The role of intelligence in aviation security

According to the Centre for the Study of intelligence (A unit under the United States' Central Intelligence Agency, CIA), civil aviation, unlike defence (military) aviation, has mostly been in the centre of aviation security concerns for obvious reasons (Raffel, 2007). First, civil aviation has a high-value asset (Human capital, goods, property and wealth) which makes it attractive for criminals and terrorist. Ordinarily, high value asset should not, in itself, constitute a severe security threat, but significant concentration of high value asset attracts crime (Wheeler, 2005: 7). In 60's and 70's, some aircraft were hijacked in the united state solely for the purpose of collecting ransom (Poole, 2008: 9). Subsequently, an increase s hijacking (for ransom) attack led to the formulation of various aviation security policies and programs especially in America and Europe. So, criminals may seek economic benefit are likely to attack an aviation unit for that reason. On the other hand, terrorist seek economic loss through massive collateral damage. But, not all aviation security attacks are ' economically motivated'. For example, 9/11 attacked was suspected to have been a socio-politically motivated. The severity of the attached is exacerbated by the massive human loss. It can be assumed that Al-qaeda figured the human loss as part of the objectives of their attack. Another example of massive human capital loss was caused by the attacks on Rome and Vienna airport in 1985 (Raffel, 2007). Then, it may be argued that criminals (especially terrorist) in their bid to make cynical statements and increase the severity of their attacks take advantage of the high human traffic associated with civil aviation to cause massive human loss. The CIA calls this ' massacre' ibid. Moreover, unlike defence aviation, traditional civil aviation systems (aircraft, personnel, airports) are not intrinsically designed with self-defence mechanisms,

making them prone to (frequent) attacks. Given the vulnerability of civil aviation to security attacks, aviation security and intelligence discussion focuses on civil aviation and its complex inter-relations makes multi-perspective discourse.

Aviation Security Intelligence: Information Gathering, Sharing and Analysis

Combating crimes and averting potential criminal and terrorist attacks is underpinned on well-versed understanding of the goals and resources of criminal and terrorist groups. Wheeler (2005: 37-38) explained intelligence procedure as mainly: covert gathering of information related to criminals and terrorist, a deep and broad ‘ centralized analysis’ of the information and a drawing a conclusion against previously known fact about the gang (terrorist and criminal). Doing this, security operation will not only get a foreknowledge of terrorist but also be able to predict (to a degree of accuracy) their next move. However, there is an ongoing discussion on how to best to deal with security intelligence in civil aviation which according to Raffel CIA, (2007) is ‘ drawn-out, confusing and inconclusive’. One can quickly associate and gain better understanding of Raffel’s assertions from the analysis of civil aviation and security threats previously discussed above. The question remains clear: How do we deal with information of a proposed attack? Answering this question requires a system wide, multi-stakeholder analysis which captures the views of the passenger, regulators (government) and the airline operators. Who should know what and when?

Airport and airline operators do feel that up to date and appropriate information sharing could help them plan and handle security issues. In

practical sense, vigilance can help reduce (if not eliminate) security risks. But in reality, most airline and airport operator do not have access to accurate, meticulously collected and analyzed information. Mostly, the available information or intelligence are too broad that they very difficult (perhaps, impossible) to employ in a specific airport or scheduled flight. This set-back is a flaw of the data capturing process; data is acquired on an informal basis instead of an organized, process driven method (Raffel, 2007). Besides the incongruity of available information and intelligence, there is a caveat on the source of such information. Technology has made all kind of information readily available and as such the accuracy of information and credibility of the source cannot be ordinarily ascertained. This is a dilemma for information analyst, including airport security analyst. Emphasis is placed on the source: general information on the public domain and confidential and sensitive intelligence which stealthy sourced and accumulated. As expected, classified intelligence are restricted, seldom available for open propagation. Security agencies control the dissemination of such information and place a strict need-to know requirement. In a separate argument, Wheeler (2005: 33) described the inhibition of information sharing as a ‘ culture’, a phenomenon which characterized every human endeavour. How then would airport and airline operator be able access the much needed information (intelligence) given the strict rules on the availability? The absence of an information sharing framework is a potential risk factor in aviation security intelligence.

