Aviation security essay

This paper aims to address the impact of aviation security systems at airports which are implemented through controlled security programmes. It is without a doubt that our society has patterned to continually evolve into a technologically-based information age. With the ease of acquiring information even for the ‘ average joe’ today, governing authorities must respond by continually placing newer and improved security systems, particularly in the aviation industry.

Jones (2002) describes technology as a pillar of counter-terrorism, and suggests that significant attacks expand the array of technology initiatives required. Advances in technology include airport baggage screening, postal monitoring, biometric identification, radio and television broadcasting, and personal security. The scope of this discussion will focus on the influence of electronic screening, biometrics and e-chip passport features, particularly how they have developed and caused an impact to aviation security.

The refining of these systems significantly shapes the way we approach aviation security through a legislative and operational view-point. A flawless security system is what we continually strive for, and the main thrust for investing in costly security methods and researching new initiatives. As the ‘ security pendulum’ swings toward the desired outcome of attaining the ideal security system with prime safety levels; changes will be identified together with arising hindrances. The first part will focus on electronic screening, and the latter –biometrics and e-passports. Electronic Screening

While the means of screening passengers and items are primarily a preventive security measure for minimising the threat of terrorism and upholding an acceptable level of safety; it serves to fulfill the published ICAO (International Civil Aviation Organization) standard and recommended practices of the current Annex 17 (8th edition), according to the Chicago Convention. Standard 4. 1 of Annex 17 states: Each Contracting State shall establish measures to prevent weapons, explosives or any other dangerous devices, articles or substances, which may be used to commit an act of unlawful interference, the carriage or bearing f which is not authorized, from being introduced, by any means whatsoever, on board an aircraft engaged in civil aviation. (ICAO, 2006) For the last few years the ICAO has enforced a strategic objective to screen 100 percent of checked baggage –applicable to contracting states from January 2006. These objectives are expressed in Standard 4. 4. 8 and Recommendation 4. 4. 9 of the publication. In depth scrutiny of security methods and airport safety initiatives are set in place to prevent acts of preceded criminal activity and to deter unlawful interference.

For example since the September 11 attacks -programmes for federal air marshals were introduced for domestic operations, also with air crew being armed for safety (Haas, 2004). Although there may be no such thing as a 100% fail-proof security system, such measures including screening of passengers aid to moderate errors that are inevitable in the airport environment. Frederickson & LaPorte (2002) describes two types of errors related to screening which deters effectiveness when loading passengers and cargo. Type 1’ errors occur when a hypothetical person or item should be boarded (i. e. posing no threat in reality), but is kept from boarding an aircraft. Although this error may often be overlooked as an error, with a ‘

better be safe than sorry' mentality, its consequences can be significant in time, money and opportunity costs.

An accumulation of type 1 errors (also known as false positives) leads to ineffective air travel. ' Type 2' errors conversely occurs when a hypothetical person or item that should not board an aircraft (i. e. otentially harmful or threatening people or items), and a decision is made to allow boarding. Type 2 errors are clearly regarded and esteemed to be potentially catastrophic. Security exists to minimise such errors through methods of screening and other security measures, allowing air travel to be most efficient for an expected level of safety. Operational and legislative developments in Screening The introduction of X-ray screening came to be as a response to the hijackings of Dawson's Field on September 6, 1970 (Kazda & Caves, 2007).

Acts of terrorism manifested by the PFLP group (Popular Front for the Liberation of Palestine) orchestrated the hijackings of various passenger flights from operators including Pan America, TWA, Swiss Air and BOAC. The PFLP diverted flights to Dawson's Field, Jorden (with the exception of Pan America B747 commandeered toward Cairo) holding hostages for political reasons. The operational practices of screening in this era were mostly basic hand-held metal detectors, along with early versions of walk-through metal detectors as the birth of passenger detection.

The conventional x-ray systems introduced at this time were initially for carry-on baggage scanning, a system widely adopted by many airports. With increased usage, operators also utilised conventional x-rays in large quantities for hold-checked baggage, manually searching a minimum of 10% of all screened items for effective practices (Shanks ; Bradley, 2004). Two years after, in 1972, magnetometer-type screening was practiced in airports with 100% of all carry-on baggage being checked for domestic shuttle flights in the United States.

