are subject to the confiscation regime which may include money laundering, drug trafficking, trafficking in human beings and any other serious offence.[219] Furthermore it is stated in the Convention that each Party shall adopt such legislative or other measures as may be necessary to require that, in respect of a serious offence or offences as defined by national law, an offender demonstrates the origin of alleged proceeds or other property liable to confiscation to the extent that such a requirement is consistent with the principles of its domestic law.[220] There is also provision for each Party to adopt such legislative and other measures as may be necessary to enable it to identify, trace, freeze or seize rapidly property which is liable to confiscation, in order in particular to facilitate the enforcement of a later confiscation.[221] A significant provision of the Convention lies ain Article 5 which states that each Party shall adopt such legislative and other measures as may be necessary to ensure that the measures to freeze, seize and confiscate also encompass: the

[217] http://www.fatf-gafi.org/pages/0,2987,en_32250379_32235720_1_1_1_1_1,00.html. The 34 members of the FATF are: Argentina; Australia; Austria; Belgium; Brazil; Canada; China; Denmark; the European Commission; Finland; France; Germany; Greece; the Gulf Co-operation Council; Hong Kong; Iceland; Ireland; Italy; Japan; Luxembourg; Mexico; the Kingdom of the Netherlands; New Zealand; Norway; Portugal; Russia; Singapore; South Africa; Spain; Sweden; Switzerland; Turkey; the United Kingdom; and the United States.

[218] ***http://conventions.coe.int/Treaty/EN/Treaties/Html/198.htm***

[219] *Article 3.3*.

[220] *Article 3.4*.

[221] *Article 4*.

property into which the proceeds have been transformed or converted; property acquired from legitimate sources, if proceeds have been intermingled, in whole or in part, with such property, up to the assessed value of the intermingled proceeds; and income or other benefits derived from proceeds, from property into which proceeds of crime have been transformed or converted or from property with which proceeds of crime have been intermingled, up to the assessed value of the intermingled proceeds, in the same manner and to the same extent as proceeds.

Cutting off funding and enforcing rigid legislation against the financing of terrorism and implementing such is indeed an effective international measure against terrorism. While some countries have taken effective measures in this regard others are developing legislation.[222] However, for any measure against terrorism, the fundamental and compelling factor is the need to infuse a security culture among nations. A security culture, if such were to exist among States, would mean that the States would be aware of their rights and duties, and, more importantly, assert them. Those who belong to a security culture also know which conduct would compromises security and they are quick to educate and caution those who, out of ignorance, forgetfulness, or personal weakness, partake in insecure conduct. This security consciousness becomes a "culture" when all the States of the world as a whole make security violations socially and morally unacceptable within the group.

With regard to other measures against terrorism, the first step that should be taken to deter terrorism is to be equipped with the expertise to detect a potential threat beforehand and to be prepared for an attack. The next is to intensify security in all susceptible areas, particularly in such places as airports, subway terminals, etc. Surveillance of all people who are seen in such areas as are revealed to be targets of terrorist acts is imperative. There should be more awareness of the threat of terrorist activity particularly in international airports and international bus and train terminals where travel documents should be checked and passengers double checked. Electronic surveillance of passports and other documents have proved to be effective methods of deterrence in this context. Perhaps the most important facet of surveillance is the use of personnel who do not reveal their identity to the public but unobtrusively mingle with the crowds. This category of person can easily detect an irregularity without arousing suspicion and without alarming the common man. It is recommended that together with the armed personnel there should also be trained personnel who in all informality may work together with the security forces in such instances. Another significant requirement is the support of the people. The media should be made maximum use of to educate the common man as to how to react in an emergency and also to be totally distrustful of the terrorist whose acts are

[222] For a list of countries and a discussion see http://www.iss.co.za/pubs/Other/ahsi/Goredema_Botha/pt2chap12.pdf.

calculated to evoke sympathy. The State or persons against whom the terrorist attack is launched should, at all times, use the media to convince the public that responsibility for any destruction or harm resulting from a terrorist act devolves totally on the terrorist.

3.5 Civil Unrest and Aviation

What started on 17 December 2010 with an act of self immolation by Mohammed Bouazizi, a 26-year-old man trying to support his family by selling fruits and vegetables in the central town of Sidi Bouzid in Tunisia, led to massive protests in the country, resulting in the overthrow of Zine El Abidine Ben Ali, the country's president on 14 January 2011. On 25 January 2011, protests, at least partly inspired by the toppling of the authoritarian government in Tunisia, erupted in Egypt[223] and grew increasingly worse. As a result, Hosni Mubarak, President of Egypt, was deposed within weeks of a virulent peoples' uprising. Contemporaneous protests went on other States such as in Algeria, Yemen, and Bahrain, the last of which held a "day of rage" on February 14, instigated by youths, and inspired by events in Egypt and Tunisia. Furthermore, at the time of writing, there was acute unrest in Libya as a result of mass civil unrest.[224]

In the context of the Libyan crisis, many airlines adopted a cautious approach in planning their flights to Libya while others cancelled scheduled flights.[225] Stocks of European airlines rapidly declined and airlines such as British Airways and KLM cancelled their flight to Tripoli.[226] An inevitable corollary to intensifying violence in Libya, which is a large oil supplier to Europe, would be that airlines will be forced to charge higher fares. IATA observed that if the unrest were to continue in the various countries in the Middle East and North Africa, airlines would be forced

[223] Tourism and transport combined forms the largest industry in the world. Air transport is a significant driver of tourism and visitors arriving by air directly support approximately 6.7 million jobs worldwide in the tourism industry with the foreign exchange they spend during their travels. Both the tourism industry and air transport industry depend on the policies of governments and the individual stability of States for their sustenance and development. The unrest wrought by mass protests in North Africa and the Middle East in 2011 seriously disrupted tourism and air transport. Tourism earned Egypt more than 11 billion dollars in the last fiscal year. In the third quarter of 2010, Egypt was receiving about 280 million US dollars a week from tourism. See http://www.suite101.com/content/tourism-crisis-as-foreign-visitors-desert-egypt-a342840.

[224] Wikipedia identifies civil unrest with synonyms such as civil disorder, or civil strife, which are broad terms typically used by law enforcement to describe one or more forms of disturbance caused by a group of people.. Examples of civil disorder include, but are not necessarily limited to: illegal parades; sit ins; and other forms of obstructions; and other forms of crime. http://en.wikipedia.org/wiki/Civil_disorder.

[225] Airlines wary on operating to Libya, *Air Letter*, No. 17,180, Thursday 24 February 2011at p. 3.

[226] *Id.* at p.4.

to stop operating flights into those States, which would definitely result in significant losses to the airlines.[227]

In Libya, the runway at Benghazi airport was destroyed as a result of the continuing clashes between anti-government protesters and security forces.[228] It is reported that protesters against the government of Libya had surrounded the airport and the government of the United Kingdom, among others, was "urgently seeking landing permission from the Libyan Government" for a charter aircraft to airlift stranded British citizens out of the country.[229] The first point of contact of a tourist is the airport and if the airport premises is under severe civil unrest and attack, there will be no tourists visiting that country.

The security of a State is entirely dependent on the level of peace prevailing in its territory and any breach of that security, starting at the entry points to its territory, will also impact on loss of income for the State as the case is with tourism. Most, if not all countries affected by the civil unrest in the Middle East and North Africa are tourist intensive and their income will suffer immensely. Many States issued travel advisories on Tunisia, Egypt and Libya. At the time of the unrest in early 2011, Tunisia was recovering from the devastating effects on its tourism industry brought about by the terrorist attacks of 2001 and 2002 when the country lost a substantial number of tourists from its traditional markets of France, Germany, Italy and the United Kingdom. The 500,000 German tourists lost in the process was a big blow to Tunisia's tourism.[230] With regard to Egypt, hotel capacity increased by approximately 7,000 rooms between 2009 and 2010 to a total of 220,000 hotel rooms. In December 2010 The United Nations World Tourism Organization (UNWTO) increased its collaboration with Egypt in enhancing the country's tourist intake worked closely with Egypt in enhancing its capacity to measure the economic impact of tourism and provide consistent, internationally benchmarked tourism statistics.[231] With such an upsurge in tourism promotion, It is therefore heartening that tourism in Tunisia and Egypt, States that carried out a successful revolution in overthrowing their existing regimes, did not suffer for too long and recovered quickly. UNWTO has expressed its appreciation of proactive efforts by national authorities to restore confidence among tourists and by foreign governments to update travel advisories accordingly. Tourism is a significant contributor to both

[227] Airlines set for losses as mid-east unrest continues, *Air Letter,* No. 17,181, Friday, 25 February 2011at p.3.

[228] Kelly Reals, Runway at Benghazi Airport Destroyed: Capita Symonds, *Air Transport Intelligence News*, 22 February 2011. Seehttp://www.flightglobal.com/articles/2011/02/22/353498/runway-at-libyas-benghazi-airport-destroyed-capita.html.

[229] *Ibid.*

[230] This loss gradually balanced from the new European markets and especially from Poland, Czech Republic and Hungary. See http://www.traveldailynews.com/pages/show_page/23601-Tunisia-unveils-new-tourism-plan.

[231] http://www.ameinfo.com/252453.html.

countries' economies and, as tourism returns to normalcy, overall economic recovery can be stimulated.[232]

As the situation in both Egypt and Tunisian returns to normal, tourism stakeholders from the private and public sectors have reacted accordingly. Major tourism sites are open to the public, airlines have resumed flights, tour operators in many of the main source markets have restarted selling holidays and governments have updated their travel advisories to reflect the unfolding situation.

From an aviation and tourism perspective the unrest in these regions has impelled the markets to respond with oil prices shooting skywards to $119 a barrel for Brent crude. these higher oil prices is highly worrying for airlines. Having retrenched and cut back, airlines were hoping for a return to profitability in 2011 as growth returns following the downturn. However, the latest rise in oil prices could, as IATA forecasts extinguish any airline gains this year, causing a global domino effect on aviation. leaving carriers with heavy losses. Airlines were hoping for a return to profitability in 2011 as growth returns following the downturn.[233]

3.5.1 Keeping Airports Open

To begin with, The 37th Session of the ICAO Assembly of the International Civil Aviation Organization (ICAO)[234] held from 28 September to 10 October 2010 officially recognized that ICAO has three Strategic Objectives: safety, security and environmental protection and sustainability of air transport. The last strategic objective, although relevant to the consequences of civil unrest on air transport by no means impels ICAO to intervene in the internal affairs of States or to ensure that amidst the clash of arms air transport carries on regardless. However, what it does is to draw a nexus between ICAO and the Convention on International Civil

[232] http://www.traveldailynews.com/pages/show_page/41810-UNWTO-welcomes-signs-of-tourism-recuperation-in-Egypt-and-Tunisia.

[233] http://www.aerosocietychannel.com/aerospace-insight/2011/02/shifting-sands/.

[234] The International Civil Aviation Organization, a specialized agency of the United Nations, was established by Article 44 of the *Convention on International Civil Aviation* (Chicago Convention), signed at Chicago on 7 December 1944 (*infra*, note 12). The main objectives of ICAO are to develop the principles and techniques of international air navigation and to foster the planning and development of air transport. ICAO has 190 Contracting States. ICAO's Mission and Vision Statement is "to achieve its mission of safe, secure and sustainable development of civil aviation through cooperation amongst its member States". In December 2004, following a decision by the 35th Session of the ICAO Assembly, the Council of ICAO approved six Strategic Objectives for 2005–2010: They were: safety; security; environmental protection; efficiency; continuity; and rule of law. From 2011, ICAO's Strategic Objectives will be based on safety; security; environmental protection and the sustainable development of air transport. However, during the 37th Session of the Assembly, the Strategic Objectives were reduced to three: safety; security; environmental protection and sustainable development of air transport.

Aviation (Chicago Convention)[235] which provides inter alia that an aim of ICAO is to foster the planning and development of international air transport so as to meet the needs of the peoples of the world for safe, regular, efficient and economical air transport.[236]

The Chicago Convention requires States to keep their airports open to all airlines operating into and out of their territories and provide meteorological, radio and other information as well as facilities such as ground services. Of course, one might argue that Article 89 of the Chicago Convention enables Contracting States to have freedom of action irrespective of the provisions of the Convention in case of war, whether belligerents or neutrals. It also allows a State which has declared a state of national emergency (and notifies the ICAO Council of such) to have the same freedom of action notwithstanding the provisions of the Convention. Therefore, unless a State is at war (which the Convention does not define)[237] or has declared a state of national emergency, it would be bound by the provisions of the Convention.

The first duty of a Contracting State not falling within the purview of Article 89 of the Chicago Convention is to keep its airport open to all incoming aircraft. Article 15 of the Convention requires inter alia that, uniform conditions shall apply to the use, by aircraft of every contracting State, of all air navigation facilities, including radio and meteorological services, which may be provided for public use for the safety and expedition of air navigation. This condition is subject to Article 9 which stipulates that each contracting State may, for reasons of military necessity or public safety, restrict or prohibit uniformly the aircraft of other States from flying over certain areas of its territory, provided that no distinction in this respect is made between the aircraft of the State whose territory is involved, engaged in international scheduled airline services, and the aircraft of the other contracting States likewise engaged. The provision goes on to say that Each contracting State reserves also the right, in exceptional circumstances or during a period of emergency, or in the interest of public safety, and with immediate effect, temporarily to restrict or prohibit flying over the whole or any part of its territory, on condition that such restriction or prohibition will be applicable without distinction of nationality to aircraft of all other States.