The contest about ‘ privacy’ is another issue with aviation security. In 2004, ‘ National Commission on Terrorist Attacks upon the United States – an inquiry

on 9/11 attacks – recommended that the US president determines the guideline for information sharing among government agencies, protecting the privacy of the individual of whom they share information about (Wheeler 2005: 132). Perhaps, this recommendation may have been suggested by the Classified Information Procedures Act (CIPA) of 1980 which ensures the protection of protecting national security while also protecting the rights of the suspected individual. (Berman and Flint, 2003: 3)

Wheeler (2005: 32) identified a missing link between ‘ information gathering’ and ‘ information sharing’ which can cause a drawback in effective policing. The covert method of gathering and analyzing intelligence requires that these two phases (information gathering and sharing) makes this interconnection necessary. Terrorist and criminals can capitalize on the difference between knowledge centres in while planning for and executing attacks on their targets. Inquiries into September 11 showed that the incidence can be blamed on the intelligence failure – the government failed to ‘ make good use’ of prior information it had gathered and ‘ failed to utilize’ available ‘ information sharing’ framework. ‘ Misguided targeting’ is another weak point of intelligence gathering. Accumulating vast amount of information (of which some could be irrelevant) without ‘ exclusive suspicion’ will not catch terrorists and criminals instead it could make worse this Berman and Flint (2003: 2)

Critique of Aviation Security Intelligence Programs

Before September 11, 2001, aviation security intelligence was cantered around baggage screening (Poole, 2008: 17; Raffel 2007). But the 9/11 attack has set up a new atmosphere: The need to identify precarious

passengers (on a flight) and persons (within the perimeters of an airport) so as to nip potential attack in the bud before they are hatched. Before now, there have doubts on the effectiveness of these intelligence program (British Medical Journal 2010), increasing the outcry after the failed Christmas day bombing attack. The question is how did the terrorist (Abdul Mutallab) pass through the ‘ walls of screening’? Clearly, terrorist organizations are keenly abreast of the trends of aviation security and they are in a relentlessly pursuit to circumvent it. KhaleejTimes. com (2010) claimed that the little success of Christmas day attack should be blamed on failure of human side of intelligence, suggesting the need to revisit the framework of intelligence program, if they will ever prosper.

Computer Assisted Passengers Pre-screening System (CAPPS)

CAPPS (also Computer Assisted Passengers Screening CAPS) was first introduced in 1996, by an airline, as ‘ temporary measure’ to assist in passengers’ bag screening for explosives. Over time, it was reviewed. The later version (CAPPS II) was modified to classify all passengers into various class according to ‘ a risk assessment score’ allotted to the passenger. CAPPS II, depending on ‘ experimental data algorithm’ from various database (government and commercial), has a double sided central focus: scrutinizing ‘ high-risk’ passengers at the same time as reducing the harassment of ‘ low risk’ (innocent) passengers. Like the suspended US Defence’s ‘ Total Information Awareness program’, it is designed at profiling innocent people. Should the TSA invest so much on profiling (innocent) people who do not pose any security threat? In addition to initial public scepticism about the

effectiveness of this profiling program, there is a growing debate over the ‘ appropriateness and the privacy and security risks of such systems’ (EPIC 2007a). In 2003, TSA started the Aviation Security Records (ASSR) – an information database containing financial and transactional data as well as almost limitless data from other public and private information centre – which the TSA said it will allow government, public and private entities to access the records. The unrestricted access to the database raises concern about the privacy and the security of the database. Is it possible for criminals and terrorist to obtain seemingly classified information, under false pretence? ‘ How passengers can contest and redress risk score’ is another missing details in the program.

Secure Flight Program and the Terrorist Watch list

Soon after the TSA discarded the later version Computer Assisted Passenger Pre-screening System (CAPPS II) in August 2004, it started the Secured Flight Program which was aimed to match up passengers information contained in the Passenger Name Record (PNR) – data by provided by passenger – and the state maintained watch list. The program transcended beyond simply ‘ matching names on two list’ to a complex system of profiling persons in order to estimate the security risk which they pose (DHS, 2004). Although TSA performed test for the Secure Flight Program, the program faced some criticism which lead to its temporary suspension. According to GAO (2006), at point when the secure flight program was scheduled to commence in September 2005, it was faulted with ‘ an inconclusive risk assessment’ and ‘ 144 known vulnerabilities’.

TSA has a United State legislation backed mandate to keep a watch list of names of persons alleged to constitute a ‘ risk of air piracy’ or ‘ terrorism’ or ‘ a threat to airlines or passenger safety’. The agency’s watch list is categorized into two: ‘ no fly’ and ‘ selectee’ lists (EPIC, 2007). The airlines collaborate with TSA on this in that when a passenger checks in for a flight, they match the passenger’s identity with the record. Should the passenger’s name matches any on the ‘ no fly’ list, he or she is tagged a threat, and is refused to embark on the flight. Not only that, TSA is notified at once and a law enforcement officer is called to detain and interrogate the person. In case the person’s identity is matches any name on the select list, the person is tag ‘ S’ and he or she receives stricter security screening. But, what if there is a case of mistaken identity – when a person name is mistakenly matched with those on the watch list? Would an innocent passenger be disallowed from boarding a flight despite his constitution guaranteed right to travel? There are Tens of thousands of application of persons seeking redress for been wrongly mismatched (EPIC, 2007b)

Multi-perspective Evaluation of Aviation Security intelligence Program

This section will attempt to provide an analytic and multi-dimensional view of the role of security intelligence in aviation, exploring the economic, technological and social perspectives leaving out the legal and human right issues.