Moore (1991) defines such early magnetometer detection as ‘ passive detectors’, highlighting a flawed system design in that though a humble beginning, they were ineffective against scanning metals which were “ incapable of being magnetized”. This posed as a problem in security because a large portion of guns manufactured from the United States were made from nonferrous metals for ‘ light weight’ purposes and therefore, could easily remain undetected. In terms of how the legislative framework of screening in airports has been impacted, an iconic event was the ‘ Lockerbie Bombings’ of December 21, 1988.

A concealed explosive on-board a Pan American Airliner flight 103 was detonation over-head the town of Lockerbie, Scotland via a timing device. Casualties included all 259 passengers and crew on-board, as well as 11 residents on ground. Investigations found ‘ plastic explosives’ stowed away in passenger luggage (Beveridge, 1992). According to Moore (1991) it was the close-relatives of those victimised on-board Pan Am 103 who played a large role in getting authorities to address security issues by improving and creating change, from a legislative view-point.

As a result, the ‘ President’s Commission on Aviation Security and Terrorism’ was established in May of 1990, a report of over 60 recommendations serving as potential solutions to seeming vulnerabilities in security. Six months after the issuance of the report, congress and the authorities reacted quickly in passing the Aviation Security Improvement Act of 1990, where most of the recommendations of the President’s Commission were implemented in the new act (Moore). Some elevant findings include: “ The report of the President’s Commission on Aviation Security and Terrorism, dated May 15, 1990, found that current aviation security systems are inadequate to provide such protection”; “ The United States Government, in bilateral negotiations with foreign governments, should emphasize upgrading international aviation security objectives” This same legislative act addressed the negligence of screening mail and cargo; however the practicability of screening mail and cargo was still found to be ambiguous at this time.

As it is common amongst legal objectives, desired outcomes are clear but the means of attaining such outcomes are not addressed. For example, it was unclear if the same safety procedures used for detecting mail would also be used for checked-baggage (Moore 1991). Later on, amendments in security and screening were made in 1991 by the ‘ Convention on the Marking of Plastic Explosives for the Purpose of Detection’ published by the International Civil Aviation Organisation (ICAO).

Updated resolutions were made for contracting states to comply with ICAO standards, calling for immediate research and development on detection of explosives and on security equipment. In more recent times, the threat of terrorism has continued to raise security measures to a new level. On Christmas Day of 2009, Umar Abdulmutallab attempted to detonate explosive PETN powder (known as pentaerythritol), sewn discretely into the suspect’s underwear. The suspect intended to cause an explosion in a Northwest Airlines flight (NFW 253), above Detroit, however failed to work as planned(AFP: ABC news, 2009).

The attempted incident gives reason to utilise more modern instruments, like full-body scanners for the cause of public safety and also to simply fulfill the expectations of an operationally effective airport safety system. In a 2010 report the Transport Security Administration (TSA) announced full-body imaging machines have improved the security of airports markedly, successfully exposing over 60 “ artfully concealed” prohibited and illegal items within a one year period.

Officials say the ability to detect small concealed items reflects its effectiveness, revealing photos of suspected drugs which standard detectors would not have otherwise picked-up (Meserve ; Ahlers, 2010). If safety is the priority of security, what are the hindrances in practicing these effective security measures? Passenger safety vs. passenger rights Perhaps during early times (before events like Lockerbie, or significant hijackings such as 9/11), when technology was not quite as advanced and screening considered in its infancy; the security pendulum favoured passenger satisfaction (i. . minimum time delays due to scanning) however, far from being an comprehensive security system. This is certainly a contrast to the security system today, where we have reached a technological-edge to strive for accuracy in passenger screening (and enhanced safety measures); yet human rights are found violated, and passenger satisfaction seems to be on a decline. A recent report in May 2010, details the soon-to-arrive trail run of full-body scanners at Delhi airport, India.

Local airport authorities ‘ DIAL’ are trying new body scanners sourced from AS; E (American Science and Engineering Inc.) claiming the accuracy of such technology will reveal every detail of passengers -even genitals, for the purposes of enhanced electronic screening (Srivastav, 2010). The benefits of such a system are the improved definition in detecting guns or explosives hidden under clothing, also showing “ grainy outlines” of the human body, detailing outlines of breasts, buttocks and sexual organs (Sacirbey, 2010).

