JOURNAL OF SECURITY AND SUSTAINABILITY ISSUES
ISSN 2029-7017 print/ISSN 2029-7025 online
2020 June Volume 9 Number 4
https://doi.org/10.9770/jssi.2020.9.4(2)

THE IMPLEMENTATION OF SELECTIVE PASSENGER SCREENING SYSTEMS BASED ON DATA ANALYSIS AND BEHAVIORAL PROFILING IN THE SMART AVIATION SECURITY MANAGEMENT – CONDITIONS, CONSEQUENCES AND CONTROVERSIES

Krzysztof Michalski[1], Marcin Jurgilewicz[2], Mariusz Kubiak[3], Anna Grądzka[4]

[1,2]Rzeszów University of Technology, Aleja Powstańców Warszawy 12, 35-959 Rzeszów, Poland
[3]University of Natural Sciences and Humanities in Siedlce, Stanisława Konarskiego 2, 08-110 Siedlce, Poland
[4]Johns Hopkins University, MD 21218 Baltimore, USA

E-mails: [1]michals@prz.edu.pl, [2]m.jurgilewicz@prz.edu.pl, [3]mariusz.kubiak@uph.edu.pl, [4]agradzka426@gmail.com

Received 18 November 2019; accepted 18 April 2020; published 30 June 2020

Abstract Since September 11, 2001, airport security control procedures have expanded in the face of the increased threat of terrorist attacks on aircrafts and airports. Obligatory and meticulous checks are carried out on all passengers although the overwhelming majority of passengers do not pose any risk. Current airport control procedures are expensive and inefficient; they extend the time spent by passengers at the airport and contribute to increased crowding; they inhibit the development of interconnected transport systems and significantly reduce the comfort of passengers who pose no threat. As the security needs of air transport morph, security experts are considering replacing the existing across-the-board procedures with personalized and more selective control processes based on data and behavioral analysis to reduce the duration of airport check-in procedures and improve the effectiveness of security controls. Such solutions have been successfully tested over the past decades at Israeli airports and check-in terminals by the Israeli state carrier El Al, which has the reputation of being the best-protected airline in the world. The FLYSEC system, developed and tested in 2015-2018 at Luxembourg Airport in cooperation with the local university, operates on similar principles although its implementation is less invasive. Modern computer tools for analyzing travel history data and data from current bookings as well as algorithmic methods of behavioral analysis based on advanced detection, identification, crowdsourcing and tracking systems all feed into such smart, selective and personalized security controls. Smart, selective control systems are based on the basic assumption that passengers can be accurately and effectively sorted into different risk groups (e.g. low-risk/trusted passengers, normal passengers, high-risk passengers), long before they arrive at the airport and create a real threat. There are many effective techniques for profiling and identifying perpetrators already used in criminology, criminalistics and computer forensics that are also suitable for use in smart security systems to better meet the current and future needs of civil air transport. The article presents the idea and general characteristics of smart, selective and personalized security control systems, followed by structuring of the analytical field and problem analysis in terms of their implementation conditions, opportunities, threats, conflict-forming potentials and controversies, as well as the needs for more detailed research and their suggested directions.

Keywords: behavioral analysis; profiling and typing of high-risk travelers; security science; technology assessment; aviation security

Reference to this paper should be made as follows: Michalski, K., Jurgilewicz, M., Kubiak, M., Grądzka, A. 2020. The implementation of selective passenger screening systems based on data analysis and behavioral profiling in the smart aviation security management – conditions, consequences and controversies. *Journal of Security and Sustainability Issues,* 9(4), 1145-1155.
https://doi.org/10.9770/jssi.2020.9.4(2)

JEL Classifications: 032

1. Problem area

Civil air transport has many structural and functional peculiarities that give security problems a special rank while stoking specific fields and analytical perspectives for security research unknown in other social systems. For many reasons that are beyond the scope of this article, terrorist threats have been promoted to among the highest priorities in security policy in recent years, pushing aside the organizational and technical aspects of flight safety and device reliability; natural and environmental conditions of air traffic safety and continuity; economic and financial aspects; as well as other dimensions of safety related to individual travelers, including physical, mental, and occupational safety and health; crime (e.g. the smuggling of drugs, means of payment and illegal goods) and broader social issues such as staff strikes, conflicts with local communities, panic outbreaks, humanitarian disasters and crisis situations. Scientific and technical progress has ensured greater independence of air traffic from natural factors (e.g. atmospheric conditions) and increased the reliability of aircraft and airport infrastructure. From a security perspective, natural and technical threats are decreasing in likelihood and, accordingly, in priority. At the same time, threats caused by the human factor, not only inadvertent human errors but terrorist and criminological threats, are gaining in importance (Grzywna et al. 2018, 185).