The question arises as to whether a State in which there is acute civil unrest is bound to follow the abovementioned principles of the Chicago Convention. States or international organizations which are parties to such treaties have to apply the

[235] Signed at Chicago on 7 December 1944. See ICAO Doc 7300 9th Edition: 2006.

[236] *Id.* Article 44 d).

[237] Article 31.1 of the *Vienna Convention on the Law of Treatie* provides that "a treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose". See *Vienna Convention on the Law of Treaties 1969*, done at Vienna on 23 May 1969. The Convention entered into force on 27 January 1980. United Nations, *Treaty Series*, vol. 1155, p. 331. The ordinary meaning of war can be considered as a behavior pattern of organized violent conflict typified by extreme aggression, societal disruption, and high mortality. This behavior pattern involves two or more organized groups. http://en.wikipedia.org/wiki/War.

treaties they have signed and therefore have to interpret them. Although the conclusion of a treaty is generally governed by international customary law to accord with accepted rules and practices of national constitutional law of the signatory States, the application of treaties are governed by principles of international law. If however, the application or performance of a requirement in an international treaty poses problems to a State, the constitutional law of that State would be applied by courts of that State to settle the problem. Although Article 27 of the *Vienna Convention*[238] requires States not to invoke provisions of their internal laws as justification for failure to comply with the provisions of a treaty, States are free to choose the means of implementation they see fit according to their traditions and political organization.[239] The overriding rule is that treaties are juristic acts and have to be performed.

3.5.2 Airport and Aviation Security

The biggest threat to security in the vicinity of the airport, where aircraft landing and takeoff are at their lowest altitude, is Man Portable Air Defence Systems (MANPADS). Since the events of 11 September 2001, there have been several attempts against the security of aircraft in flight through the misuse of Man Portable Air Defense Systems (MANPADS).[240] The threat of MANPADS to aviation security is by far the most ominous and the international aviation community has made some efforts through ICAO. MANPADS have posed a serious threat to aviation security. On 5 January 1974, 220 soldiers and 200 police sealed off five square miles around Heathrow International airport in London after receiving reports that terrorists had smuggled SA-7s into Britain in the diplomatic pouches of Middle-Eastern embassies and were planning to shoot down an El Al airliner.[241]

Another significant incident occurred on 13 January 1975 when an attempt by terrorists to shoot down an El Al plane with a missile was believed to have brought civil aviation to the brink of disaster. Two terrorists drove their car onto the apron at Orly airport, where they set up a rocket launcher and fired at an El Al airliner which was about to take off for New York with 136 passengers. The first round missed the target thanks to the pilot's evasive action and hit the fuselage of a Yugoslav DC-9 aeroplane waiting nearby to embark passengers for Zagreb. The rocket failed to

[238] *Id.*

[239] Reuter (1989).

[240] The use of SAMs and anti-tank rockets by terrorists goes back to 1973. On 5 September 1973 Italian police arrested five Middle-Eastern terrorists armed with SA-7s. The terrorists had rented an apartment under the flight path to Rome Fumicino Airport and were planning to shoot down an El Al airliner coming in to land at the airport. See Dobson and Payne (1987).

[241] Mickolus (1980).

explode and no serious casualties were reported. After firing again and hitting an administration building, which caused some damage, the terrorists escaped by car? A phone call from an individual claiming responsibility for the attack was received at Reuters. The caller clearly implied that there would be another such operation, saying 'Next time we will hit the target'.

In fact, 6 days later another dramatic though unsuccessful attempt did occur at Orly airport. The French authorities traced the attack to the PFLP Venezuelan terrorist, and leader of the PFLP group in Europe, Carlos.[242] It is also known that once again an El Al airliner had been deliberately chosen as a target by Gadafi in an attempt to avenge the loss of the Libyan airliner shot down by Israel over the Sinai Desert.[243]

MANPADS are extremely effective weapons which are prolific in their availability worldwide. The significance of the abuse of MANPADS as a threat to civil aviation in the airport context is that MANPADS could be used in the vicinity of the perimeter of the airport or in the airport premises itself in view of the short range needed to hit an aircraft approaching an airport or departing from one. Introduced in the 1950s and originally meant to deter terror attacks from air to ground to be used by State authorities and other protection agencies, these weapons have got into the wrong hands and are being used against civil and military aviation. The surface to air MANPAD is a light weapon which offers very little warning before impact, and is often destructive and lethal.[244] They are cheap, easily carried, handled and concealed. It is claimed that there are at least 100,000 and possibly in excess of 500,000 systems in inventories around the world and several thousands of these are vulnerable to theft from State authorities.[245] It is also claimed that there is a 70% chance that a civil aircraft will be destroyed if hit by a MANPAD.[246] A study conducted and published in early 2005 by the Rand Corporation concludes that, based on the effects of the attacks of September 11 2001, it is plausible for air travel in the United States to fall by 15–20% after a successful MANPADS attack on a commercial airliner in the United States.[247] The international aviation community is aware that civil aircraft are particularly vulnerable to hand held ground to air missiles and that susceptibility avoidance techniques (calculated to avoid being hit) and vulnerability avoidance (survival after being hit) systems must be in place. This is particularly so since tracking the

[242] Christopher Dobson and Ronald Payne, *supra*, p. 53.

[243] . *Ibid*.

[244] The lethality of the weapon can be reflected by the 340 MANPADS used by Afghan Mujaheden rebels to successfully hit 269 soviet aircraft. See http://www.janes.com/security/international_security/news/.

[245] MANPADS, *Ploughshares Monitor* Autumn 2004, at 83.

[246] *Ibid*. The deadly accuracy and ease of handling of MANPADS were demonstrated when Somali gunmen shot down two US MH-60 Black Hawk helicopters in October 1993.

[247] Infrastructure Safety and the Environment, *Protecting Commercial Aviation against the Shoulder-Fired Missile Threat*, Rand Corporation, 2005, at 9.

proliferation of MANPADS is difficult since any intelligence gathered on this particular threat is usually ex post facto, through the recovery of launchers or fragments from expended missiles. Contrary to popular belief, the MANPAD is considerably durable and can be used several years after inactivity, with recharged batteries.

The World's attention to the deadly threat posed by MANPADS was further drawn in November 2002 when there was an unsuccessful attempt to bring down a civilian aircraft leaving Mombasa, Kenya. Over the past 35 years, significant developments have taken place in dangerous weapons systems creating more opportunities for terrorists. The ready acceptance of new modern technologies by the international community and our growing dependence on them have created many targets, such as nuclear and civil aircraft in flight. Similarly, developments in electronics and microelectronics, and the trend towards miniaturization and simplification have resulted in a greater availability of tactical weapons with longer ranges and more accuracy that are also simpler to operate. One of the most effective developments in individual weaponry is portable, precision-guided munitions (PGMs), which are lightweight and easy to operate. They can usually be carried and operated by a single person. The United States-made Stinger, the British-made Blowpipe and the Russian-made SA-7 missiles are examples of these smaller weapons. These are shoulder-fired, anti-aircraft missiles that have infra-red, heat-seeking sensors in the projectile that guide it to the heat emitted from an aircraft engine. It is known that more than 60 States possess SA-7 missiles and there is no doubt that most of them maintain strict security measures to prevent the outflow of the weapons. However, it has been alleged that some States, including Libya, have supplied PGMs to terrorist organizations. It is incontrovertible that in the hands of terrorists these missiles are not likely to be used against conventional targets such as tanks and military fighter aircraft. Of particular concern is the prospect of civilian airliners being shot at by SAMs and anti-tank rockets as they land at or take off from airports[248] Dr. Richard Clutterbuck subsumes the great threat of missile attacks:

> Recent years have seen increasing use of expensive and sophisticated surface-to-surface and surface-to-air missiles (SSM and SAM) by terrorists, generally of Russian or East European origin and redirected by Arab Governments, notably Colonel Gadafi's. Continuing development of these weapons for use by regular armies will ensure that new and more efficient versions will become available for terrorists.[249]

With increased airport security, the possibility of placing explosive devices on civil aircraft is becoming more difficult, but now the same destructive result can be achieved far more easily by using modern missiles or rockets.

Perimeter security at the airport is a vital element in ensuring security of the airport itself as well as the security of incoming and outgoing aircraft. For a successful missile attack against aircraft, the firing position has to be located within range of the

[248] Hanle (1989), Ofri (1984), Pierre (1975–1976), Dorey (1983).

[249] Clutterbuck (1991).

flight path. A missile's guidance system is such that the weapon has to be fired within a few degrees of the flight path if the infra-red guidance is to locate the target. Accordingly, a possible preventive measure would be to prevent terrorists from getting into a firing position with their missiles. However, it would be very difficult to cut off areas of up to 6 km wide that lie in the paths of aircraft as they land and take off. This measure is therefore impracticable if not impossible.[250] This difficulty can be overcome to an extent by patrolling the outer areas of airports in times of stringent security conditions might prevent such attacks. Even in times when no specific threat has been received, it is within the capacity of most States to monitor those strips of land from which a SAM could be launched and thus minimize the risk. At the same time, these security operations would deter terrorists from spending vital resources on buying SAMs given the limited possibilities for their use.

Although the success rate so far of Western States in preventing terrorist missile attacks against civil aviation is satisfactory, and security forces, with the help of good intelligence, have been successful in tracking down and capturing missiles before they could be used, it is not unlikely that there will be attempts to use surface-to-air missiles to attack civil aviation in the near future. As some targets are becoming more difficult for terrorists to attack it can be anticipated that they will make efforts to overcome the enhanced security systems as well as redirecting their efforts towards less secure targets. The displacement of the increasingly ineffective system of hijacking by missile attacks against civil aviation is a real threat.

Another aspect in securing aviation in times of civil unrest is diplomacy and the meaning and purpose of aviation as interpreted by the founding fathers of the Chicago Convention. Given its strategic objective on sustanbility of air transport and its compelling diplomatic role which ICAO has played over the past 66 years with aplomb and competence, member States of ICAO could well consider the role of aviation in bringing about peace. The importance of aviation toward maintaining peace has been accepted since World War 2 and is aptly reflected in the Statement of the British at that time, that civil aviation holds the key to power and importance of a nation and therefore it must be regulated or controlled by international authority. Lord Beaverbrook for the British Government of that time stated in Parliament:

> Our first concern will be to gain general acceptance of certain broad principles whereby civil aviation can be made into a benign influence for welding the nations of the world together into a closer cooperation. . .it will be our aim to make civil aviation a guarantee of international solidarity, a mainstay of world peace.[251]

The intensely political overtones that moulded the incipient civil aviation system of the world immediately after the War, thereby incontrovertibly establishing the relevance of diplomacy, international politics and international relations in civil aviation, is borne out by the statement of the first President of the ICAO Council, Edward Warner, when he said:

[250] Dorey (1983).

[251] *Flight,* Vol. XLV No. 1331, January 27, 1944, at pp. 97–98.

> It is well that we should be reminded. . .if the extent of the part which diplomatic and military considerations have played in international air transport, even in periods of undisturbed peace. We shall have a false idea of air transport's history, and a very false view of the problems of planning its future, if we think of it purely as a commercial enterprise, or neglect the extent to which political considerations have been controlling in shaping its course.[252]

In retrospect, it must be noted that this statement is a true reflection of what civil aviation stood for at that time, and, more importantly, that the statement has weathered the passage of time and is true even in the present context. A more recent commentator correctly observes that over the past decades, civil aviation has had to serve the political and economic interests of States and that, in this regard, ICAO has alternated between two positions, in its unobtrusive diplomatic role and its more pronounced regulatory role.[253]

> An inherent characteristic of aviation is its ability to forge inroads into human affairs and promote international discourse. It also promotes international goodwill and develops "a feeling of brotherhood among the peoples of the world".[254] Therefore, it has been claimed that problems of international civil aviation constitute an integral part of the universal political problems of world organization and therefore aviation problems cannot be solved without involving the world political and diplomatic machinery.[255] It is at these crossroads that one encounters the profound involvement of the United Nations mechanism in general and ICAO in particular.

As for ICAO, the Organization has acted in the past on non-aviation issues which were related to the need to ensure peace. At its various sessions the ICAO Assembly has addressed instances of social injustice such as racial discrimination as well as threats to commercial expediency achieved through civil aviation. The 15th session of the ICAO Assembly adopted Resolution A15-7 (Condemnation of the Policies of Apartheid and Racial Discrimination of South Africa) where the Resolution urged South Africa to comply with the aims and objectives of the Chicago Convention, on the basis that the apartheid policies constitute a permanent source of conflict between the nations and peoples of the world and that the policies of apartheid and racial discrimination are a flagrant violation of the principles enshrined in the Preamble to the Chicago Convention.[256]

The Preamble[257] was also quoted in Resolution A17-1 (Declaration by the Assembly) which requested concerted action on the part of States towards

---

[252] Warner (1942).

[253] Sochor (1991).

[254] Schenkman (1955).

[255] *Id.* Vi.

[256] See *Repertory Guide to the Convention on International Civil Aviation,* Second Edition, 1977, Preamble – 1.This subject was also addressed at a later session of the Assembly when the Assembly, at its 18th Session adopted Resolution A18-4 (Measures to be taken in pursuance of Resolutions 2555 and 2704 of the United Nations General Assembly in Relation to South Africa).

