Available online at www.elixirpublishers.com (Elixir International Journal)

International Law

Elixir Inter. Law 65 (2013) 19671-19672

ISSN: 2229-712X

Security risks facing the civil aviation sector in India: need for review of the existing law

Siddharth Mehta
Amity Law School, Delhi, IP University.

ARTICLE INFO

Article history:
Received: 3 October 2013;
Received in revised form:
25 November 2013;
Accepted: 3 December 2013;

Keywords
Aviation,
Civil,
Law,
Legislative.

ABSTRACT

Over the past one decade, the Indian Aviation sector has moved from being a closed, poorly managed and excessively regulated industry to a more open, liberalized and investor friendly sector. The growth in this sector has been threatened inter alia by a lot of challenges such as high fares, high operational costs, global slowdown and security and law and order issues. According to the estimates of Centre for Asia Pacific Aviation (CAPA) by 2020, Indian Airports in all probability be able to serve over 100 million passengers every year. The figures revealed by the Ministry of Civil Aviation also indicate that the number of International passengers are expected to increase to 50 million. In such a scenario, it is important to maintain a fool proof security paraphernalia which is capable of adequately dealing with the rapidly changing techniques adopted by the terrorists groups. The security mechanism in the aviation sector needs a reconditioning to bring it in tune with the constantly evolving terror issues. The Aircrafts Act has become obsolete, it does not contain any special provisions with regard to the security of the Aircrafts, it is often felt that a comprehensive legislation pertaining to Civil Aviation Security is required for setting up a legal framework to inter alia provide for deterrent punishment for such offences, a specially trained task force for dealing with such contingencies and a summary disposal of such cases. The paper makes a humble attempt to suggest the procedural and legislative changes in the light of the civil aviation security laws of the other nations. A critical analysis of the current law has been done to show the various anomalies present therein. It is the objective of this paper to suggest a reconciliation between the interests of the passengers and the security of the state.

Introduction

In India, the BCAS is in charge of the aviation security whereas the DGCA acts as a regulator and a safety evaluator in the Indian Civil Aviation Industry. There are several legislations governing the Indian Aviation Sector. They are :

1)Aircrafts Act, 1937
2)Aircraft Rules,
3)Tokyo Convention Act,1975
4)Anti Hijacking Act, 1982
5)The Suppression of Unlawful Acts against Safety of Civil Aviation, 1982

India is also a signatory to various International Convention on Civil Aviation such as Tokyo Convention, Montreal Convention etc and has enacted various laws to fulfill its commitments under those conventions. The Tokyo Convention Act,1975 is a manifestation of one such legislation.

The civil aviation sector of our country faces a constant threat from cyber terrorism particularly emanating from some of our neighbouring countries, the famous military strategist of China Tsu Zu said in The Art of War that "battles are won or lost even before they are fought", and the modern means to win a war even without fighting it is covert war or proxy war and an important tool of this covert war is cyber terrorism. It is evident from the past terrorist attacks that terrorists are now aiming to harm the economy of nations as harming economy of a state can have disastrous ramifications for the people and government of the state, thus terrorists may use cyber terrorism to harm the civil aviation sector of our country as it will be highly detrimental to our economy and such harm to the aviation sector will also draw the attention of the entire world which will further the objective of the terrorists and will tarnish India's image worldwide. United States of America's Federal Bureau of Investigation defines cyber terrorism as any "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents."

The civil aviation infrastructure is extraordinarily dependent on computer-telecommunications information systems. Some of the most prominent and widely used systems include those for air traffic control, navigation, reservations, and aircraft flight control. Others are used extensively for airport and airline management. Individual flights can now be tracked on the Internet in close to real time. These information systems have become critical to the complete spectrum of activities in the civil aviation industry. The Aviation is heavily dependent upon Cyber Space for its effective functioning. Unfortunately, the Indian Law does not even contemplate cyber attacks on Aviation Sector as a separate crime in any of the above Convention and simply treats them under the head of "cyber terrorism'' in the Information Technology Act.[1] Consequentially, there is hardly

[1] Section 66E of The Information Technology Act, 2000

Tele:
E-mail addresses: siddharthlaw19@gmail.com

any provision to prevent such attacks from taking place. It is well recognized that terrorists are quite capable of inflicting terror attacks through the use of internet. The Internet may be used by them to hack the computer system of an airport and cause the services to come to a standstill, the hacking may be directed at the Air Traffic Control of an airport, in which case the ramifications of such an attack can be disastrous. The terrorists can virtually wreak havoc without having to fire a single bullet or blow a single bomb. The Internet can also be used to steal critical information from the information systems of the Airports which may be sold to terrorists or which may be used by the terrorists to conduct physical attacks against the aircraft.