A decision of purchasing and implementing the scanners in Delhi airport will be made only after the trail run, as personal and human right violations have been raised. “ At present, security checks at Indian airports comprise pat-down searches, doorframe metal detectors and hand-held device scans” (Srivastav). Although these new scanners are designed to increase efficiency and effectiveness of screening (achieving a sound goal in terms of security) – however, along with issues of human rights these systems have also raised religious concerns of modesty.

After witnessing the scanned images, 18-member Fiqh Council of North America was lead to issue a ‘ fatwa’ (a religious edict) suggesting Muslims should be entitled to request for a pat-down instead, on the grounds that “ it is a violation of clear islamic teachings that men or women be seen naked by other men and women. Islam highly emphasizes ‘ haya’ (modesty) and considers it part of faith. ” cited in Sacirbey. These concerns are not only contained to the Muslim community but to Orthodox Jews and other conservative groups. Rabbi Steven Weil, CEO of the Orthodox Union says " the canners violate Jewish laws on modesty, or tzniut".

One can question where the line should be drawn? How can airport screening procedures find a balance between optimised passenger safety verses passenger satisfaction –both of extreme importance, yet lie on separate ends of the ' ideal' security spectrum? Few ideas have been raised to strive toward a desired equilibrium. Agudath Israel, a representative of Orthodox Jewish Umbrella Group, suggests full-body scanners not be used as a standard of screening, rather solely as a secondary method of precision screening, should passengers fail the initial metal detector tests.

Other suggestions to alleviate passenger dissatisfaction are for screening officers viewing the images, to work remotely (away from screening lines, not confronting the public being scrutinised). Images should also be deleted immediately or, machines being designed so as not to have an imagine-storing capability (Sacirbey, 2010). Fort Wayne International Airport also plans to implement full-body scans, being funded by the federal Transportaion SecurtiyAdministration (TSA), and is scheduled for installation by mid-March in 2010.

Leninger (2010) reports that passengers at Fort Wayne who do not wish to comply with full-body screening, have the option to receive a metal detector sweep check instead. From a different view-point, Director of Operations Scott Hinderman expresses that privacy concerns are exaggerated. Mr Hinderman says " It's not an invasion of privacy unless you refuse to wear a swimsuit. And you don’t have to do it…I’ve seen the pictures (of scanned bodies), and if that’s excitable, that’s just not right. ” (Leninger).

The Australian Counter-Terrorism White Paper (2010), states the Australian government wills to invest over $200 million (over four years) to strengthen aviation and border security regimes. This includes assistance to industry in the implmentation of new screening technologies such as body scanners at international gateway airports; next generation multi-view X-ray machines; bottle scanners capable of detecting liquid-based explosives; and X-ray screening (increased explosive trace detection technology for air cargo).

Biometrics and e-Passports

Derived from the Greek root words, ‘ bio’ and ‘ metron’ “ denotes the recognizing of humans on the bases of intrinsic physical or behavioural traits” (Maguire, 2009). There is an array of biological characteristics which may be scanned for detection. Common analyses of biometrics include fingerprinting, facial recognition; hand geometry; measurements of the eye (iris or retina imaging); or behavioural specifications such as voice, gait and signature (Haas, 2004) Electronic passports have stored information in a micro-chip inserted either in the middle or the back of the passport booklet.

The chip contains five types of information namely, similar data visually displayed on the front data page; holders passport picture (digital form); chip I. D. number; digital signature to verify signing authority also for detecting data alteration; and any additional data required by governing states. Standards for e-passports are set out by the ICAO. According to Turle (2007) the advantages of biometric security are three fold; firstly it sustains a high degree of reliability as biometric traits are not easily lost or forgotten. Secondly, simplicity.

The technology makes the need of passwords and pins redundant -the person is the password. Thirdly, sound levels of integrity, every individual possesses a unique set of biometric traits. These fundamental benefits greatly reduces possibilities of fraud and increasing the precision of security. Complications of such precise technology are not on the operational level rather, much like advanced screening instruments, legal implications do apply. “ Biometrics pose new and complex questions about compatibility with individuals’ rights to privacy” (Turle).