[257] The Preamble to the Chicago Convention states., inter alia, that the future development of international civil aviation can greatly help to create and preserve friendship and understanding

suppressing all acts which jeopardize safety and orderly development of international civil aviation. In Resolution A20-2 (Acts of Unlawful Interference with Civil Aviation) the Assembly reiterated its confidence that the development of international civil aviation can be an effective tool in bringing about friendship and understanding among the peoples of the world.

These discussions would suggest that civil unrest, as it affects aviation, and aviation, as it affects the sustenance of peace are two sides of the same coin.

3.5.2.1 The Beijing Convention of 2010

Aviation is an important global business and a significant driver of the global economy. It is vital, therefore, that stringent measures are taken to counter acts of unlawful interference with civil aviation. Following a diplomatic conference, held in Beijing from 30 August to 10 September 2010 under the auspices of the International Civil Aviation Organization, representatives from more than 80 States adopted two international air law instruments for the suppression of unlawful acts relating to civil aviation. The two instruments are the *Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation* and the *Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft*. This discussion will only be on the Beijing Convention.

The Beijing Convention (See the full text in the **APPENDIX**) serves international civil aviation well, by requiring parties to criminalize a number of new and emerging threats to the safety of civil aviation, including using aircraft as a weapon and organizing, directing and financing acts of terrorism. These new treaties reflect the international community's shared effort to prevent acts of terrorism against civil aviation and to prosecute and punish those who would commit them. The treaties promote cooperation between States while emphasizing the human rights and fair treatment of terrorist suspects. The Convention also obligates States to criminalize the transport of biological, chemical, nuclear weapons and related material.

Many provisions of the Convention, which is a newcomer to aviation security in the context of some new provisions it introduces, may need reflection, particularly in interpreting the intent of its founding fathers.

Under the auspices of ICAO, a diplomatic conference, held in Beijing from 30 August to 10 September 2010, composed of representatives from more than 80 States,[258] adopted two international air law instruments for the suppression of unlawful acts relating to civil aviation.

---

among the nations and peoples of the world, yet its abuse can become a threat to the general security; and It is desirable to avoid friction and to promote that cooperation between nations and peoples upon which the peace of the world depends.

[258] Some 400 participants from more than 80 States and international organizations attended the Conference. The Conference unanimously elected Mr. XIA Xinghua from China as the President, and Mr. Terry Olson from France as the First-Vice President.

The two instruments adopted by the Diplomatic Conference are the *Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation* and the *Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft*. This article will only discuss the former instrument.

Since the 1960s, a number of treaties on aviation security have been concluded under the auspices of ICAO.[259] These legal instruments criminalize acts against international civil aviation, such as hijacking and sabotage, and facilitate the cooperation between States to make sure that such acts do not go unpunished. The treaties adopted in Beijing further criminalize the act of using civil aircraft as a weapon, and of using dangerous materials to attack aircraft or other targets on the ground. The unlawful transport of biological, chemical and nuclear weapons and their related material[260] becomes now punishable under the treaties. Moreover, directors and organizers of attacks against aircraft and airports will have no safe haven. Making a threat against civil aviation may also trigger criminal liability. The Convention also implicitly addresses the threat of cyber attacks on aviation, as the discussion to follow will illustrate.

Aviation is an important global business and a significant driver of the global economy. It is vital, therefore, that stringent measures are taken to counter acts of unlawful interference with civil aviation. The *Convention on International Civil Aviation* signed at Chicago on 7 December 1944,[261] states in its *Preamble* that whereas the development of civil aviation may help preserve friendship and understanding among the people of the world, yet, its abuse could become a threat to general security. Therefore, air transport is intrinsically linked to peace and is far

[259] See generally Abeyratne (1998) which discusses extensively the treaties. See also, Abeyratne (2010a).

[260] Abeyratne (2007).

[261] The Convention on International Civil Aviation, signed at Chicago on 7 December 1944 (*supra*, note 1), which is the founding document of commercial aviation, in its Preamble, recognizes that the future development of international civil aviation can greatly help to create and preserve friendship and international understanding among the nations and peoples of the world, yet its abuse can become a threat to the general security; and it is desirable to avoid friction and to promote that cooperation between nations and peoples upon which the entire peace of the world depends. See ICAO Doc 7300/9 Ninth Edition: 2006, *Preamble*. The most significant modernist construction of the role of civil aviation in securing world peace and security comes from language used in the letters of invitation issued by the United States to the participant States to the Chicago Conference that, consequent to the war, the restorative processes of prompt communication may greatly facilitate the return to the processes of peace. However, the conscious awareness of the parties to the Convention, that in securing this peace, prudent economic and business principles must not be compromised, should not be forgotten. See Proceedings *of the International Civil Aviation Conference*, Chicago, Illinois, November 1–7 December 1944, US Department of State Volume 1 at 7.

removed from its antithesis – terrorism – which is usually linked with acts of unlawful interference with civil aviation.

The genealogy of the term "*Terrorism*" lies in Latin terminology meaning "to cause to tremble"(*terrere*). Since the catastrophic events of 11 September 2012, we have seen stringent legal measures taken by the United States to attack terrorism, not just curb it. The famous phrase "war on terror" denotes pre-emptive and preventive strikes carried out through applicable provisions of legitimately adopted provisions of legislation. The earliest example is the *Air Transportation Safety and System Stabilization Act* (ATSAA) enacted by President Bush less than 2 months after the 9/11 attacks. Then, 2 months after the attacks, in November 2001, Congress passed the *Aviation and Transportation Security Act* (ATSA) with a view to improving security and closing the security loopholes which existed on that fateful day in September 2001. The legislation paved the way for a huge federal body called the Transportation Security Administration (TSA) which was established within the Department of Transportation. The *Homeland Security Act of 2002* which followed effected a significant reorganization of the Federal Government.

All this goes to show that the law plays a significant role in ensuring aviation security, and the Beijing instruments play a crucial role in furthering this objective. Since the events of 11 September 2001, there have been several attempts against the security of aircraft in flight. These threats have ranged from shoe bombs to dirty bombs to explosives that can be assembled in flight with liquids, aerosols and gels. In every instance the global community has reacted with preemptive and preventive measures which prohibit any material on board which might seemingly endanger the safety of flight. Some jurisdictions have even gone to extremes in prohibiting human breast milk and prescriptive medications on board.

New and emerging threats to civil aviation are a constant cause for concern to the aviation community. Grave threats such as those posed by the carriage of dangerous pathogens on board, the use of cyber technology calculated to interfere with air navigation systems, and the misuse of man portable air defence systems are real and have to be addressed with vigour and regularity. ICAO has been addressing these threats for some time and continues to do so on a global basis.

The Aviation Security Panel of ICAO met at its 20th Meeting in Montreal from 30 March to 3 April 2009. One of the key areas of discussion at this meeting concerned new and emerging threats to civil aviation. The Panel worked through the Working Group on New and Emerging Threats and noted that significant progress in efforts to proactively identify vulnerabilities and potential gaps in existing measures had been made, that would strengthen *Annex 17* (Aviation Security) to the Convention on International Civil Aviation. At this meeting, the European Civil Aviation Conference (ECAC) stressed the importance of the challenge posed by cyber threats in light of the current lack of related provisions in Annex 17.

Consequently, the Panel considered the threat of cyber attacks, and some members stressed that this threat is significant. With reference to a proposal to include a Recommended Practice in Annex 17 to ensure that information and

communication technology systems used for civil aviation purposes be protected from cyber attacks, the Panel agreed that, given the complexity of this issue, which involves air traffic management systems, aircraft design and operations, the matter requires further analysis by the Working Group on New and Emerging Threats prior to inclusion in Annex 17 or any guidance material. Depending on the results of the analysis, the Working Group on Amendment 12 to Annex 17 will develop a proposal for amending the Annex, to be presented to the Panel at its 21st meeting.

The Panel also considered the merits of building unpredictability into the aviation security regime. While concern was expressed regarding the impact of unpredictable security measures on passenger confidence in aviation security, many Panel members supported implementation of the concept because of its value as a deterrent. It was suggested that States adopt an approach providing for a baseline regime, but with the addition of unpredictable measures, thus achieving a balance between certainty and unpredictability. With regard to an amendment to Annex 17 in this regard, the need for introducing unpredictability into the aviation security regime was considered, and it was agreed that unpredictability should be promoted in principle but not prescribed. The Panel suggested that if an Annex 17 specification related to unpredictability were to be developed, it would be necessary to ensure that the introduction of this concept by States does not diminish the level of security or result in delays for passengers. Further, the Panel noted that appropriate guidance material may be required to address the potential negative impact of introducing the concept of unpredictability, and proposed the development of guidance material related to unpredictability prior to the introduction of an amendment to Annex 17.

A Conclusion of the Panel was, inter alia, that the threat of cyber attacks is real and cannot be ignored, and that further analysis by the Working Group on New and Emerging Threats would be appropriate. Another Conclusion was that the ICAO focal point of contact (PoC) Network is an important tool for sharing critical threat information and should be used more effectively, and that the Secretariat should consider the establishment of a web-based community page. Yet another was that the concept of building unpredictability into the aviation security regime is in principle a useful tool, however, concerns expressed regarding the possible impact on the level of security and the impact on passenger confidence should be resolved before its inclusion as a Recommended Practice in Annex 17.

The 37th Session of the ICAO Assembly, which was held from 28 September to 8 October 2010 at ICAO Headquarters in Montréal, built on the achievements of the diplomatic Conference in Beijing in September 2010 by recognizing the need to strengthen aviation security worldwide. In a Declaration on Aviation Security, unanimously adopted by participants, international commitment was reaffirmed to enhance aviation security collaboratively and proactively through screening technologies to detect prohibited articles, strengthening of international standards, improvement of security information-sharing and provision of capacity-building assistance to States in need.

The Assembly also put its full support behind the new ICAO Comprehensive Aviation Security Strategy.

It must be underscored that the following discussion is not meant to criticize a fine treaty that will serve as a landmark against new and emerging threats to civil aviation. Rather, the discourse is meant to be creative and attenuate the logicality behind certain key provisions of the Convention. The author's comments in the Conclusion are mere observations which the drafters of the Convention would undoubtedly have answers to.

Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation

The Beijing Convention has a short Preamble, which sets the tone and theme of the treaty. It recognizes *in limine* that the State Parties to the instrument are deeply concerned that unlawful acts against civil aviation jeopardize the safety and security of persons and property; seriously affect the operation of air services, airports and air navigation; and undermine the confidence of the peoples of the world in the safe and orderly conduct of civil aviation for all States. States Parties also recognize that new types of threats against civil aviation require new concerted efforts and policies of cooperation on the part of States. As such they are convinced that in order to better address these threats, there is an urgent need to strengthen the legal framework for international cooperation in preventing and suppressing unlawful acts against civil aviation.

New Types of Threat

The distinctive feature of this treaty, which makes it stand out from its predecessors, is that it bases itself on responding to new and emergent threats to security. As already mentioned, This subject has its genesis in the ICAO Aviation Security Panel which met at its 20th Meeting in Montreal from 30 March to 3 April 2009. One of the key areas of discussion at this meeting concerned new and emerging threats to civil aviation.

Cyber-terrorism has the advantage of anonymity, which enables the hacker to obviate checkpoints or any physical evidence being traceable to him or her. It is a low budget form of terrorism where the only costs entailed in interfering with the computer programs of an air transport system would be those pertaining to the right computer equipment.

Any interference with air transport, which would be inextricably linked to the purpose of international civil aviation as enunciated in the *Preamble* to the Chicago Convention, which states that the future development of international civil aviation can greatly help to create and preserve friendship and understanding among the nations and people of the world, yet, its abuse can become a threat to the general security.

The leakage of dangerous pathogens[262] from laboratories also presents an ominous analogy to the aviation sector in that the same could well occur in the carriage of such dangerous goods by air. Although past instances of the escape of dangerous pathogens are small in number, nonetheless their occurrence and the threat posed to the wellbeing of humanity cannot be underestimated. In 2002 when Anthrax spores escaped from two military laboratories in the United States, the authorities agreed that the leakage was due to a security lapse.[263] In 2003 a string of such leakages occurred in Asia, this time of the SARS virus.[264]

Offences Under the Convention

The first offence identified by the Convention relates to any person committing an offence if that person unlawfully and intentionally performs an act of violence against a person on board an aircraft in flight if that act is likely to endanger the safety of that aircraft.[265] This offence has three salient elements: the offence has to be committed by a person "on board"[266] an aircraft; the aircraft has to be "in flight"; and the act perpetrated should endanger the safety of the aircraft. According to the Convention, the aircraft is considered to be in flight at any time from the moment when all its external doors are closed following embarkation until the moment when any such door is opened for disembarkation; in the case of a forced landing, the flight shall be deemed to continue until the competent authorities take over the responsibility for the aircraft and for persons and property on board.[267]

---

[262] Pathogens are microorganisms (including bacteria, viruses, rickettsia, parasites, fungi) or recombinant microorganisms (hybrid or mutant) that are known or are reasonably expected to cause infectious disease in humans or animals.

[263] An year earlier, a covert event occurred in October 2001 when anthrax spores were sent through the mail exposing persons in the eastern USA to contaminated mail resulting in deaths, illnesses and identified exposures to Anthrax. Overt, announced events, in which persons are warned that an exposure has occurred, have taken place in the United States, although most of these were determined to have been hoaxes, that is, there were no true exposures to infectious agents.