Airports are a preferred target of terrorist operations for many reasons. Effective, tailored control and response measures are limited because of the increased congestion and the human flow at airports. Far from the days when air travel was still the privilege of the rich, air transport is increasingly accessible. Accordingly, terror attacks in airports target victims indiscriminately, and such attacks are socially perceived as an attack on the whole society, an event affecting everyone. These events arouse fear of leaving home, force people to change their behavior and undermines trust and confidence in the social order, which is, after all, the mission of terrorism. An additional factor that increases terrorist interest in civil passenger air transport is the uniquely spectacular, traumatic and symbolic nature of airplane disasters and dangerous incidents at airports. In addition, as air travel has become more accessible, it has achieved heightened strategic, economic and social importance and now plays a key role in societal infrastructures. Air transport systems are also inherently vulnerable to destruction or destabilization. All these circumstances make passenger air transport at once an attractive target for terrorist operations and an extremely difficult system to protect (Chorzępa 2019). No wonder that the era of terrorism coincided with the rapid development of passenger air transport in the second half of the twentieth century, and attacks on passenger planes or attempts to abduct them and attacks on airports, representing nearly 2.5% of total terrorist incidents, are now the second most common form of terrorist operations against transport systems after attacks on rail and metro systems (Nowacki et al. 2015, 8065). Unprecedented attacks on September 11, 2001 in the US, as well as a bombing at Moscow Domodedovo airport on January 24, 2011, the shooting down MH17 of Malaysia Airlines over Donbass on July 17, 2014 and bombings carried out by ISIS in the morning of March 22, 2016 at Zaventem Airport in Brussels have made societies painfully aware of the increasing vulnerability of air transport to serious terrorist threats and the need to continually strengthen and improve protections against such threats. There are many concerns about impact of terrorism on various life areas (Kordík, Kurilovská, 2017**;** Plėta et al., 2020; Masood et al. 2020; Chehabeddine, Tvaronavičienė 2020).

Therefore, concern regarding safety in civilian passenger aviation has grown and has rightly been promoted to the priority of international and national security policies, particularly as because passenger flows are increasing rapidly all over the world. Currently, air transport annually has over 3 billion passengers served (PAX) worldwide, of which nearly 700 million are EU citizens. These numbers are constantly growing due to various factors, including:

- Political, economic and cultural internationalization and globalization, the breakdown migration barriers (e.g. visas) and increasing human mobility;
- Demographic development, global population growth;
- Economic development and the growing prosperity of populations all over the world;
- Increasing accessibility of air travel, both price accessibility -- resulting from the increasing competition due to the expansion of LCC carriers -- as well as accessibility related to the progressive thickening of the airport networks, the connection network and the development of new concepts of complementary, inter- and multimodal transport, which integrates multiple means of transport into one harmonized system;
- The growing competitiveness of air transport compared to other modes of travel (rail transport, road transport) not only in terms of comfort and duration of travel, but also in terms of price - not only over traditionally long haul flights between time zones, but also short haul and domestic connections (cruises between cities, such as Warsaw and Rzeszów).

Air transport market analysts have identified a correlation between air traffic growth rate, measured in revenue passenger kilometer, and a country's GDP. The first indicator is usually higher by 2 percentage points (Ruciński, Madej 2016, 28). This coincides with the forecasts for the development of the passenger air transport market in Poland, whose growth dynamics for the number of passengers handled (PAX) by 2030 is expected to be above 5% per year (Ruciński, Madej 2016, 28).

The increasing complexity of threats as well as the increasingly sophisticated methods and measures used by the organizers of terrorist attacks make it necessary to constantly strengthen and improve airport security management and security systems so that these systems can meet new challenges. These challenges have engendered the implementation of more and more time-consuming and expensive security methods and measures, which are for most passengers completely inadequate and disproportionate. They are increasingly invasive, violating the privacy of travelers, significantly reducing travel comfort and causing travelers stress and dissatisfaction while straining security officers. However, simulation tests show that currently widely practiced non-selective security control procedures, despite their restrictiveness, are not very effective, and in combination with the growing flow of passengers at airports, they create overly long security lines, extending the duration of and wait time for check-in and security check. As a consequence, these non-selective protocols increase congestion at airports, which in turn cause additional security problems.