The happenings of September 11, 2001 continue to stir nations around the globe to use state-of-the-art technology for increased border security. Comprehensive use of biometric technology in airports require technical changes in airports, for example upgrading passport documents to electronic passports (e-passports), also implementing the appropriate technology or programmes compatible to support the use of e-passport documentation. After the ‘ 9/11’ attacks, initiation of the Machine Readable Passport (MRP) program was launched by the Bush Administration; and in late 2006 the U. S. overnment announced the issuance of e-passports to the public, albeit amid numerous privacy concerns.

The upgraded e-passports contained traditional passport information (such as name, date of birth, gender, place of birth, date of issuance/expiration, and passport number) along with personal biometric information for facial and fingerprint recognition purposes on a 64 kilobyte chip. (Yong & Bertino, 2007). Although the initial issuance of e-passports to the public was expected by the end of 2006, privacy concerns created demand for increased security measures before the acceptance of widespread adoption.

In response to public concerns, the U. S. Department of State added personal privacy security measures to e-passport features. Specific additions included an anti-skimming shield built into the cover of the passport, along with Basic Access Control (BAC), which encrypts the transmission between the passport and reader. BAC also creates a unique " unlock code from a scan of the machine-readable portion of the passport" (King, Meingast, & Mulligan, 2007). BAC and passive authentication (PA) are required for ICAO contracting states. Technical concerns and solutions

With the introduction of biometrics and e-passports in airports, new risks arise concerning issues with identification security and privacy. Safety devices must be in place to counteract such risks of potential hacking and other contemporary crimes. Some concerns include skimming, eavesdropping and tracking Skimming is the process of obtaining data from an individual that has not granted permission to access such information. The e-passport includes a metal insert in the cover (a Faraday cage) that blocks RF (radio frequency) transmission.

When closed, the passport chip will remain passive, even in a matching radio frequency field (King, Meingast, & Mulligan, 2007). Skimming and eavesdropping were the two primary privacy concerns among privacy advocates addressed by the Department of State (US DOS, 2009). Eavesdropping is defined as the interception of information as it is transferred from the passport micro-chip to a legitimate reader. Though similar to the issue of skimming, eavesdropping is a passive operation and therefore can be executed from a distance.

Preventative measures to reduce eavesdropping primarily involve the use of Basic Access Control (BAC). The aim of BAC is enhanced confidentiality, focusing on providing authentication and creating a ‘ secure channel’ of communication, that is free from interception. A reader must first optically scan the Machine Readable Zone (MRZ) -located at the bottom of the passport, and derive the access key from the scanned information. Once a communication channel is developed, the reader authenticates the passport based on an encrypted key embedded in the MRZ.

Only when the authentication is successful, the chip releases the encrypted data to the reader, which is decrypted securely on the reader. BAC provides security against both skimming and eavesdropping as it limits access to readers by using access keys (King, Meingast, & Mulligan, 2007). Tracking is the process of obtaining information related to the movement of a person or object (King, Meingast, & Mulligan, 2007). When the reader initially communicates with the chip, the unique ID (UID) of the chip is transferred in order to begin passive authentication.

If the ID were to remain static, a potential hacker would need to intercept the communication channel only once to track a passport holder. As a solution, each chip has a built-in random number generator that changes the UID before each session to prevent the use of the UID for tracking purposes. In conclusion, the features of screening, biometrics and e-passports have brought vast changes to aviation, creating the need to improve from a legislative view-point; leading to operationally and technical changes, and also financially (funding for new programmes or initiatives).

Whilst most of these changes and decisions are expected to be addressed by government authorities, some require public acceptance –this includes the tension between attaining the prime security system (national security) and preserving personal security (human rights). National security and human rights are two factors that must be considered equally important to aviation security. Although it is not wrong for the ‘ security pendulum’ to favour advanced security methods and utilise state-of-the-art equipment for border protection, perhaps the line is crossed when personal rights are breached.

Governing bodies and authorities alike must work together to bring aviation security closer to this ideal equilibrium, keeping in mind that even complex contemporary security methods (such as biometrics and e-passports), though effective, also imposes new areas of risk and potential threat to security. A strong cohesive framework of legal, operational and technical functions must evolve accordingly to support the effectiveness of such security features, if the benefits are to outweigh the costs.