[264] The leakages occurred in China, Taiwan and Singapore. See Air-Tight Security, *Intersec*, June 2007 33–35 at 34.

[265] *Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation,* done at Beijing on 10 September 2010, Article 1. (a).

[266] The offender has to be physically inside the aircraft. This offence therefore does not *ex facie* apply to an offence committed outside the aircraft. The Convention does not define "on board". However, it must be noted that the term "on board" has been judicially defined in absolute terms to mean that as long as a person is physically in the aircraft, it matters not whether the flight had been terminated or not. See *Herman* v. *Trans World Airlines*, 330 N.Y.S.D. 2nd 829 (Sup.Ct. 1972) where the Court held that although the aircraft in which the passenger was travelling had been hijacked and flown to the desert, and the passenger was kept in the aircraft for several days, he was nonetheless considered to have been on board, irrespective of whether the purpose of the flight had been fulfilled or not. See also *Pfug* v. *Egyptair*, 961F. 2d. 26 (2nd Cir.1992).

[267] *Supra*, note 269, Article 2 (a).

The next consideration within this specific offence is that the act perpetrated should endanger the safety of the aircraft. This seemingly excludes acts of air rage which in many instances only affect the safety of the person against whom the offence is committed. By restricting the offence to safety of the aircraft in flight, the Convention has ensured that every offence under this provision must essentially endanger the safety of the aircraft in which the offence is committed. Undoubtedly the ultimate arbiters of the Convention, which were the ICAO member States, had a reason for adopting this approach and it would be interesting to learn of the rationale of this approach, particularly in the context of a recommendation offered by the ICAO Aviation Security Panel at its 21st Meeting held from 22 to 26 March 2010, where the Panel suggested that the *Secretariat Study Group on Unruly Passengers* be reconvened in order to study the issue of unruly passengers and consider whether the existing international legal regime should be re-examined.

The second offence under the Convention is committed when a person destroys an aircraft in service or causes damage to such an aircraft which renders it incapable of flight or which is likely to endanger its safety in flight.[268] An aircraft is considered to be in service from the beginning of the pre-flight preparation of the aircraft by ground personnel or by the crew for a specific flight until 24 h after any landing; furthermore, the period of service will, in any event, extend for the entire period during which the aircraft is in flight as defined in the Convention.[269] This provision does not seem to cover an act which causes damage to an aircraft but which does not affect the safety of the flight. Therefore, a wilful or wanton act committed by a member of a technical team (for example a maintenance engineer) at pre flight stage, if it damages the aircraft but does not affect the safety of a flight would not, under this provision, be considered an unlawful act relating to international aviation.

The third offence identified by the Convention relates to a person who places or causes to be placed on an aircraft in service, by any means whatsoever, a device or substance which is likely to destroy that aircraft, or to cause damage to it which renders it incapable of flight, or to cause damage to it which is likely to endanger its safety in flight.[270] Here again, the offence must relate to the destruction of the aircraft or damage which renders the aircraft unserviceable, or adversely affects the safety of the aircraft. It is interesting that the Convention does not define the words

[268] Id. Article 1 (b).
[269] *Id*, Article 2 (b).
[270] *Id*, Article 1 (c).

"device"[271] or "substance".[272] It is even more interesting that the Convention did not include the word "weapon" as it has done in a following provision.[273]

The fourth offence is a first for any treaty on unlawful interference with civil aviation. 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.[274] This undoubtedly refers, inter alia to cyber terrorism, but links the offence exclusively to the safety of aircraft in flight. If therefore as a result of an act of cyber terrorism, a taxiing 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 under the Treaty either against the second aircraft or its disembarking passengers.

The Beijing Treaty of 2010 is a step forward in the right direction with the threat of cyber terrorism looming, affecting the peace of nations. Air transport could well be a target towards the erosion of that peace. The maintenance of international peace and security is an important objective of the United Nations,[275] which recognizes one of its purposes as being inter alia:

> To maintain international peace and security, and to that end: take effective collective measures for the prevention and removal of threats to the peace, and for the suppression of acts of aggression or other breaches of peace, and to bring about by peaceful means, and in conformity with the principles of justice and international law, adjustment or settlement of international disputes or situations which might lead to a breach of the peace.[276]

It is clear that the United Nations has recognized the application of the principles of international law as an integral part of maintaining international peace and security and avoiding situations which may lead to a breach of the peace.

---

[271] The free Online Dictionary defines "device" as inter alia a contrivance or an invention serving a particular purpose, especially a machine used to perform one or more relatively simple tasks, or a technique or means, or a plan or scheme, especially a malign one. See http://www.thefreedictionary.com/device.

[272] The free Online Dictionary defines "substance" as that which has mass and occupies space; matter or a material of a particular kind or constitution. See http://www.thefreedictionary.com/substance.

[273] Article 1.2 of the Convention provides that A person commits an offence if that person unlawfully and intentionally, using any device, substance or weapon: (a) performs an act of violence against a person at an airport serving international civil aviation which causes or is likely to cause serious injury or death; or (b) destroys or seriously damages the facilities of an airport serving international civil aviation or aircraft not in service located thereon or disrupts the services of the airport, if such an act endangers or is likely to endanger safety at that airport.

[274] Beijing Convention, *supra*, Article 1 (d).

[275] Charter of the United Nations and Statute of the International Court of Justice, Department of Public Information, United Nations, New York, DPI/511 – 40108 (3–90), 100 M at 1.

[276] *Id.* at 3.

Cyber terrorism would not only affect the security of air transport. One commentator says:

> Cyber-terrorism can be used in many ways. In its simplest form, it can be used as a means of disinformation or psychological warfare by manipulating media attention regarding possible threats, thus causing disruption to airport and aircraft operations. This could result in the reluctance of persons to travel which, in turn, could affect the economies of nations dependent on the movement of air passengers. In its most serious form, cyber-terrorism could lead to fatalities, injuries and major damage at airports and to aircraft in flight.[277]

The particularity of cyber-terrorism is that the threat is enhanced by globalization and the ubiquity of the Internet. It is a global problem in search of a global solution.

The fifth offence identified in the Convention covers an instance where a person communicates information which that person knows to be false, thereby endangering the safety of an aircraft in flight.[278] This seemingly rules out a message communicated negligently, where the purveyor of the message did not bother to find out the veracity of the information he was providing. Furthermore, this provision raises an important issue. One could argue that the exclusivity of "safety in flight" may unduly restrict the scope of this provision. For instance, if a phony telephone call claims that there would be a bomb on board a flight that would be operated the next day, and the air operator cancels that flight incurring an economic loss, there would be no offence as the aircraft in question was not "in flight" as defined in the Convention. This consideration may be particularly relevant in the context of the title of the Treaty which is "*Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation*" which obviously does not restrict itself to safety or security issues. Another consideration is that if such a communication were to come just as the doors of an arriving aircraft are opened for disembarkation and passengers are injured or killed in a stampeded, this provision would not apply.

The sixth offence is a throwback on 9/11 and provides that any person who uses an aircraft in service for the purpose of causing death, serious bodily injury, or serious damage to property or the environment commits an offence.[279] The interesting feature of this provision is that it has included environmental damage that could be caused by such an act. In the maritime context, there are analogous provisions[280] where important safeguards are prescribed when a State Party takes measures against a ship, including boarding. The safeguards include: not

[277] Guill (2000).

[278] Beijing Convention, *supra*, Article 1 (e).

[279] *Id*, Article 1. (f).

[280] Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf adopted 10 March 1988; Entry into force 1 March 1992; 2005 Protocols: Adopted 14 October 2005; Entry into force 28 July 2010.

endangering the safety of life at sea; ensuring that all persons on board are treated in a manner which preserves human dignity and in keeping with human rights law; taking due account of safety and security of the ship and its cargo; ensuring that measures taken are environmentally sound; and taking reasonable efforts to avoid a ship being unduly detained or delayed.[281] *The European Convention on the Protection of the Environment through Criminal Law*[282]calls upon each State Party to adopt such appropriate measures as may be necessary to establish as criminal offences or administrative offences, liable to sanctions or other measures under its domestic law, when committed intentionally or with negligence the unlawful discharge, emission or introduction of a quantity of substances or ionising radiation into air, soil or water.[283]

The next provision[284] makes it an offence to release or discharge from an aircraft in service any BCN[285] weapon or explosive, radioactive, or similar substances in a manner that causes or is likely to cause death, serious bodily injury or serious damage to property or the environment. This provision provides, inter alia a response to bio terrorism, which is a new and emerging threat to civil aviation.[286] A bioterrorism attack is the deliberate release of viruses, bacteria, or other germs (agents) used to cause illness or death in people, animals, or plants. These agents are typically found in nature, but it is possible that they could be changed to increase their ability to cause disease, make them resistant to current medicines, or to increase their ability to be

[281] *Id.* Article 8 bis.

[282] Strasbourg, XI.1998.

[283] *Id.* Article 4.

[284] Beijing Convention, *supra*, Article 1 (g).

[285] According to Article 2 (h) BCN weapons are (a) biological weapons, which are: (i) microbial or other biological agents, or toxins whatever their origin or method of production, of types and in quantities that have no justification for prophylactic, protective or other peaceful purposes; or (ii) weapons, equipment or means of delivery designed to use such agents or toxins for hostile purposes or in armed conflict. (b) "chemical weapons", which are, together or separately: toxic chemicals and their precursors, except where intended for: (A) industrial, agricultural, research, medical, pharmaceutical or other peaceful purposes; or (B) protective purposes, namely those purposes directly related to protection against toxic chemicals and to protection against chemical weapons; or (C) military purposes not connected with the use of chemical weapons and not dependent on the use of the toxic properties of chemicals as a method of warfare; or (D) law enforcement including domestic riot control purposes, as long as the types and quantities are consistent with such purposes; munitions and devices specifically designed to cause death or other harm through the toxic properties of those toxic chemicals which would be released as a result of the employment of such munitions and devices; any equipment specifically designed for use directly in connection with the employment of munitions and devices and nuclear weapons and other nuclear explosive devices.

[286] A Special Sub Committee of the Legal Committee of ICAO met in Montreal from 3 to 6 July 2007 to discuss the preparation of one or more instruments addressing new and emerging threats. One of the issues addressed at this meeting was the unlawful transport of biological, chemical, nuclear weapons and other dangerous substances on board aircraft.

spread into the environment. Biological agents can be spread through the air, through water, or in food. Terrorists may use biological agents because they can be extremely difficult to detect and do not cause illness for several hours to several days. While some bioterrorism agents, such as the smallpox virus, can be spread from person to person some agents such as anthrax are incapable of doing so.

There have been several noteworthy instances of bioterrorism in the past[287] as early as 1915,[288] which send an ominous message that it is a distinct possibility in the aviation context. Until recently in the United States of America, most biological defence strategies have been geared to protecting soldiers on the battlefield rather than looking after ordinary people in cities. In 1999, the University of Pittsburgh's Center for Biomedical Informatics deployed the first automated bioterrorism detection system, called RODS (Real-Time Outbreak Disease Surveillance). RODS is designed to draw collect data from many data sources and use them to perform signal detection, that is, to detect a possible bioterrorism event at the earliest possible moment. RODS, and other similar systems, collect data from sources including clinical data, laboratory data, and data from over-the-counter drug sales. In 2000, Michael Wagner, the co director of the RODS laboratory, and Ron Aryel, a subcontractor, conceived of the idea of obtaining live data feeds from "non-traditional" (non-health-care) data sources. The RODS laboratory's first efforts eventually led to the establishment of the National Retail Data Monitor, a system which collects data from 20,000 retail locations nation-wide.

Another noteworthy provision[289] to follow states that where it is an offence to perform an act of violence against a person at an airport serving international civil aviation which causes or is likely to cause serious injury or death; or to destroy or seriously damage the facilities of an airport serving international civil aviation or aircraft not in service located thereon or disrupts the services of the airport, if such an act endangers or is likely to endanger safety at that airport. It is quite curious that an attack against an airport, to be classified under this Convention has to endanger safety *at* the airport and does not include safety *of* the airport. Therefore the

[287] In 1984 followers of the Bhagwan Shree Rajneesh attempted to control a local election by incapacitating the local population by infecting salad bars in eleven restaurants, doorknobs, produce in grocery stores and other public domains with Salmonellas typhimurium in the city of The Dalles, Oregon. The attack caused about 751 people to get sick (there were no fatalities). This incident was the first known bioterrorist attack in the United States in the twentieth century. In September and October of 2001, several cases of anthrax broke out in the United States which were reportedly caused deliberately. This was a well-publicized act of bioterrorism. It motivated efforts to define biodefense and biosecurity.

[288] In 1915 and 1916, Dr Anton Dilger, a German-American physician used cultures of anthrax and glanders with the intention of committing biological sabotage on behalf of the German government. Other German agents are known to have undertaken similar sabotage efforts during World War I in Norway, Spain, Romania and Argentina.

[289] Beijing Convention, *supra*, Article 1.2.

provision seems to imply that any wanton damage to an airport or its infrastructure; insofar as it does not affect the safety of persons would not be an offence.