Recently, while at a briefing with Chairman of US Joint Chief of Security, the Chairman of the People's Liberation Army's General Staff commented that "If Internet security cannot be controlled, it's not an exaggeration to say the effects could be no less than a nuclear bomb,"[2]

The statement is reflective of the dangers posed by cyber crime to the International Community.

Civil Aviation has remained one of the favourite targets of the Terrorists, there is a long history of unlawful acts against aircrafts taking place, it is because of the kind of publicity that attacks on civil aviation provide. The publicity is enough to instill a fear in the minds of the citizens and since such acts always invariably catch the attention of the international community, it provides a forum to the terrorists to publicize their agenda at an international level. Another incentive to the offender may be the anonymity associated with cyber attacks and the unavailability of effective mechanism to direct a response against such attacks. The extent of the threat posed by cyber terrorism is reflected in the Annual Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence22 of 2010 which states that the agility and technological innovation demonstrated by the cyber criminal sector far exceeds the response capability of network defenders. The Threat Assessment drew an implicit parallel between cyber terrorism and international organized crime, expanding that international criminal organizations will increasingly damage the ability of legitimate businesses to compete and may drive some legitimate players out of the market.[3] It may be noted that Cyber Crime against the government establishments is not a new phenomena in the world. Often, many countries have accused its enemies of hacking the websites of its important government establishments to steal critical defence related information. A barrage of cyber attacks were directed against the government websites in India in December 2012,the government officials suspected the role of Pakistani and Chinese hackers. [4] Similarly, two days ago, the website of Dubai International Airport was hacked allegedly by hackers based in portugal.[5] The phenomena is very poignantly expressed by Cyber Expert Mr Pawan Duggal, he observes that Cyber Warfare has become a reality for the World, and the next war shall necessarily be a cyber war.[6] In such a scenario, it is important to plug the loopholes in the Civil Aviation Industry, no legislation in India recognizes Cyber Terrorism against Aircrafts as a specific crime and hence, no special measures have been laid down to protect aircrafts and airports from the nuisance of such an attack. The law also lacks in terms of providing for an effective investigation mechanism, the provision of separate courts with well equipped judicial officers to deal with such complexities. It is relevant to note that the International Conventions such as the Tokyo Convention of 1963, The Hague Convention of 1970 and the Montreal Convention of 1971 do not directly deal with the question of cyber terrorismthe 2010 Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation adopted in Beijing29 in Article 1 d) 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. This undoubtedly refers, inter alia to cyber terrorism, but links the offence exclusively to the safety of aircraft in flight. Article 2a) of the Convention provides that 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 would be deemed to continue until the competent authorities take over the responsibility for the aircraft and for persons and property on board. 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. Notwithstanding this lacuna, it is felt that the Beijing Convention is a direction in the right step and should be adopted and ratified by India. The law should also be comprehensive as regards the investigation of such offences, the trial of such offenders etc. It is also necessary for India to enter into bilateral treaty agreements with other countries to provide for extradition of offenders when the crime is committed by persons based in other countries. A committee of Cyber Security and Aviation experts should be formed to formulate a counter strategy to cyber crimes directed against the Civil Aviation Sector which may then be codified in the form of a comprehensive law.

---

[2] http://www.sfgate.com/business/bloomberg/article/China-General-With-Dempsey-Compares-Cyber-Attack-4453520.php

[3] Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence, February 2, 2010, ATA FEB 2010—IC STATEMENT FOR THE RECORD at 3. See http://www.cfr.org/ intelligence/annual-threat-assessment-intelligence-community-senate-select-committee-intelligence-2010/ p21369

[4] http://articles.economictimes.indiatimes.com/2011-12-03/news/30471838_1_cyber-attacks-hackers-symantec-india

[5] http://www.arabiansupplychain.com/article-8627-dubai-airports-website-hacked-info-leaked-on-web/

[6] http://www.vifindia.org/article/2012/february/13/An-Indian-Cyber-Security-Mechanism-Need-of-the-Hour