The problem of low efficacy of security controls, despite their widespread and mandated use, has recently been publicized in the media after leaks of secret reliability test reports that the Transportation Security Administration (TSA) -- the service responsible in the USA for transport safety, airport security and airport controls -- had carried out for fifteen years after the attacks on September 11, 2001 at several US international airports, including in Minneapolis-St. Paul International Airport. The test consisted of a "red team" of secret TSA agents acting as ordinary passengers who tried to smuggle 18 different prohibited items through security including dummy weapons, explosives, drugs, and other dangerous goods and materials. The leaked reports illustrated that in most cases items that should have been easily detected and confiscated as part of security checks were not detected or seized, and the test was finally terminated when the failure rate reached 95%. The TSA declined to comment on the leaks, condemning the disclosure of any information that could threaten the security of the American nation (Blake 2017). The US Department of Homeland Security referred to the case with a specially issued statement confirming that recent secret reliability tests conducted at many security checkpoints at US airports showed that controllers, devices and equipment or procedures had failed in more than half of the cases, and inspectors identified some gaps in the security control system. As a result, eight recommendations regarding sealing the system and improving its reliability were given to the TSA. The recommendations were classified as top secret in the interest of national security (Kerley, Cook 2017). Two years earlier, the American media had released additional secret reports concerning worryingly low effectiveness of airport security controls. The reporting also included the TSA's remediation program ordered by then-Secretary of Homeland Security J. Johnson. The agency launched a special training program for transport security officers and changed many procedures, including the reduction of long security lines. In the aftermath of the media storm, members of the US House of Representatives Homeland Security Committee demanded the immediate implementation of a recovery program, including replacing scanning equipment used at airport security control points with three-dimensional technologies and biometric scanners, as well as investment in security staff. According to American commentators, equipment changes have only been implemented at two airport checkpoints, and wider implementation has been inhibited due to budgetary constraints as President Trump's administration prioritizes the wall construction project along the Mexican border as a domestic security issue view (Kerley, Cook 2017).

Due to the unreliability and inefficacy of current airport security control procedures, according to aviation statisticians, by 2036 the number of check-in at airports will increase to 8 billion passengers per year (Nabożny 2019, 17), making it difficult to regard the current security control model as forward-looking and sustainable. Therefore, it is necessary to look for solutions that intelligently reconcile partially conflicting priorities: security requirements; economic interests related to cost-benefit optimization and adequate allocation of security resources based on realistic risk analysis; the need for a radical increase in the capacity of airport security checkpoints; ensuring smooth flow of airport traffic; shortening the security line and wait for check-in and security check; the need to make control procedures more flexible and to increase their adaptation not only to the actual risk level, but also to the traffic volume (Skorupski, Uchroński 2016), as well as requirements for personal data security, traveler's privacy protection and the convenience and satisfaction of passengers (Thomopoulos et al. 2018). The new forward-looking model of smart, modular, selective and multimodal security control must be primarily based on:

- Individualized and personalized procedures, including classifying travelers into various risk groups and utilizing accompanying control procedures;
- Early recognition, early warning and early response, including a procedure to check passenger credibility and begin the risk assessment at the moment tickets are purchased;
- Current scientific knowledge and innovative, technologically advanced tools and equipment solutions, including the latest achievements of psychology and cognitive science, security studies, criminology and criminalistics, computer forensics and artificial intelligence and autonomous systems, sensor engineering and detection technologies, crowdsourcing, identification and tracking of persons, intelligent remote image processing, computer image analysis, machine (algorithmic) behavior analysis, BigData and client mobile applications;
- Partial self-service, in accordance with the security model as a customer service, offering convenient, simplified and non-time-consuming forms of check-in and security check instead of requiring passengers to allow inspection of their personal information in order to travel.