Other provisions follow, which address threats to commit the offences discussed above[290] and attempts to commit such offences[291] and make them offences under the Convention. An interesting provision is contained in Article 3 of the Convention which states that each State Party undertakes to make the offences discussed above punishable by severe penalties. Here, the key word is "undertakes". It is worthy of note that the drafters have not used the word "shall" which would have made the requirement peremptory. In regular parlance "undertake" would mean to "accept as a challenge or promise to do or accomplish or enter upon an activity or enterprise"[292] Another definition of "undertake" is "to agree to be responsible for a job or project and do it".[293] Therefore, logically, one could argue that Article 3 makes States Parties promise that they would make offences under the Convention punishable. On the other hand, the word "shall" would have made the requirement obligatory.

This logicality notwithstanding, one should consider this conundrum in its legal perspective. Article 31.1 of the *Vienna Convention on the Law of Treaties*[294] provides that "a treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose". One has therefore to inquire as to what the ordinary meaning is that was given to the word "undertake" by the drafters of the Beijing Convention.

The Convention does not apply to military, customs or police services. In the absence of a definition of these services, one could seek guidance from the Chicago Convention which denies its application to State aircraft and goes onto to say that aircraft used in military, customs and police services shall be deemed to be State aircraft.[295]

In the face of the use of the word "undertakes" in Article 3 as discussed, one notices that Article 8.1 on the issue of jurisdiction provides that each State Party *shall* (author's emphasis) take such measures as may be necessary to establish its jurisdiction over the offences discussed above: (a) when the offence is committed in the territory of that State; (b) when the offence is committed against or on board an aircraft registered in that State; (c) when the aircraft on board which the offence is

[290] *Id*, Article 1. 3.

[291] *Id.* Article 1.4.

[292] http://www.audioenglish.net/dictionary/undertake.htm.

[293] http://www.macmillandictionary.com/dictionary/american/undertake.

[294] *Vienna Convention on the Law of Treaties 1969*, done at Vienna on 23 May 1969. The Convention entered into force on 27 January 1980. United Nations, *Treaty Series*, vol. 1155, p. 331.

[295] Chicago Convention, *Supra*, note 3, Article 3. a) and b). For a clear and compelling discussion on the interpretation of the terms state aircraft and military, customs and police aircraft see Michael Milde, *International Air Law and ICAO*, Eleven Publishing: Utrecht, 2008 at 69–71.

committed lands in its territory with the alleged offender still on board; (d) when the offence is committed against or on board an aircraft leased without crew to a lessee whose principal place of business or, if the lessee has no such place of business, whose permanent residence is in that State; (e) when the offence is committed by a national of that State. Each State Party may also establish its jurisdiction over any such offence when the offence is committed against a national of that State; or when the offence is committed by a stateless person whose habitual residence is in the territory of that State.[296]

With regard to extradition of offenders, the Convention obligates (again with the word "shall") the State Party in the territory of which the alleged offender is found if it does not extradite that person, without exception whatsoever and whether or not the offence was committed in its territory, to submit the case to its competent authorities for the purpose of prosecution. Those authorities are required to take their decision in the same manner as in the case of any ordinary offence of a serious nature under the law of that State.[297]

It is incontrovertible that, given the various innovative terrorist acts perpetrated against civil aviation, the Beijing Treaty of 2010 is a proactive and timely initiative of both ICAO and the international civil aviation community. In this regard it must be noted that this treaty was adopted, as are other treaties, by State Parties to the Beijing Conference and ICAO was the initiator and facilitator of the Conference. Therefore, one could assume that whatever the treaty provides is in accord with and responds to the needs of the member States of ICAO.

Firstly, one is struck by the title of the Convention, which is *Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation*. Therefore, one is to take it that the purpose of the treaty is to suppress unlawful acts relating to civil aviation. Yet, it is incontrovertible that this is an instrument exclusively addressing aviation security, although the word "security" is not used in the document. It is mainly concerned with the safety of aircraft in service or aircraft in flight, with one provision on safety pertaining to airports. Excluded from its purview are such unlawful acts as negligent entrustment which is now an unlawful and criminal act in the United Kingdom and Scotland which many common law countries may follow.[298] Also excluded from the purview of the Convention is any unlawful act calculated to cancel flights causing economic loss to air carriers. The Convention, in all practicality therefore remains one that is adopted to suppress unlawful acts relating to the safety of international civil aviation.

Secondly, one would observe that the Convention does not cover all instances of air rage although all such acts are unlawful acts relating to international civil aviation. Furthermore, the almost exclusive insistence on safety of "aircraft in flight" and the narrow definition of "in flight" as contained in the Convention

[296] Beijing Convention, *supra*, Article 8.2.

[297] *Id.* Article 10.

[298] Abeyratne (2010b).

may not cover every instance of air transport operated by a carrier when passengers are still on board an aircraft.

The above notwithstanding, the Beijing Convention serves international civil aviation well, by requiring parties to criminalize a number of new and emerging threats to the safety of civil aviation, including using aircraft as a weapon and organizing, directing and financing acts of terrorism. This new treaty reflects the international community's shared effort to prevent acts of terrorism against civil aviation and to prosecute and punish those who would commit them. The treaty promotes cooperation between States while emphasizing the human rights and fair treatment of terrorist suspects.

The Convention also obligates States to criminalize the transport of biological, chemical, nuclear weapons and related material. The provisions in the treaty reflect the nexus between non-proliferation and terrorism and ensure that the international community will act to combat both. This treaty also strengthens global efforts to ensure that these extraordinarily dangerous materials will not be transported via civil aircraft for illicit purposes and, if such attempts are made, those responsible will be held accountable under the law.

Under the circumstances, this landmark treaty leaves no room for doubt that it is a valuable contribution towards the enhancement of collaboration between States to curb unlawful acts against international civil aviation. The abovementioned features of the Beijing Treaty undoubtedly makes it a timely and proactive initiative of ICAO and the international aviation community.

Finally, it must be mentioned that treaties of this nature, although essential and innovative, merely offer an ex post facto response to aviation security. They should be accommodated by proactive measures such as one suggested by the ICAO AVSEC Panel at its 21st Meeting in March 2010: that there should be more innovative identification of passengers. Undoubtedly, this recommendation could be extended to employees and others coming into contact with aircraft and airports.

3.5.2.2 Extraordinary Rendition

Extraordinary rendition is the handing over of a person from one jurisdiction to another, without initial determination as to the possibility of that person's guilt.[299] A stronger definition is:

> The alleged acts of the U.S. authorities in the wake of "911" when suspected high-value terrorists were – without trial-abducted/arrested ("snatched" in the media jargon) in one territory and transported by aircraft to another territory for interrogation by US agents or

[299] In contrast, a rendition flight is a flight which takes a felon to a place which has jurisdiction to adjudicate the crime in question. rendition is therefore a legal measure and has its genesis in the need for the US to recapture fugitive slaves. See Article 4, Section 2, Clause 2 of the United States Constitution.

> delivered to security forces in other countries where they would not enjoy the protection against torture or other abuses.[300]

It is reported that the application and significance of this practice had a change of focus in the 1980s when foreign delinquents were transferred by United States authorities to be interrogated in countries with which the United States did not have extradition treaties, which in turn carried the connotation that such delinquents would be treated differently than they would have been in countries of the west.[301] From a conceptual standpoint, extraordinary rendition is diametrically at variance with principles of international law, which has certain safeguards against the transportation of a person against his will, unless a proper judicial determination has been made in favour of such a transfer. Protocol No. 7 to the *Convention for the Protection of Human Rights and Fundamental Freedoms*,[302] provides that an alien lawfully resident in the territory of a State shall not be expelled therefrom except in pursuance of a decision reached in accordance with law and shall be allowed: (a) to submit reasons against his expulsion, (b) to have his case reviewed, and (c) to be represented before the competent authority or a person or persons designated by that authority.[303] An alien may be expelled before the exercise of his rights, when such expulsion is necessary in the interests of public order or is grounded on reasons of national security.[304] Furthermore, Article 13 of the *International Covenant on Civil and Political Rights* (ICCPR)[305] provides that an alien lawfully in the territory of a State Party may be expelled therefrom only in pursuance of a decision reached in accordance with law and shall, except where compelling reasons of national security otherwise require, be allowed to submit the reasons against his expulsion and to have his case reviewed by, and be represented before the competent authority or a person or persons especially designated by the competent authority.[306]

---

[300] Milde (2008). Consistent with this definition, Wikipedia states that some journalists have called extraordinary rendition "*torture by proxy*". See http://en.wikipedia.org/wiki/Extraordinary_rendition.

[301] Ingrid Detter Francopan, Extraordinary Rendition and the Law of War, North Carolina Journal of International Law and Commercial Regulation, Summer 2008 (33 N.C.J. Int'lL. &Com. Reg). 657 at 659.

[302] *Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocol No. 1Rome, 4.XI.1950. The text of the Convention had been amended according to the provisions of Protocol No. 3 (ETS No. 45), which entered into force on 21 September 1970, of Protocol No. 5 (ETS No. 55), which entered into force on 20 December 1971 and of Protocol No. 8 (ETS No. 118), which entered into force on 1 January 1990, and comprised also the text of Protocol No. 2 (ETS No. 44) which, in accordance with Article 5, paragraph 3 thereof, had been an integral part of the Convention since its entry into force on 21 September 1970.*

[303] Art. 1, Nov. 22, 1984, Eur. T.S. No. 117. Article 1, titled *"Procedural safeguards relating to expulsion of aliens.*

[304] *Ibid.*

[305] International Covenant on Civil and Political Rights, adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966, (*entered into force* on 23 March 1976, in accordance with Article 49).

[306] International Covenant on Civil and Political Rights Art. 13, opened for signature Dec. 16, 1966, 999 U.N.T.S. 171.

The *Third Geneva Convention on Prisoners of War of 1949*[307] stipulates that, in the case of armed conflict not of an international character occurring in the territory of one of the High Contracting Parties, each Party to the conflict shall be bound to apply, as a minimum, that persons taking no active part in the hostilities, including members of armed forces who have laid down their arms and those placed hors de combat by sickness, wounds, detention, or any other cause, shall in all circumstances be treated humanely, without any adverse distinction founded on race, colour, religion or faith, sex, birth or wealth, or any other similar criteria. To this end the Convention prohibits: violence to life and person, in particular murder of all kinds, mutilation, cruel treatment and torture; taking of hostages; outrages upon personal dignity, in particular, humiliating and degrading treatment; the passing of sentences and the carrying out of executions without previous judgment pronounced by a regularly constituted court affording all the judicial guarantees which are recognized as indispensable by civilized peoples. The Convention also provides that the wounded and sick shall be collected and cared for. It also provides that an impartial humanitarian body, such as the International Committee of the Red Cross, may offer its services to the Parties to the conflict. In the case of *Hamdan* v. *Rumsfeld*[308] the decision of the Supreme Court suggests that all activities carried out in the "war on terror" of the United States must pass the minimum standards set out in the Convention.[309]

The above notwithstanding, there are at least three controversial cases where the rendition of the victims by air have been questionable.[310] This brings to bear two areas of concern: false arrest and imprisonment; and the significance of the role of air transport and its meaning and purpose in the backdrop of circumstances of war.

False Arrest and Imprisonment

False arrest is unlawful or unjustifiable arrest and is committed where a person unlawfully, intentionally or recklessly restrains another's freedom of movement from a particular place.[311] Physical detention is an essential ingredient for grounding an action in false imprisonment. Thus if a person agrees to go to a police station voluntarily, he has not been arrested even though the person taking him would have arrested him on refusal to go.[312]

The *Fourth Amendment* to the U.S. Constitution stipulates that unless there is probable cause, a person could not be subject to a search warrant or arrest. A good

[307] Convention (III) relative to the Treatment of Prisoners of War. Geneva, 12 August 1949.

[308] 126S.Ct.2749 (2006).

[309] *Id.* 2794–97.

[310] Sattertwaite (2007).

[311] Smith and Hogan (1992). See also *Rahman* v. *Queen* (1985) 81 Cr App Rep 349 at 353.

[312] *Campbell* v. *Tormey* (1969) 1 All E.R. 961, cited in Smith & Hogan, *Criminal Law*, *op.cit.* at 432.

example of probable cause is the 1967 case of *Terry* v. *Ohio*,[313] which arose from an arrest stemming from a policeman becoming suspicious of two men when one of them walked up the street, peered into a store, walked on, started back, looked into the same store, and then conferred with his companion. The other suspect repeated this ritual, and between them the two men went through this performance about a dozen times before following a third man up the street. The officer, thinking they were preparing to commit a misdemeanour and might therefore be armed, confronted the men, asked their names and patted them down, thereby discovering pistols the plaintiff and his companion. In affirming Terry's conviction for carrying a concealed weapon, the Supreme Court concluded that where a police officer observes unusual conduct which leads him reasonably to conclude in light of his experience that criminal activity may ensue and that the person with whom he is dealing may be armed and presently dangerous, where in the course of investigating this behavior he identifies himself as a policeman and makes reasonable inquiries, he is entitled for the protection of himself and others in the area to conduct a carefully limited search of the outer clothing of such persons in an attempt to discover weapons which might be used to assault him. Physical detention is an essential ingredient for grounding an action in false imprisonment. Thus if a person agrees to go to a police station voluntarily, he has not been arrested even though the person taking him would have arrested him on refusal to go.[314]

The law provides that where an arresting officer has reasonable grounds for suspecting that an arrestable offence has been committed, he may arrest without a warrant anyone whom he has reasonable grounds for suspecting to be guilty of that offence.[315] The offence of false imprisonment is one of "basic intent" and despite the paucity of authority as to whether the element of *mens rea* is necessary to constitute the offence of false imprisonment,[316] at least one decision[317] has recognized the requirement.