Economic (business) perspectives

Civil aviation cannot be disconnected from business. This is self evident in that the industry is deregulated to encourage capitalists who seek profits.

And the pursuit of profit is determined by the complexities of the aviation industry which include the impact of the aviation security intelligence on industry's economics that cannot be underestimated. An instance is the aftermath of September 11 which led to a down turn of aviation business. The industry recorded a steep decline of passengers booking (of about seventy four percent), several cancelled flights, reduction in route by some airline operator and consequently, loss of jobs, reduced share prices, and other business losses (Morrell and Alamdari, 2002: 1). This change in the aviation business atmosphere was caused from the ' non-fly' reaction from passengers. Passengers' reaction cannot be overlooked because it is an indication that passengers (like other consumers) are capable of intelligence sourcing and sharing (Haugtvedt et al, 2004: 283) and responding based on their analysis. Whether analysis of passenger is accurate is another subject entirely. Given the extent at which technology have increase the flow of information and the loop holes in information security, one cannot assume that sensitive security information cannot (would not) slip into the hand of the passenger (that is the set of air traveller) and the consequent passengers reaction and its ripple effect on aviation business (and industry in general) cannot be predicted. There is another dimension to this: Terrorist knowing fully that passengers can react to ' fear factor' just as they did after September 11 may explore this scenario and the weakness of existing information sharing framework to pursue an economic combat strategy simply by sparking ' panic' within the system.

Another side of the economics of aviation security intelligence is the massive and undisclosed cost of pursing an intelligence system. Poole (2008: 2)

argued that similar to other similar human endeavour where choices are to be made based resource constraints, aviation security is faced with the challenge of making a decision on how to invest ‘ scares resource’ for ‘ maximum benefit’. As anticipated, this makes decision making pretty difficult, and decision are characterized with frequent trade-offs. And if such trade -offs are not properly analyzed or hinged on wrong assumptions, the eventual decision may contribute to insecurity (KhaleejTimes. com, 2010). Based on this premise, Poole (2008: 2) developed a risk assessment framework for making choices as related to aviation security. Another effect of classified information is that the actual cost of aviation strategy is difficult to determine, especially if the costing model is extended to account to include themes like cost benefit analysis (Poole, 2008: 3).

Social perspectives

Present Focus is emphasized on international flight overlooking (or disregarding the possibility) internally originated threats like those of London bombing. This leaves one to ‘ assume’ that some intelligence campaigns are based on prejudice and ostensible conclusions. Proponent of this view may not be entirely wrong; may not fault the assumption that ‘ international flights’ poses higher degree of aviation risk. Social (racial, and religious) discrimination concerns became more prominent when the United States government announced compulsory screening for ‘ all passenger’ from 14 countries (mostly Islamic) after the failed Christmas day bombing attempt (Zakaria, 2010). One can argue that intelligence efforts are socially biased (Persico, 2002: 1472-73; Knowles and Hernandez-Murillo, 2004: 959 -60)

Political perspectives

Poole (2008: 2) insists that changes in aviation security policies are motivated ‘ political imperatives’ to ‘ reassure frightened population’ of that the nation’s air space is still very safe. For example in the United State, through legislation, the government established the Transportation Security Administration- an institution with complete responsibility for the nation’s transportation security but a huge part of its budget is committed to aviation security as directed by legislation. In a move to increase intelligence gathering, Attorney General Ashcroft approved security (FBI) agents to ‘ attend and monitor political events and religious’ which might serve as hubs for terrorist activities Berman and Flint (2003 : YY), showing the an interconnect but these themes : Politics and Security Intelligence.

Technological Issues: Open access Information and Biometric Data

The debate on information sharing is incomplete without examining the impact of technology. One of such argument is the ‘ openness’ of sensitive information to the public. For instance, Airport Law Enforcement Agencies Network (ALEAN) – information-sharing groups supporting airports – do make available information and open source material which is intended for aviation security personnel (Raffel CIA, 2007). Mindful the fact that terrorist and criminal can take advantage of the easy and open accessibility of electronic information system, the reliability of this method remains shaky. In another campaign, there is an advocacy to leverage on technology to help strengthen the various passengers profiling program through the inclusion of biometric data (KhaleejTimes. com, 2010). Biometric data are so unique so

much that incidence of identity mismatch is almost unlikely (if not impossible). Although, how this new method will be adopted remains on clear, but it shows a promise of resolving some of flaws in existing program.

Summary

The drawback in information sharing has rendered most aviation security intelligence initiatives less effective. The present demands for intelligence is expected to increase can become more effective information sharing. In spite of the doubts that present regime of security intelligence on the effectiveness, they are building blocks for the future of aviation security). It remains unbeatable that intelligence affects the aviation security and the aviation industry in general, and that the various intelligences actions and inactions can shape the future. This review has attempted to identify various linkages between these arguments and highlight possible path for future discourse.