2. Conditions for implementing the new model of smart airport security control

Historically, the visions and concepts of safety and security in passenger air transport and the changing standards of airport controls over time reflect a continuous learning process based on the "wisdom through damage" model. The intensification passenger hijacking for political reasons, which plagued Europe and the Middle East in the 1960s and 1970s, prompted the gradual tightening of airport security checks. As a result, since 1980 global regulations have required that all passengers are screened and subjected to highly invasive search procedures as part of personal checks, including detailed baggage checks up to the proverbial "last dirty sock." These checks widely criticized initially because of massive abuse, however, over time these security control standards also proved to be less and less useful as passenger aviation became subject to bombings carried out by the special services of hostile countries with excellent training, advanced technologies, large budgets and international networks of organizational cells. After the aircraft bombing at Lockerbie in 1988 (case Pan Am Flight 103), the regulations governing baggage checks were tightened and random scanning and searching of luggage for explosives was introduced. After the September 11 attacks, these checks became mandatory for all luggage without exception. Since 1992, in the USA, under the pressure of lobbying for low-cost air carriers seeking to reduce airport charges, security audits can legally be outsourced. As a result, since 1995 airports have turned to the cheapest, low-budget private security companies, which employ poorly qualified, underpaid workers to conduct airport security checks. It is widely believed that this had a significant impact on the selection of tactics for the September 11 terrorist attack against the US (Nabożny 2019). After the attacks of September 11, 2001, the Transportation Security Administration (TSA), an agency of the federal Department of Homeland Security of USA (also created after the September 11 attacks), was entrusted with responsibility for aviation safety and airport security.

In the European Union, the September 11 attacks led to the introduction of EU Directive 2320/2002, which aimed to counteract threats related to the abduction of passenger aircraft. Under the directive, airports established different security zones to which access is strictly controlled and requires certain permissions. The directive also introduced stricter standards for checking passengers and baggage as well as minimum requirements for items that travelers can take with them on board. It also imposed an obligation on Member States and airport operators to install their own technically advanced safety and security management systems and subject them to appropriate official supervision. Safety Management Systems (SMS) are a key element in ensuring air traffic safety and protecting airports, aircraft and port infrastructures (communication, logistics, service, etc.). The global civil aviation regulator -- the International Civil Aviation Organization (ICAO) -- requires operators of certified airports to implement a system based on a proactive formula of management focused on early recognition, prevention and early response to threats, including on the preparation of adequate action scenarios in the event of adverse events, emergencies or disasters (ICAO 2014, 6f.).

Such management requires the collection and processing of huge amounts of data and information relevant to security from as many sources as possible. What data and information can be relevant to security is determined by intelligence, imagination and experience. Materiality criteria relating to such information can be formulated only to a limited extent. The collected information must then be subjected to complex analyzes (preferably in real time), and the results obtained should be used for ongoing verification and, if necessary, to review and update the procedures for identifying and assessing threats and the ability to respond to accepted levels of tolerated and acceptable risk. The results can then be used to define the demand for specific resources necessary to ensure the desired level of security and protection (human resources, knowledge and competencies, equipment, financial, as well as authority) in addition to preventive, corrective, preparatory, documentary and other measures. The ICAO recommends the widest possible use of innovative solutions in the Safety Management System in the field of IT -- including electronic systems and devices -- to support the activities of airport services responsible for the implementation of comprehensive tasks in the field of security and safety. The basic infrastructure for the safety and security management system is a computer network that integrates and synchronizes the functioning of such system components as people identification systems and access control to restricted areas, anti-theft and alarm systems, exit blocks, video surveillance systems and CCTV, systems for protecting objects, devices and aircraft at parking spaces, airport fence protection systems and entrance gates, luggage transporting and control systems, body scanners, document and electronic signature readers, technical vehicle monitoring systems, time recording systems, motion sensors installed in lighting systems and parking management systems (ticket machines, gateways, signaling systems etc.) (Nowacki et al. 2015, 8069). In the case of airports, safety and security tasks can be assigned to two general objectives:

1) Those related to the ongoing service of aircraft traffic and the maintenance and development of necessary technical infrastructures. They include operations such as maintaining communication with aircraft located in the area managed by a given air traffic control service, providing aircraft crew with the necessary signals, information and instructions, securing landing (emergency if necessary), rescue operations, and ground operations including handling aircraft, parking, maintenance, and upkeep.

2) Those related to passenger and freight traffic. They include operations such as ticketing, baggage checks, passport and customs clearance, security controls for travelers, luggage and parcels, loading the aircraft and providing travelers with safe shelter in the event of delays or cancellations (Nowacki et al. 2015, 8069). This division of tasks and competences is often reflected in the organizational structure of airport safety & security services.