In the early case of *Christy* v. *Leachinsky*[318] Lord Simonds, while observing that it was the right of every citizen to be free from arrest and that he should be entitled to resist arrest unless that arrest is lawful, concluded that a person cannot be arrested unless he knows why he is being arrested.[319] This principle has however, since been replaced by Section 28 of the *Police and Criminal Evidence Act* 1984 which provides that where a person is arrested, otherwise than being informed that he is under arrest, he must be so informed as soon as practicable afterwards. While this

[313] 392 U.S. 1 (1968), argued 12 Dec. 1967, decided 10 June 1968

[314] *Campbell* v. *Tormey* (1969) 1 All E.R. 961, cited in Smith & Hogan, *Criminal Law*, *op.cit*. at 432.

[315] *Police and Criminal Evidence Act* 1984 Section 24 (6).

[316] False imprisonment is generally considered under civil actions where the element of mens rea is not relevant.

[317] *Re Hutchins* (1988) *Crim L R* 379.

[318] (1947) 1 *All E.R*. 567.

[319] *Id*. at 575.

provision holds incontrovertible the fact that a person who is arrested has to be informed of the grounds for his arrest, it dispenses with the exclusive need to inform the person at the time of arrest.[320]

In the more recent case of *Murray* v. *Ministry of Defence*[321] the plaintiff sued the Crown for false imprisonment on the ground that she had been detained and questioned by members of the armed forces for 30 min before they indicated to her that she was under arrest. She claimed that her arrest took place only when she was informed that she was under arrest and that the preceding detention was therefore unlawful. The House of Lords at appeal held that where a person was detained or restrained by a police officer and knew that he was being detained or restrained, such detention amounted to an arrest even though no formal words of arrest were spoken by the officer. Since the plaintiff had been under restraint from the moment she was identified, and must have realised that she was under restraint, she was deemed to have been under arrest from that moment, notwithstanding that the arrest took place formally, a half hour later.

Lord Griffiths, quoting an earlier decision,[322] endorsed the principle that arrest did not depend merely on the legality of the act but on the fact whether the person arrested had been deprived of his liberty. His Lordship went on address the decision in *Christy* v. *Leachinsky*[323] and noted:

> There can be no doubt that in ordinary circumstances, police should tell a person the reason for his arrest at the time they make the arrest. If a person's liberty is being restrained he is entitled to know the reason. If the police fail to inform him, the arrest will be unlawful with the consequence that if police are assaulted as the suspect resists arrest, he commits no offence. Therefore, if he is taken to custody, he will have action for wrongful imprisonment.

However, *Christy* v. *Leachinsky* made it clear that there are exceptions to this rule.[324]

The exceptions that Lord Griffiths referred to were those expressed by Viscount Simon where, when circumstances were such, that the person detained knew the general nature of the alleged offence, the requirement for informing him of the fact and grounds for his arrest did not arise. Viscount Simon held that technical or precise language need not be used and since any person is entitled to his freedom, if restraint was used and he knew the reason for such restraint, that was enough.[325]

There is however, no need anymore to rely on this aspect of the *Christy* decision since, as discussed earlier in this paper, statute has now explicitly laid down the law, leaving no room for ambivalence on the subject.

---

[320] Smith & Hogan, *Criminal Law*, *op. cit*. at 438.

[321] (1988) 2 *All E.R*. 521.

[322] *Spicer* v. *Holt* (1976) 3 *All E. R*. 71 at 79.

[323] *Supra*, note, 315.

[324] *Id*. 526.

[325] *Christy* v. *Leachinsky, supra*, note 315, at 572–573.

The Use of Air Transport for Peaceful Purposes

The attacks of 11 September 2001 inevitably highlighted the strategic position of civil aviation both as an industry vulnerable to attack and as an integral tool in ensuring peace and security in the world. The modernist view of civil aviation, as it prevailed when the Chicago Convention was signed on 7 December 1944, was centred on State sovereignty[326] and the widely accepted post-war view that the 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 general security.[327] This essentially modernist philosophy focussed on the importance of the State as the ultimate sovereign authority which can overrule considerations of international community welfare if they clashed with the domestic interests of the State. It gave way, in the 1960s and 1970s to a post-modernist era of recognition of the individual as a global citizen whose interests at public international law were considered paramount over considerations of individual State interests.

The 11 September 2001 events led to a new era that now calls for a neo-post modernist approach which admits of social elements and corporate interests being involved with States in an overall effort at securing world peace and security. The role of civil aviation in this process is critical, since it is an integral element of commercial and social interactivity and a tool that could be used by the world community to forge closer interactivity between the people of the world.

The Chicago Convention was signed at the height of the modernist era of social justice and commercial interaction. As *Milde* says: "It is in the first place a comprehensive codification/unification of public international law, and, in the second, a constitutional instrument of an international inter-governmental organization of universal character".[328] Be that as it may, the real significance of the Convention, particularly as a tool for ensuring political will of individual States, lies in the fundamental philosophy contained in its Preamble. In its Preamble, the Convention enunciates a message of peace through aviation. It makes mention of the future development of international civil aviation being able to help preserve friendship and understanding among the nations of the world, while its abuse (i.e. abuse of future development of international civil aviation) can become a threat to "the general security". By "general security" the Chicago Conference meant the prevention of threats to peace. These words have been interpreted in the widest possible sense by the Assembly of the ICAO[329] at its various sessions to cover instances of social injustice such as racial discrimination as well as threats to

[326] Article 1 of the Chicago Convention provides that the Contracting States recognize that every State has complete and exclusive sovereignty over airspace above its territory.

[327] Preamble to the Chicago Convention, *supra* note 3.

[328] Milde (1994).

[329] ICAO is the specialized agency of the United Nations dealing with international civil aviation. t has 190 member States, all of whom signed or ratified the Chicago Convention.

commercial expediency achieved through civil aviation. The 15th session of the ICAO Assembly adopted Resolution A15-7 (Condemnation of the Policies of Apartheid and Racial Discrimination of South Africa) where the Resolution urged South Africa to comply with the aims and objectives of the Chicago Convention, on the basis that the apartheid policies constitute a permanent source of conflict between the nations and peoples of the world and that the policies of apartheid and racial discrimination are a flagrant violation of the principles enshrined in the Preamble to the Chicago Convention.[330]

The Preamble was also quoted in Resolution A17-1 (Declaration by the Assembly) which requested concerted action on the part of States towards suppressing all acts which jeopardize safety and orderly development of international civil aviation. In Resolution A20-2 (Acts of Unlawful Interference with Civil Aviation) the Assembly reiterated its confidence that the development of international civil aviation can be an effective tool in bringing about friendship and understanding among the peoples of the world.

The general discussions which took place during the Chicago Conference gives one an overall view of the perspectives of each State, particularly in terms of what they expected out of the Convention with regard to the role to be played by civil aviation in ensuring peace, security and economic development in the world in the years to come. However, in some cases of extraordinary rendition, unfortunately, the converse has happened and in the instances already mentioned the attendant circumstances have even caused strife among nations. Arguably, the most dangerous risk of arrest of an innocent airline passenger suspected of terrorist activity would arise from profiling. It is an incontrovertible fact that profiling is a useful tool in the pursuit of the science of criminology. Profiling is also a key instrument in a sociological context and therefore remains a sustained social science constructed through a contrived process of accumulation of single assumptions and propositions that flow to an eventual empirical conclusion. However, profiling raises well reasoned latent fears when based on a racial platform. Jonathan Turley, Professor of Constitutional Law at George Washington University, in his testimony before a United States House of Representatives Committee on Airport Security regarding the use of racial profiling to identify potentially dangerous travellers observed:

> [R]acial profiling is to the science of profiling as forced confessions are to the art of interrogation. Like forced confessions, racial profiling achieves only the appearance of effective police work. Racial profiling uses the concept of profiling to shield or obscure a racist and unscientific bias against a particular class or group. It is the antithesis of profiling in that it elevates stereotypes over statistics in law enforcement.[331]

[330] See *Repertory Guide to the Convention on International Civil Aviation,* Second Edition, 1977, Preamble – 1.This subject was also addressed at a later session of the Assembly when the Assembly, at its 18th Session adopted Resolution A18-4 (Measures to be taken in pursuance of Resolutions 2555 and 2704 of the United Nations General Assembly in Relation to South Africa).

[331] Turley (2002).

Notwithstanding this telling analogy, and the apprehensions one might have against racial profiling, it would be imprudent to conclude that racial profiling is per se undesirable and unduly discriminatory, particularly in relation to profiling at airports which should essentially include some considerations of ethnic and national criteria. This article will examine the necessary elements that would go into effective and expedient airport profiling of potential undesirable passengers. It will also discuss legal issues concerned with the rights of the individual with regard to customs and immigration procedures. The rights of such persons are increasingly relevant from the perspective of ensuring air transport security and refusing carriage to embarking passengers who might show profiles of criminality and unruly behaviour on board.

A legitimate profiling process should be based on statistically established indicators of criminality which are identified through a contrived aggregation of reliable factors. The application of this criterion to airport profiling would immediately bring to bear the need to apply nationality and ethnic factors to passenger profiles. Although one might validly argue that racial profiling would entail considerable social and political costs for any nation, while at the same time establishing and entrenching criminal stereotypes in a society, such an argument would be destitute of effect when applied to airport security which integrally involves trans boundary travel of persons of disparate ethnic and national origins. This by no means implies that racial profiling is a desirable practice. On the contrary, it is a demeaning experience to the person subjected to the process and a de facto travel restriction and barrier. It is also a drain on law enforcement resources that effectively preclude the use of proven and conventional uses of enforcement.

The sensitive conflict of interests between racial profiling per se, which at best is undesirable in a socio-political context, and airport profiling, raises interesting legal and practical distinctions between the two. Among these the most important distinction is that airport profiling is very serious business that may concern lives of hundreds if not thousands in any given instance or event. Profiling should therefore be considered justifiable if all its aspects are used in screening passengers at airports. Nationality and ethnicity are valid baseline indicators of suspect travellers together with other indicators which may raise a 'flag' such as the type of ticket a passenger holds (one way instead of return) and a passenger who travels without any luggage.

Racial profiling, if used at airports, must not be assumptive or subjective. It must be used in an objective and non discriminatory manner alongside random examinations of non-targeted passengers. All aspects of profiling, including racial and criminal profiling, should as a matter of course be included in the Computer Assisted Passenger Screening System (CAPS)[332] without isolating one from the

[332] The CAPS system was adopted in 1994 by Northwest Airlines to single out high risk passengers. After the TWA flight 800 disaster in July 1996, the Clinton Administration appointed the Al Gore Commission to study aviation security. The Commission recommended that all airlines use the CAPS system provided profiling did not rely on material of a constitutionally suspect nature such as race, religion or national origin of United States citizens.

other. In this context the now popular system of compliance examination (COMPEX) is a non threatening, non discriminatory process which transcends the threshold debate on "profiling" by ensuring a balanced and proper use of profiling in all its aspects by examining "non targeted" passengers as well as on a random basis.

Another critical distinction to be drawn between discriminatory and subjective racial profiling on the one hand and prudent airport profiling on the other is the blatant difference between racism and racial profiling. The former is built upon the notion that there is a causal link between inherent physical traits and certain traits of personality, intellect or culture and, combined with it, the idea that some races are inherently superior to others.[333] The latter is the use of statistics and scientific reasoning that identify a set of characteristics based on historical and empirical data. This brings to bear the clear difference between "hard profiling", which uses race as the only factor in assessing criminal suspiciousness and "soft profiling" which uses race as just one factor among others in gauging criminal suspiciousness.

The nature of Air Transport in Extraordinary Rendition

Extraordinary rendition is an act of state and therefore the question arises as to whether aircraft used in this activity are military aircraft. Article 3 (a) of the Chicago Convention provides that the Convention will be applicable only to civil aircraft and not to state aircraft. It is an inclusionary provision which identifies military, customs and police service aircraft as being included in an undisclosed list of state aircraft. The Convention contradicts itself in Article 3 (c), where it says that no state aircraft of a contracting State shall fly over the territory of another State or land thereon without authorization by special agreement or otherwise, and in accordance with the terms thereof. The question arises as to how an international treaty, which on the one hand prescribes that it applies only to civil aircraft, turns around and prescribes a rule for state aircraft. Article 3 (c) effectively precludes relief flights over the territory of a State by state aircraft if the State flown over or landed upon does not give authorization for the aircraft to do so. *Milde* cites several instances of different types of aircraft being used in rendition flights[334] and concludes that a State aircraft may be identified by the design of the aircraft and its technical characteristics; registration marks; ownership; and type of operation.[335]

The distinction between civil and state aircraft is unclear as the Chicago Convention does not go to any length in defining or specifying as to how the two categories have to be distinguished. The ICAO Assembly, at its 14th Session held in Rome from 21 August to 15 September 1962, adopted Resolution A14-25

[333] *Britannica Macropedia*, 15 Ed. Vol. 9. at p. 880.
[334] Milde. *supra* at 478.
[335] *Id*. 481–482.

