UDC 658. (075.8)

Tetiana Zagnii,
(ICAO Training Institute, National Aviation University,
Kyiv, Ukraine)

Human Factor in Aviation Security

The paper presumes that human resources are critical to aviation security. Security personnel – passenger and baggage screeners, guards and law enforcement officers, and airport and airline employees, in general, are important elements of a system that prevents and deters hostile acts against air carriers. The human role in a security system should be taken into account as well.

Introduction

Technology can enhance, but cannot replace, the capabilities of people and the many services they provide. Moreover, management practices based on behavioral research findings can further improve human performance. The human role in a security system is complex; thus the nature of human errors, from mental to physical, varies widely. Mental or cognitive errors can include improper judgment or decision-making, while physical errors may stem from motor skill deficiencies or faulty equipment design. A combination of physical and mental processes may influence other kinds of errors, such as those involving communication, perception, or alertness.

Human factors, a discipline combining behavioral sciences and engineering, focuses on improving the performance of complex systems of people and machines. Designing and operating a system so that it does not induce human error (in fact, designing it so that human error may be minimized) is one critical component of human factors and limiting the impact of a human error once it occurs is another aspect.

Many types of human error are systematic, following certain predictable patterns; once these patterns are identified, countermeasures can be developed. For example, poor location of switches or dials can induce manual or perceptual errors. For those types of human error that do not follow predictable patterns, mitigation techniques are difficult to develop. Some examples of mitigation techniques include automatic monitoring and warning devices. These subsystems, when properly designed and implemented, can be invaluable tools for negating human error.

Passenger Profiling

In-depth questioning of all airline passengers and detailed examination of each of their personal belongings and baggage is impossible in a modern transportation system. Since most of the millions of passengers that fly on different airlines each year pose no security risk, targeting security resources on the small number of passengers who exhibit some elements of the threat “profile” is one way to increase security without clogging transportation flows. Profiling can be a valuable component of a transportation security system, providing an independent complement to hardware-based (and often more expensive) explosives and weapons detection technologies. Successful profiling depends on a large support system

including comprehensive intelligence networks and threat analyses, information system technology to process large databases, behavioral research and analysis, and trained and motivated screening personnel.

There are two general approaches to operational profiling. One compares passenger demographic and other background data (age, gender, nationality, travel itinerary, etc.) to historic or recent intelligence derived "threat profiles". The other is based on the examiner's psychological assessment of the passenger, taking into account nervousness, hostility, or other suspicious characteristics. Most profiling systems currently use elements of both approaches to varying degrees.

To establish an effective system, States should implement a combination of physical screening and other personnel security controls, which may include behavioural detection of non-passengers (including informal interaction with non-passengers).

Human role in a security system

The human role in a security system is complex; thus the nature of human errors, from mental to physical, varies widely. Mental or cognitive errors can include improper judgment or decision-making, while physical errors may stem from motor skill deficiencies or faulty equipment design. A combination of physical and mental processes may influence other kinds of errors, such as those involving communication, perception, or alertness. Human factors, a discipline combining behavioral sciences and engineering, focuses on improving the performance of complex systems of people and machines. Designing and operating a system so that it does not induce human error (in fact, designing it so that human error may be minimized) is one critical component of human factors and limiting the impact of a human error once it occurs is another aspect.

Many types of human error are systematic, following certain predictable patterns; once these patterns are identified, countermeasures can be developed. For example, poor location of switches or dials can induce manual or perceptual errors. For those types of human error that do not follow predictable patterns, mitigation techniques are difficult to develop. Some examples of mitigation techniques include automatic monitoring and warning devices. These subsystems, when properly designed and implemented, can be invaluable tools for negating human error.