It is difficult to consider the world-dominant current model of safety & security management in passenger air transport and airport security smart, as airport operators use ineffective and mostly single-function, often technologically advanced infrastructures, despite the obvious benefits of synergies that would arise as a result of system integration. This article only allows for an overview of the growing problem of congestion at airports and the multidimensional importance of this problem for safety and security. In normal situations, the increase in congestion can be attributed to the ever-increasing flow of travelers; the progressive massification of air transport; the increasing needs of mobility; the intensification of migration processes; the increase in the price, spatial and reservation availability of air transport and their increasing compatibility with other transport systems; centralization processes related to the rapid development of large transit ports; the progressive thickening of the connection network and the enrichment global flight offerings with new, more distant travel available; the development of sustainable, integrated, intermedia and multimodal transport systems and the associated change in the function of airports and increased numbers of people not using air connections, dictated by price competition considerations; the continuous increase in transport volumes by exchanging the fleet for broad-body aircraft with higher payloads; as well as the pricing policy of carriers encouraging the use of cheap connections with long transfer times, among others. The problem of congestion is also intensified by the current, mandatory and detailed security checks required for all passengers carried out in the block system, the capacity of which is not flexibly adjusted to the level of danger or present traffic conditions. There is also an increase in congestion in emergencies, caused by flight delays or cancellations, serious incidents, weather conditions, staff strikes, technical failures or aviation accidents. Congestion has many negative and often even fatal consequences, ranging from objective problems with crowd management, monitoring of threats, ensuring order, protection of persons, property, important functions and infrastructures, detection and prosecution of crimes, typing potentially dangerous persons, conducting rescue operations , exploration and evacuation, as well as matching adequate security forces and measures, to subjective effects on passengers, which may increase the level of danger. For instance, congestion negatively affects the sense of security, and failure to meet territorial needs can act as a stressor for many people, leading to undesirable changes in behavior described by Calhoun as the "behavioral swamp." Under this phenomenon, congestion can lead to increased aggression, a sense of alienation, antisocial attitudes and behavior, a tendency toward anarchy, a refusal to comply, lack of solidarity, loss of interest in the fate of others and loss of readiness to help others, a decrease in the sense of responsibility, and satisfaction with other people's failures. Despite the obvious negative impact of crowding on airport security, most airports do not use any systems to monitor the number of people in the airport, which is problematic in terms of proper matching of forces and security measures. In practice, data on the number of people currently staying at the airport are not collected and analyzed (in real time). Airport facilities can in fact easily be equipped with electronic control systems to register the number of people entering and leaving; such systems are commonly used, for example, in other commercial facilities. Motion detectors, such as those that open automatic doors or turn on lights can be converted into person-tracking systems at almost no cost. Without knowing how many people are staying in a given facility at the moment, it is difficult to plan, let alone execute an adequate response in the event of an emergency or other undesirable situation. If it is necessary to evacuate people, it is difficult to determine with sufficient certainty whether after the evacuation operations whether people remain in the danger area, and if there are, how best to evacuate them. The constant availability of reliable data on the number of people in the airport at any given time allows for ongoing planning of preventive and protective measures as well as crisis response activities, in particular for estimating the current demand for resources (forces, resources, information, time), mobilization of reserves, launching procedures, planning breaks at work, as well as analyzing trends, early problem recognition and early response, forecasting future needs (e.g. personnel, equipment, procedural, etc.) and planning future tasks.

If the technical infrastructure existing at most airports were to be combined with technologies and network services commonly used by operators selling airline tickets, current security and security systems could be transformed into more smart systems based on personalized, selective, multi-module, partly autonomous (unmanned) and, to an extent, self-service security control procedures that could improve the reliability of these procedures and better ensure the security of passenger air traffic while increasing check-in capacity, reducing costs, shortening the waiting time for check-in and checking and the passenger's stay within the airport. These factors would combine to reduce congestion at airports, itself a security threat, while increasing convenience and making the passenger's airport experience overall more pleasant.. Such solutions have been successfully tested over recent decades at Israeli airports and check-in terminals at the Israeli state carrier El Al, which enjoys the reputation of being the best-protected airline in the world. The FLYSEC system operates on similar principles, although executed in a less invasive manner, developed and tested from 2015-2018 at the airport in Luxembourg in cooperation with the university as part of a pilot research and development project financed from the EU Horizon 2020 grant program. Additionally, smart, personalized security control systems can take advantage of modern computerized data analysis tools for travel history data and data from current bookings as well as algorithmic methods of behavioral analysis based on advanced detection, identification, crowdsourcing and tracking systems.

There are many visions for the meaningful use of artificial intelligence in behavioral analysis and assessment of individual's risk at different levels of the airport control system. Algorithms that recognize behaviors indicating stress, affective states and emotional arousal could revolutionize not only security controls carried out in terms of possible threats to public security (e.g. counteracting terrorist attacks), but also improve the detection of customs and fiscal crime, including smuggling Prohibited Goods (e.g. drugs, weapons, foreign exchange, counterfeit goods, prohibited articles under the CITES Convention) and illegal migration of persons (contingent upon forged documents).