(Coordination of Civil and Military Air Traffic) which was on the subject addressed in Article 3(d) – that the Contracting States undertake, when issuing regulations for their state aircraft, that they will have due regard to the safety of navigation of civil aircraft. In A14-25, the Assembly directed the Council to develop guidance material for the joint civil and military use of airspace, taking into account the various policies, practices and means already employed by States to promote the satisfactory coordination or integration of their civil and military air traffic services.

At its 21st Session of the Assembly, Held in Montreal from 21 September to 15 October 1974, ICAO saw the adoption of Resolution A21-21 (Consolidated Statement of Continuing Policies and Associated Practices Related Specifically to Air Navigation) where, at Appendix O, on the subject of coordination of civil and military air traffic, the Assembly resolved that the common use by civil and military aviation of airspace and of certain facilities and services shall be arranged so as to ensure safety, regularity and efficiency of international civil air traffic, and that States would ensure that procedures and regulations pertaining to their state aircraft will not adversely affect or compromise the regularity and efficiency of international civil air traffic. In order to effectively implement the proposals of the Resolution, Contracting States were requested to initiate and improve the coordination between their civil and military air traffic services and the ICAO Council was required to ensure that the matter of civil and military coordination in the use of airspace is included, when appropriate, in the agenda of divisional and regional meetings.[336]

The ICAO Assembly, at its 36th Session (Montreal, 18–27 September, 2007) adopted Resolution A36-13 (Consolidated statement of continuing ICAO policies and associated practices related specifically to air navigation), Appendix O of which reiterates for the most part the text of Appendix O of Resolution A21-21, adding that the ICAO Council should endeavour to support States in the establishment of civil/military agreements by providing advice and guidance.[337]

One of the fundamental issues in the determination of aircraft category under Article 3 of the Chicago Convention is the use of civil aircraft in some instances for military purposes.[338] In emergency situations, States may acquire or in any other manner use civil aircraft for the transport of military personnel or goods meant for official use. In such circumstances any determination of the category of the aircraft concerned must be made taking into account all pertinent circumstances of the flight. Perhaps the most fundamental difference between the operation of civil and military aircraft lay in the fact that, although they were expected to share the same

[336] It will be recalled that the ICAO Council, at the Sixth Meeting of its 37th Session, held on 15 May 1959, noted the need for the Secretary General to pursue as effectively as possible the problem of accommodation of civil and military traffic in the available airspace. The efforts of the Secretary General were primarily meant to focus on the prevention of mid air collisions by the proper coordination of civil and military air traffic.

[337] See Assembly Resolutions in Force (as of 28 September 2007) Doc. 9902, at II-I7 to II-18.

[338] See Abeyratne (1997).

skies, the procedures by which they did this varied greatly. Civil aircraft depended entirely on predetermined flight paths and codes of commercial conduct which varied depending on aircraft type and types of traffic carried, whereas military aircraft operated in line with the exigency of a situation and were not necessarily always guided by predetermined flight paths. This dichotomy led to the adoption of Resolution A10-19 by the Tenth Session of the ICAO Assembly in 1956. The Assembly Resolution, while recognizing that the skies (airspace) as well as many other facilities and services are commonly shared between civil and military aviation, focused on ICAO's mandate to promote safety of flight[339] and reinforced the thrust of Article 3(d) of the Chicago Convention. The Resolution called for all Contracting States to co-ordinate between their various aeronautical activities in order that the common use of airspace inter alia be so arranged that safety, regularity and efficiency of international civil air navigation be safeguarded.

There is also the issue of military aircraft being used in some circumstances for civil aviation purposes. At the time of writing, there were no clear international rules, generally accepted, whether conventional or customary, as to what constitutes state aircraft and what constitutes civil aircraft in the field of air law.[340] Often, particular international air law instruments will in some way make reference to these or similar concepts, either without defining them, or at the most providing very broad general definitions which sometimes vary from one instrument to another. The situation also appears to be the same in the domestic legislation of States, with the meaning of terms such as "public aircraft", "state aircraft", "civil aircraft" or "private aircraft" varying according to the State in question and the object and purpose of the legislation.

Military aircraft, more than any other kind of aircraft including customs and police aircraft, personifies the public or sovereign power of a State, and several attempts have been made to arrive at an internationally acceptable definition thereof. The Treaty of Versailles of 1919 ending World War I, provided that the armed forces of Germany must not include any military or naval air forces, and several attempts were made to distinguish between military and commercial (or civil) aeronautical material. Between 1919 and 1922, the relationship between civil and military aviation was debated at length by three international committees of air experts which met, respectively, in Paris, Geneva and Washington. They concluded independently that no means could be devised to prevent the conversion of civil aviation to military purposes, which would not at the same time prejudice the

[339] As per Article 44 of the Chicago Convention.

[340] In the earliest days of this century, jurists divided aircraft into two categories, public and private, with differing applicable legal regimes. The majority of European powers which replied to a questionnaire submitted by the French Government in 1909 agreed that public and private aircraft should be distinguished. The first diplomatic conference on air navigation, which met in Paris in 1910, defined public aircraft as "aircraft employed in the service of a contracting State, and placed under the orders of a duly commissioned official of that State." More particularly, a very specific regime to govern military aircraft was outlined. The Conference did not formally adopt a convention, but provisions drafted heavily influenced the Paris Convention of 1919.

development of civil aviation. In 1920, the Supreme War Council of the Paris Peace Conference asked one of these committees, the Aeronautical Advisory Commission to the Peace Conference, which had given its opinion in 1919, to draw up rules to distinguish between civil aviation and the military and naval aviation forbidden by the Peace Treaties. The Commission, referring to its 1919 report, replied that the task was impossible. The Supreme Council insisted that the rules be drawn up; after several months of debates, the Commission submitted what is known as "The Nine Rules" of 1922, for differentiating between military and civil aircraft. The distinction was based on technical criteria such as engine size, speed, "useful load" etc. It soon became clear that many civil aircraft fulfilled these criteria and the Rules were later abandoned.

At the Chicago Conference of 1944, which paved the way for the adoption of the Chicago Convention, a United States proposal of a Convention on Air Navigation provided that the Convention 'shall be applicable only to civil aircraft.' "Civil aircraft" was defined as "any aircraft other than military, naval, customs and police aircraft of any State or any political subdivision thereof." A Canadian draft repeated, *mutatis mutandis*, the provisions of Chapter VII of the Paris Convention. Air Navigation principles were allocated to Subcommittee 2 of Committee I. The United States draft was used as the primary basis for discussion in Subcommittee 2. On 10 November 1944, the following suggestions were referred to the drafting Committee of Subcommittee 2. chaired by Mr. J.C. Cooper (United States): "(a) that the term 'civil aircraft' be used as suggested. in place of 'private aircraft' as used in the Paris Convention; (b) that a definition of 'military aircraft' be drafted which would cover military, naval, and air forces; (c) that the Status of military and state (customs and police) aircraft in relation to the requirements of the Convention be defined in a separate section." On that day, Sweden proposed an amendment which later emerged as Article 3 (d). The drafting Committee examined the issue and responded with what became Article 3 of the Chicago Convention in its final form. The metamorphosis of the relevant provisions of the United States draft into Article 3 (a) to (c) took place entirely in the drafting Committee, and no official record exists of the reasons behind the shift from the Paris Convention or even the U.S. draft. It should be noted that no definition of military aircraft was provided.

With regard to Conventions other than the Chicago Convention, one can see some provisions which are relevant to the discussion on the distinction between civil and military aircraft. The Convention on the International Recognition of Rights in Aircraft (Geneva, 1948), the Convention on Offences and Certain Other Acts Committed on Board Aircraft (Tokyo, 1963), the Convention for the Suppression of Unlawful Seizure of Aircraft (The Hague, 1970) and the Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation (Montreal. 1971), all contain a provision that "this Convention shall not apply to aircraft used in military, customs or police services." This appears to be a more simple way to indicate the scope of applicability of these Conventions than the provisions of Article 3 (a) and (b) of the Chicago Convention, although the end result seems to be the same. Furthermore. the clear implication is that all aircraft not so used would be subject to the provisions of the respective Conventions (paragraph 1.4 above refers).

The Convention on Damage Caused by Foreign Aircraft to Third Parties on the Surface (Rome, 1952) states in Article 26 that, "this Convention shall not apply to damage caused by military, customs or police aircraft." It should be noted that a "military, customs or police aircraft" is not necessarily the same thing as an "aircraft used in military, customs and police services" although again the expression "military, customs or police aircraft" was left undefined. Similarly, other "state" aircraft fall within the scope of the Convention. However, the 1978 Protocol to amend this Convention reverts to more familiar language; it would amend Article 26 by replacing it with, "this Convention shall not apply to damage caused by aircraft used in military, customs and police services."

The Convention for the Unification of Certain Rules Relating to the Precautionary Attachment of Aircraft (Rome, 1933) provides that certain categories of aircraft are exempt from precautionary attachment, including aircraft assigned exclusively to a government service, including postal services, but not commercial aircraft. On the other hand, the Convention for the Unification of Certain Rules Relating to Assistance and Salvage of Aircraft or by Aircraft at Sea (Brussels, l938 "apply to government vessels and aircraft, with the exception of military, customs and police vessels or aircraft . . .".

The Convention for the Unification of Certain Rules Relating to International Carriage By Air Warsaw, 1929) applies, inter alia. to all international carriage of persons. luggage or goods performed by aircraft for reward, regardless of the classification of the aircraft. Article 2 specifically provides that the Convention applies to carriage performed by the State or by legally constituted public bodies, but by virtue of the Additional Protocol, Parties may make a declaration at the time of ratification or accession that Article 2 (1) shall not apply to international carriage performed directly by the State. The Hague Protocol of 1955 to amend this Convention, in Article XXVI allows a State to declare that the Convention as amended by the Protocol shall not apply to the carriage of persons, cargo and baggage for its military authorities on aircraft, registered in that State, the whole capacity of which has been reserved by or on behalf of such authorities. Identical provisions are contained, *mutatis mutandis*, in the Guatemala City Protocol of 1971 (Article XXIII) the *1975* Additional Protocol No. 2 (Montreal), the *1975* Additional Protocol No. 3 (Montreal) and in Montreal Protocol No. 4 of 1975. It is submitted that Article 3 (b) of the Chicago Convention has no bearing on the applicability of these instruments of the "Warsaw System" which specify their own scope of applicability.

This analysis of some international air law instruments illustrates that many post-Chicago air law instruments (Geneva 1948, Tokyo 1963, The Hague 1970, Montreal 1971 and Rome 1952 and as amended in 1978) all have broadly similar provisions to Article 3 (a) and (b) of the Chicago Convention. The private air law instruments of the Warsaw System on the other hand, because of their nature, have adopted different formulae.

The provisions of the Chicago Convention and Annexes would not apply in a case where a state aircraft is (mistakenly or otherwise) operated on the basis that it is a civil aircraft. Similarly, the Geneva Convention of 1948, the Tokyo Convention

of 1963, The Hague Convention of 1970, the Montreal Convention of 1971 and the Rome Convention (*1952*) as amended in 1978, will also not be applicable where it is determined that the aircraft was "used in military, customs or police services". The converse, of a civil aircraft being operated on the basis that it is a state aircraft, would theoretically raise the same problems (i.e. legal regimes thought to be inapplicable are in fact applicable). Concern is not often expressed in this regard.

Another frequently mentioned difficulty is claimed to be the loss of insurance coverage in respect of the aircraft (hull), operator, crew and passengers or other parties where the aircraft is in fact state aircraft. The question whether a particular insurance coverage is rendered invalid in such situations is primarily a private law matter of the construction and interpretation of the insurance contract. Unless the contract has an exclusion clause which specifically makes reference to the classification in Article 3 of the Chicago Convention (e.g. loss of coverage where the operation is of a state (or civil) aircraft as defined in the Chicago Convention), where the Convention will have no bearing on the contract, and the issue of the loss of insurance coverage becomes moot, the Chicago Convention's application to the insurance contract would prevail. Frequently, the policy will exclude usage of the aircraft for any purpose other than those stated" in a Schedule; among the exclusions would be any use involving abnormal hazards. Nearly every aviation hull and liability policy now excludes losses due to war, invasion, hostilities, rebellion. etc., although insurance to cover such losses can usually be obtained by the payment of a higher premium. However, the instances mentioned do not require a determination of whether the aircraft is considered to be state or civil under the Chicago Convention.

A question sometimes asked is whether national civil laws and regulations would apply to civilian flight crews operating what is a state aircraft under the Chicago Convention. Would civil or military investigative and judicial processes be applied, for example. in the case of an accident? The answer would depend largely on the domestic laws of the State concerned. The fundamental principle is stated in Article 1 of the Convention: every State has complete and exclusive sovereignty over the airspace above its territory. Furthermore, subject to the provisions of the Convention, the laws and regulations of a contracting State relating to the admission to or departure from its territory of aircraft engaged in international air navigation, or the operation and navigation of such aircraft within its territory, shall be complied with by (civil) aircraft of other contracting States, upon entering or departing from or while in the territory of that A fortiori, state aircraft are also subject to the laws of the subjacent State.