Behaviour detection (BD)

Behaviour detection, at its core, is a method of observing human signals, both behavioural and physiological ones, which can alert an officer that someone requires additional screening. During the application of BD, screeners observe for a combination of verbal and non-verbal indicators to evaluate someone's behaviour. Each of the behavioural indicators that the screeners have been trained to detect were identified by academic research literature (e.g., deception detection), operational experience (e.g., law enforcement agencies from around the world), and documented cases of terrorism as well as criminal activity. With the exception of only a few indicators, some form of behavioural clustering is required. Only the most critical, or those that may indicate an attack is imminent, precipitate immediate action. Otherwise, an individual is seamlessly 'referred' for additional screening, which is similar to a standard secondary search and includes a brief interview

component. It is through this referral process that a resolution is reached regarding whether an individual is considered a higher risk and thus required to undergo further intervention from law enforcement or other security entities. The data collected through BD includes cases with known ties to terrorism and a myriad of criminal type incidents: drug smuggling, fraudulent identification scams, money laundering, and individuals carrying bomb parts in their checked baggage, just to name several. Terrorism is funded through activities such as these and stopping them during this stage is paramount to hindering those potential future acts. The apex of BD, in this context, is that it does not discriminate between activities. Similar behaviour, whether you are a drug smuggler or a terrorist will manifest due to the underlying stress or fear response that the human body may emit when trying to conceal something. These behaviours can occur unbeknownst to the person displaying them and some are rather difficult to control (e.g., physiological behaviours). This provides a way for screeners to route individuals to additional screening to ensure something else is not going on and to ensure the safety of the travelling public.

Behaviour detection is one of the only capabilities that are not restricted to identifying a single method of attack – any individual attempting to circumvent security or cause unrest can be identified as high-risk by observing human behaviour, even internal threats. It is vital for the global community to implement strategies that can identify and detect individuals who not only have the means to carry out an attack (e.g. a bomb), but also identify those who harbour ill intent and the desire to harm innocent civilians. Without BD as a supplemental layer of security, it may not be possible to proactively mitigate a threat before it happens.

Conclusions

Including a behaviour detection component within the larger security strategy can help detect and deter potential acts of violence and hostile intent, something that technology cannot do. Without this component, a security system is not efficient enough and is vulnerable to unknown threats. The ICAO and global community are working together to create a capability that is accepted and implemented within security paradigms. It is necessary to emphasize that BD is scalable, flexible, and threat neutral, which, in turn, can be considered a great advantage.

We have two major considerations:

1. Designing a new set of tasks, with dedicated staff (an opportunity to reconsider Human Factors in reference to the best practices)

2. Behavior Detection relies 100% on the human competency. This fact raises the question of efficiency and reliability. In this regard, there is a need for careful thinking on:

- the staffing
- overseeing of activities
- performance evaluation

References

1) Adrian Schwaninger, November 2006. Airport security human factors: From the weakest to the strongest link in airport security screening. Conference Paper (PDF Available). DOI: 10.13140/RG.2.1.1561.4965. Conference: International Aviation Security Technology Symposium, At Washington, D.C., USA, Volume 4.

2) Annex 17 to the Convention on International Civil Aviation. Security. Protection of international civil aviation from acts of unlawful interference. International Civil Aviation Organization, 999 University Street, Montréal, Quebec, Canada.

3) ICAO Doc 8973/9. Manual on Aviation Security. International Civil Aviation Organization, 999 University Street, Montréal, Quebec, Canada.

4) Les Ainsworth, 2003. Human Factors Considerations in Airport Security. Synergy Consultants Ltd. United Kingdom.

5) Dillingham, G.L. (2001) Aviation Security: Weaknesses in Airport Security and Options for Assigning Screening Responsibilities. US General Accounting Office Rept. No.GAO-01-1165T

6) Gale, G.A., Mugglestone, M.D., Purdy, K.J. and McClumpha, A. (2000) Airport Baggage Inspection – Just Another X-ray Image. In Contemporary Ergonomics 2000,

7) McCabe, P.T., Hanson, M.A. and Robertson, S.A. (eds.), pp 426–430, London: Taylor and Francis.

8) Harris, D.H. (2002) How to Really Improve Airport Security. Ergonomics in Design,10/1, 17 – 22.

9) Mead, K M et al. (1987) Aviation Security: FAA Preboard Passenger Screening Test Results. US General Accounting Office Rept. No. GAO/RCED-87-125FS

10) ECAC Doc 30. ECAC policy in the field of aviation security. https://www.ecac-ceac.org