These types of solutions can not only significantly increase the level of security in passenger air transport, but also would substantially improve the overall passenger experience by increasing comfort and satisfaction, minimizing time loss, reducing the stress of interacting with security agents or often-armed police officers, and reduce staff workload as well as the liability for errors or oversights.

3. Smart Airport Security Control Systems in Practice

Case El Al

Israeli state airline El Al, widely regarded as the best protected airlines in the world (Kohn 2002), is considered as a global pioneer in the implementation of intelligent, selective, prospective, personalized airport security control procedures (Kohn 2002), although this distinction does not mean the airline is the safest. Israeli airports and El Al check-in terminals employ some of the most restrictive control procedures in the world because of the complexity of the political situation facing this Middle Eastern country, tensions in relations with neighboring countries and a legacy of experiences with terrorism. Under the influence of bloody attacks and fear of danger, El Al was the first in the world to introduce legally and ethically controversial practices of racial profiling of travelers, the procedure of checking data recorded during the purchase of a ticket against data provided by leading intelligence services around the world and special crew training programs in the recognition and incapacitation of potentially dangerous persons. Passengers traveling on El Al flights must arrive to check in at least three hours before the scheduled departure and undergo an extremely meticulous security check. The check includes searching for passenger data in the FBI, INTERPOL, Canadian CSIS, British Scotland Yard and Israeli Shin Bet databases, a personalized interview conducted by security agents trained by special services aimed at detecting signals of insincerity or nervousness activating the “red lights” and control of luggage in a decompression chamber which simulate flight conditions in order to cause detonation of any explosives hidden in luggage. These security measures are implemented even though every passenger who goes to the airport has already been meticulously checked for security with the help of personalized electronic databases and the most advanced surveillance technologies. Each passenger is then re-checked when entering the airport in Tel Aviv. The airport infrastructure is specially designed so that even toll gate and release thresholds are part of the security system. Someone who drives too fast or too slow is immediately registered and qualified for additional control. Suspicious cars or people are searched by armed guards in the parking lot before they can even approach the terminal building. It is also common practice to thoroughly search the contents of luggage in the event that a scanner detects suspicious items. Terminals and planes of this line are equipped with a system of detectors specifically for explosives both on travelers and in luggage, and are also equipped with technologically advanced monitoring systems. Since the 1960s, El Al flights are the only ones in the world to employ specially trained and armed ‘sky marshals’, who travel incognito on every flight to ensure passenger security and react to any suspicious behavior of travelers. The sky marshals serve as the last layer of security in the whole system. Any security agent intervention means that the security system failed.

The signal that evokes the greatest mobilization of services is haste. If the Turkish proverb “The devil takes a hand in what is done in haste” holds true, it is most prominently on display at Ben Gurion airport in Tel Aviv. People who hurry to the plane are more likely to be interviewed for hours than to board. Finally, it is worth mentioning an important detail that differentiates security at Israeli airports from airport security in other countries: despite the fact that almost half of the staff at the airport are involved in security, security is almost invisible. Security agents dressed in civilian clothes hide automatic weapons under sweaters and it is usually difficult to spot people in uniforms, while in the US, the European Union or Russia there are conspicuous uniformed officers throughout airports, although their visibility has not prevented attacks or incidents in recent years. At an Israeli airport, only an attentive observer would realize that from time to time the same people dressed civilian clothing check the bins and look behind the vending machines in search of explosives. It is most likely that a traveler’s first encounter with security will be a discussion with a young woman, appearing to be a student and dressed in a t-shirt and jeans, a few questions to check if the answers match the secret profiles of people suspected of terrorism (Kohn 2002).

Thanks to extraordinary control and security procedures, there has been no attack on Israeli air routes or passenger aircraft in recent years. Potential perpetrators are aware of the low chance for such operations to succeed.