In the case of an accident involving state aircraft, States are not bound by Article 26 of the Chicago Convention and Annex 13. They can voluntarily (through their legislation) so apply' these provisions. Sometimes, the legislation specifies a different procedure in relation to military aircraft only; all other aircraft, including those used in customs or police services, are treated as civilian in this regard. In the case of other incidents, where for example the requisite over-flight permission has not been obtained by a state aircraft, which is then forced to land and charges brought against the crew, again the answer would depend on the domestic laws of

the over-flown State and the factual circumstances. It is impossible to give a definitive answer in a vacuum. but it is the view of the Secretariat that the classification of an aircraft as "state" aircraft under the Convention does not necessarily mean that military laws and procedures of a State would apply to that aircraft or its crew. The current or any different classification of aircraft under the Convention would not be determinative whether a particular State, in the exercise of its sovereignty, would make that aircraft and/or its crew subject to civil or military laws and regulations. As a matter of practice States usually apply military rules and processes to military aircraft and personnel only. Paragraph 2.1.3 above shows that at the international level, attempts to arrive at a common, acceptable definition of military aircraft have met with a singular lack of success.

The question may arise as to the status of airline pilots and other crew under the Geneva Conventions of August 12, 1949 for the protection of war victims (the Red Cross Conventions) which apply, inter alia, in all cases of declared war or armed conflict between two parties, even if the state of war is not recognized by one of them. The Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (No. I) applies to "persons who accompany the armed forces without actually being members thereof, such as civil members of military aircraft crews ... provided they have received authorization from the armed forces which they accompany" and to "... the crews of civil aircraft of the Parties to the conflict ..." The same provisions are found in Convention for the Amelioration of the Condition of the Wounded, Sick and Shipwrecked Members of the Armed Forces at Sea (No. 2) and the Convention relative to the Treatment of Prisoners of War (No. 3). The Geneva Conventions, and in particular the provisions quoted above, do not link their own scopes of applicability to the determination under the Chicago Convention of the status of an aircraft. The Conventions of 1949 refer to civil and military aircraft, but not to these terms as "defined" under Chicago. Consequently, the provisions of the Chicago Convention does not, and cannot, determine whether and to what extent the flight crew of an aircraft is given protection by these Conventions.

Apart from the significance of aviation in its role in transporting suspected delinquents under extraordinary rendition, particularly in the face of its intended role in securing world peace, avition could act as a useful evidentiary tool in tracing rendition flights. For example, flight logs, which are kept by aviation authorities for years have been used to trace the transportation of particular prisoners from one jurisdiction to another.[341] The most significant role played by aviation, however, is in assisting the world community in realizing that current political and diplomatic problems mostly emerge as a result of the inability of the world to veer from its self serving concentration on individual perspectives to collective societal focus. This distorted approach gives rise to undue emphasis being placed on rights rather than duties; on short-term benefits rather than long-term progress and advantage and on purely mercantile perspectives and values rather than higher human values.

[341] Solomon (2007).

Against this backdrop, the fundamental principle and the overriding theme of international civil aviation has been, and continues to be, the need to foster friendship and understanding among the people of the world with the ultimate objective of ensuring global peace. Toward this end both the principles of air navigation and aviation economics have to ensure that aviation is developed in a manner that would make sure the world has a safe, reliable, economical and efficient civil aviation system.

References

Abeyratne RIR (1992) The development of the machine readable passport and visa and the legal rights of the data subject. Ann Air Space Law/Annales de Droit Arien et Spatial XVII (Part II) 99:1–31

Abeyratne RIR (1997) The use of civil aircraft and crew for military purposes. Annals Air Space Law/Annales de Droit Arien et Spatial XXII(II):1–23

Abeyratne RIR (1998) Aviation security. Aldershot, Ashgate, pp 131–196

Abeyratne RIR (2001) The exchange of airline passenger information – issues of privacy. Commun Law 6(5):153–162

Abeyratne RIR (2002a) Intellectual property rights and privacy issues: the aviation experience in API and biometric identification. J World Intellectual Property 5(4):631–650

Abeyratne RIR (2002b) Attacks on America – privacy implications of heightened security measures in the United States, Europe, and Canada. J Air Law Commerce 67(1)

Abeyratne RIR (2003) Profiling of passengers at airports – imperatives and discretions. Eur Transport Law XXXVIII(3):297–311

Abeyratne RIR (2007) The safe carriage of dangerous pathogens by air: legal and regulatory issues. Eur Transport Law XLII(6):689–704

Abeyratne R (2010a) Aviation security law. Heidelberg, Springer, pp 205–264

Abeyratne RIR (2010b) Negligent entrustment of leased aircraft and crew: some legal issues. Air Space Law 35(1):33–44

Adams J (1989) The financing of terror. Simon & Schuster, New York, p 12

Becker T (2006) Terrorism and the state, hart monographs in transnational and international law. Hart Publishing, p 155

Becker T (2006b) Terrorism and the state; rethinking the rules of state responsibility. Hart Publishing, Portland

Bennet CJ (1992) Regulating privacy. Cornell University Press, Ithaca, NY, 13

Blackstone W, Morrison W (eds) (2001) 4 Commentaries on the laws of England (1765–69). Cavendish, London, p 68

Bobbitt P (2008) Terror and consent: the wars for the twenty first century. Knopf, New York, at 98–179

Brownlie I (1983) System of the law of nations: state responsibility, Part 1. Clarendon, Oxford, p 39

Burnham D (1983) The rise of the computer state. Random House, New York, p 20

Caron DD (1998) The basis of responsibility: attribution and other trans-substantive rules. In: Lillich RB, Magraw DB (eds) The Iran-United States claims tribunal: its conclusions to state responsibility, vol 109 (Irvington-on-Hudson) NY. Transnational Publishers, pp 153–54

Cate FH (1997) Privacy in the information age. Brookings Institution Press, Washington, DC, p 49

Chen TC (1951) The international law of recognition, London

Clutterbuck R (1991) Living with terrorism. Butterworths, London, p 175

Cohen and Felson (1979) Social change and crime rate trends: a routine activity approach. Am Sociol Rev 44:588–589

Cooley TM (1888) A treatise on the law of torts, 2nd edn. Callaghan, Chicago
Cortes WI (2004) Cyber terrorism post 9/11 in the Western Hemisphere. Monograph presented to the Inter American Defence College as a requisite for obtaining the diploma of completion for the course on defence and hemispheric security, Fort Leslie J. McNair, Washington DC, April 2004
de Arechaga EJ (1968) International responsibility. In: Sorenson M (ed) Manual of public international law. St. Martin's Press, New York, 531 at 535
De Vattel E, Fenwick CG (tr) (1916) 2, The law of nations or, the principles of natural law: applied to the conduct and to the affairs of nations and sovereigns. Legal Classics Library, New York, NY, p 72
Delaney RF (1979) World terrorism today. Calif Western Int Law J 9:454
Dobson C, Payne R (1987) Appendix B: the chronology of terror: 1968–1987. In: War without end: the terrorists: an intelligence dossier. Sphere Books, London, p 366
Dorey FC (1983) Aviation security. Granada, London, p 142
Dunnigan JF (2003) The next war zone: confronting the global threat of cyber terrorism. Citadel Press, New York, p 4
Embar-Seddon SA (2002) Cyber terrorism: are we under siege? Am Behav Sci 45(6):1033–1043, at 1034
Ferguson N (2008) The ascent of money. The Penguin Press, New York, at 188
Flaherty DH (1991) On the utility of constitutional rights to privacy and data protection. Case W Res 41:831 at 833–834
Foschio LG (1990) Motor vehicle records: balancing individual privacy and the public's legitimate need to know. In: Kuferman TR (ed) Privacy and publicity. Meckler, London, p 35
Freund PA (1971) Privacy: one concept or many. In: Pennnock JR, Chapman JW (eds) Privacy. Atherton Press, New York, p 182
Fried C (1978) Privacy: economics and ethics a comment on posner. Ga L Rev 12:423 at 425
Gavison R (1980) Privacy and the limit s of the law. Yale L J 89:421
Grotius H, Scott JB (tr) (1646) 2 De Jure Belli Ac Pacis, pp 523–26
Guill M (2000) Cyber-terrorism poses newest and perhaps elusive threat to civil aviation. ICAO J:18
Halpin A (1997) Rights & law analysis & theory. Hart Publishing, Oxford, p 111
Hanle DJ (1989) Terrorism: the newest face of warfare. Pergamon-Brassey's, New York, p 185
Hoffer S (2000) World cyberspace law. Juris Publishing, at 8.1
Hoffman LJ (ed) (1980) Computers and privacy in the next decade. Academic Press, New York, 142
Hyde C (1928) Concerning damages arising from neglect to prosecute. 22 Am J Int L 140:140–142
J. Montgomery Curtis Memorial Seminar (1992) The public, privacy and the press: have the media gone too far? American Press Institute, p 2
Jennings RY, Watts AD (eds) (1992) Oppenheim's international law, 9th edn. London
Jones RV (1973) Some threats of technology to privacy, privacy and human rights. In: Robertson AH (ed) Presented at the third colloquy about the European convention on human rights, Brussels, 30 Sept–3 Oct 1970. Manchester University Press
Jorgensen NHB (2000) The responsibility of states for international crimes. Oxford University Press, Oxford, pp 249–254
Lauterpacht H (1947) Recognition in international law, Cambridge
Lee D (2005) Why terrorism? An agent-based model of culture and violence. Paper presented at the annual meeting of the International Studies Association, Hilton Hawaiian Village, Honolulu, Hawaii, Mar 05:2005
McMunn MK (1996) Aviation security and facilitation programmes are distinct but closely intertwined. ICAO J51:9 at 7
Mickolus EF (1980) Transnational terrorism: a chronology of events, 1969–1979. Aldwych Press, London, p 428
Milde M (1994) The Chicago convention – are major amendments necessary or desirable 50 years later? Ann Air Space Law XIX (Part I):401–452 at p 403

Milde M (2008) "Rendition flights" and international air law. Zeitschrift Fur Luft-und Weltraumrecht 4:477–486 at 477
Miller AR (1971) The assault on privacy. The University of Michigan Press, Ann Arbor, MI, 42
Misra S (2003) High tech terror. The American City and County, at 118
Nock SL (1993) The costs of privacy. Aldine De Gryter, New York, 43
Ofri A (1984) Intelligence and counterterrorism. ORBIS:49
Orwell G (1978) Nineteen eighty-four. Clarendon Press, Oxford
Orwell G (1984) Nineteen eighty-four. Clarendon Press, Oxford
Pember DR (1972) Privacy and the press. University of Washington Press, Seattle, p 227
Pierre AJ (1975–1976) The politics of international terrorism. ORBIS 19:1256
Posner R (1978) The right of privacy. Ga L Rev 12(3):393 at 409
Poulsen K (2002) FAA confirms hack attack, security focus, p 4–25, at http://www.securityfocus.com/news/378
Prowda JB (1995) A layer's ramble down the information superhighway: privacy and security of data. Fordham L Rev 64:738 at 769
Rapoport DC (1971) Assassination and terrorism. Canadian Broadcasting Corporation, Toronto, p 79
Regan PM (1995) Legislating privacy. The University of North Caroline Press, Chapel Hill, NC, p 33
Reidenberg JR (1995) Data protection law and the European union's directive: the challenge for the United States: setting standards for fair information practice in the U.S. private sector. Iowa L Rev 80:497 at 498
Reuter P (1989) Introduction to the law of treaties. Pinter Publishers, London and New York, p 16
Sattertwaite ML (2007) Rendered meaningless: extraordinary rendition and the rule of law. George Washington Law Rev 75:1333, at 1335–1336
Schenkman J (1955) International civil aviation organization. Librairie E. Droz, Geneve, p 6
Scott GG (1995) Mind your own business – the battle for personal privacy. Insight Books, New York, p 307
Shaw MN (2003) International law, 5th edn., Cambridge, p 367
Silets HL (1987) Something special in the air and on the ground: the potential for unlimited liability of international air carriers for terrorist attacks under the warsaw convention and its revisions. JALC 53:321 at 358
Simitis S (1995) From the market to the polis: the ec directive on the protection for personal data. Iowa L Rev 80:445 at 447–448
Simmel A (1971) Privacy is not an isolated freedom. In: Pennnock JR, Chapman JW (eds) Privacy. Atherton Press, New York, p 71
Smith and Hogan (1992) Criminal law, 7th edn. Butterworths, London, p 431
Sochor E (1991) The politics of international aviation. Macmillan, London, p xvi
Solomon D (2007) Breaking Jeppessen. Metroactive June 13–17
Starke JG (1989) Introduction to international law, 10th edn. Butterworths, London, p 3
Stohl M (2006) Cyber terrorism: a clear and present danger, the sum of all fears, breaking point or patriot games? Crime Law Soc Change 46:223–238
Treasury HM (2007) The financial challenge to crime and terrorism, p 8
Turley J (2002) A useful mechanism. Transec:24
Warner E (1942) Foreword to international air transport and national policy by Lissitzyn O.J. New York, p V
Warren SD, Brandeis LD (1980) The right of privacy. Harv L Rev 4(5):193 at 195
Warren SD, Brandies LD (1890–1891) The right to privacy. Harvard Law Rev 4:193
Weimann G (2006) Terror on the internet: the new arena, the new challenges. United States Institute of Peace Press, Washington, DC, at 148
Westin A (1967) Privacy and freedom. Atheneum, New York, p 368
Westin AF (1970) Privacy and freedom. Bodley Head, at 124
Young JB (1978) A look at privacy. In: Young JB (ed) privacy. Willey, New York, p 1
Zelermyer W (1959) Invasion of privacy. Syracuse University Press, Syracuse, p 16