FLYSEC

The Interdisciplinary Center for Security, Reliability and Trust (SNT) of the University of Luxembourg together with the Luxembourg Airport and ten other partners carried out a research and implementation project FLYSEC founded by the Horizon 2020 Framework Program of the European Union for Research and Innovation (www.fly-sec.eu) from 2015 to 2018. As part of the project, an innovative, integrated, technologically advanced, comprehensive airport security system was developed and tested. The system aimed to achieve all three priorities of the IATA / ACI Smart Security program: strengthened security, increased operational efficiency and improved passenger experience. The FLYSEC system was designed in accordance with the security management paradigm based on risk assessment and customer service, and is centered around discreet, personalized security controls able to conduct individual risk assessments for each passenger and while incorporating self-service elements. The goal of the project was to increase airport output and to eliminate long check-in queues while improving security by increasing the efficiency of passenger checks, replacing random personal checks with targeted procedures while improving passenger comfort and satisfaction at the same time. The individualized risk assessment is based on data on travel history, results of previous security checks and passenger booking profiles. As part of the initial security check, passenger data is analyzed to classify and select passengers into three risk categories: trusted passenger, normal passenger and high-risk passenger. Depending on the results of the initial check, passengers in different risk groups are assigned to different restrictive control procedures after arriving at the airport (so-called virtual secure tunnels). From the moment the passenger arrives at the airport, the FLYSEC system builds upon the initial risk assessment with data collected through a special mobile application assisting passengers during check-in, security checks and moving around the airport. These data allow passive monitoring and intelligent analysis of passenger behavior from the moment the traveler enters the airport hall up to the moment of he or she boards the plane, using traffic patterns to identify unusual or suspicious behavior early and direct travelers for additional, more thorough control procedures if necessary. Passenger risk analysis is continuous, security management is agile and flexible, and the passenger can be suddenly redirected to another secure tunnel if needed. In terms of technology, the FLYSEC system integrates modern solutions in the field of artificial intelligence, sensory engineering, video monitoring and video surveillance, computer vision analytics, intelligent remote image processing, biometrics, big data analysis, crowdsourcing, RFID, mobile application technologies with the latest scientific achievements, primarily all in the area of behavioral analysis, neuroscience and cognitive science and machine learning algorithms (Kyriazanos et al. 2016). The system also has a built-in methodology to check the correctness of operations, allowing the algorithms to self-improve continuously.

During the Luxembourg International Airport pilot field test in 2018 in a real operational environment with active security personnel, a group of 100 volunteers had the role of passengers and recreated various scenarios including adverse and hazardous events. The test results have demonstrated a high level of technological readiness of the FLYSEC system and have shown that improving the level of security, improving the efficiency of airport operations and improving traveler experience do not have to be mutually exclusive.

4. Controversies

Despite the indisputable advantages of an intelligent, selective, personalized airport security control model compared to the standard control procedures, mandatory for all without exception, the execution of such innovative solutions is always met with social skepticism, as well as legal and ethical controversies due to fear of unauthorized invigilation and misuse by security services, discrimination, data theft or leakage and the potential for dreadful consequences of machine errors in addition to countless cyber threads. Those controversies are not altogether new, most of them are well-known from social debates concerning the ethical and legal considerations around citizen invigilation by online activity tracking tools or video monitoring in public spaces. However, the current control procedures used at most airports are also not entirely free of ethical and social controversies or objections. It bears remembering that the primary objective of new security procedures is the broad understanding of the rationalization for security management and protective procedures Admittedly, the pillars of the current security management system in civil aviation are important principles on which European legal order is based: universality, equality, security and data protection as well as respect for privacy. However, it is clear that such an egalitarian understanding of security requires subjecting to the same restrictive, embarrassing and ultimately unnecessary control procedures hundreds of millions of people who pose no threat to air traffic. Therefore, it seems that apart from certain cultural stereotypes and prejudices, there are no obstacles to profile and categorize people in terms of safety, and to select high-risk passengers and qualify them to additional control procedures.

The assessment of the social acceptability of a new, intelligent model of selective, personalized security control based on risk analysis and advanced technologies depends on the context, which encompasses level of awareness, political situation, possessed experience, value systems and safety & security culture among other factors. However, it seems that despite sincere sympathy for such values as equal treatment, privacy and informational self-determination, profiling, sorting people based on risk cannot be abandoned entirely in the present day as far as safety and security in civil aviation go, primarily because terrorist organizations are growing in strength, possessing great capital and are using increasingly sophisticated actions (Kohn 2002). Finding a bomb has become increasingly difficult, as explosives no longer feature the characteristic protruding fuse, but rather can resemble any object, have any shape and be made of many types of materials. It is much easier to identify a terrorist, even in a dense crowd, but this requires profiling and typing passengers that match specific profiles and behavioral patterns. Initial profiling based on data stored in electronic systems and observation and analysis of behavior does make it much more difficult to identify naive people unaware that they are used by terrorists. Kohn recalls the example of a pregnant Irishwoman, Anne Marie Murphy, who in 1986 took a trip on an El Al flight from London to Tel Aviv to meet the parents of her fiancé, a Palestinian. She was unaware that the wedding was in fact false, and that her fiancé hid a bomb, made of plastic with a chemical detonator invisible even to 3D luggage scanners, in her luggage. Thanks to an interview with the Irish woman during the check-in, Israeli security agents happened to learn of her fiancé and, having grown suspicious, decided to check the contents of her luggage in detail, likely saving the lives of more than a hundred people.

Invasive profiling practices, a complete lack of understanding of the need for privacy and confidentiality are the price to pay for fragile security guarantees in Israel. Ongoing tensions mean that the authorities cannot afford any oversight. However, since no human-made system is perfect, mistakes also happen there. The writer Rosemary Mahoney from Rhode Island experienced it on a one-way El Al flight from Mumbai to Tel Aviv. Without any evil intentions or connections to terrorist organizations, Rosemary Mahoney was selected as a high-risk passenger on the basis of profiling, namely, that she had traveled to Egypt several times, had a Syrian visa and had purchased a one-way ticket. After several hours of interrogation and a thorough search of luggage up to the “last dirty sock” Rosemary Mahoney was finally allowed to board another plane (Kohn 2002). After the September 11 attacks, Rosemary Mahoney voiced support for El Al’s conduct and advised Americans to follow Israeli practices.

The combination of discrete, machine, partially autonomous and remote, non-interactive analytical control procedures with security functions operated by the passenger himself with the help of mobile applications gives rise to a certain other psychosocial problem. Security checks are not only intended to detect and eliminate threats, but also give passengers a sense of security -- in this sense they also have a symbolic, ceremonial function. It can therefore be assumed that intelligent, selective control procedures will counterproductively affect the collective sense of security, which may result in additional problems.

Certainly, for many different reasons, automated personal control procedures would be desirable. These systems come with their own pitfalls, however, including the “madness” of collecting useless data (which can compromise effective security), data abuse, lack of full anonymity and difficulty evaluating the materiality of flagged risks, but above all with the aforementioned impossibility to ensure an adequate level of privacy protection. Undoubtedly, the most serious obstacle to implementing intelligent, selective airport control procedures will be overregulation in the field of personal data security and privacy protection in Europe.

The interests of collective security and individual protection and the invasive techniques of preventive surveillance, profiling and selection of passengers associated with them certainly conflict with the legal and ethical standards of protection of individual fundamental rights, including the right to privacy, confidentiality and anonymity, the right to informational self-determination and the right to equal treatment. However, the fundamental conflict between the interests related to the protection of privacy and the interests related to the protection of the individual and the community against the unpleasant consequences of protecting the privacy of dangerous persons is not to be overlooked. Therefore, such solutions should not be introduced by force, but should be enacted through consulting with and agreement from governing bodies and their citizens. Ultimately, the problem of assessing the social acceptability of this type of solution boils down to the choice of priorities, which should be carried out on socially fair terms and preceded by social discourse and the process of social learning. In the course of such discussions, it is unlikely that those involved will entirely resolve the conflicting needs across technical (e.g. computing capacity), economic (cost-benefit analysis), legal and ethical (legality of new solutions and possible legislative needs, civil rights and freedoms, data security and privacy protection), the calculation of goods and the distribution of damages (benefits and setting norms), social (acceptance issues, conflict-forming potentials, conflict resolution and consensus building) and cultural (travelers' preferences, ethno-cultural conditions) considerations. Resolving such issues would require undertaking appropriate scientific research and conducting a comprehensive, comparative technology assessment. A rational, ethical assessment of the acceptability of a possible breach of passenger privacy and confidentiality could be based on the principle of pragmatic consistency, which justifies exposing other people to certain risks without their knowledge or consent, provided that they do accept comparable or larger risks (Gethmann, Kloepfer 1993, 42-45). Societies must also consider that the high price paid for improving security through the use of intelligent, selective airport control procedures based on invasive profiling techniques ultimately will not guarantee full protection against terrorist threats or other threats caused by human factors. In the case of the writer Rosemary Mahoney, the alarm activated in the system turned out to be false, while in the case of Anne Marie Murphy the system failed and both she and her fellow passengers owed their rescue to the security agent's questioning. In the current global geopolitical context, however, security strategists are best served by the strategy that Hans Jonas referred to as "heuristics of anxiety" (Jonas 1984): the socially destructive impact of certain traumatic events means that protective measures must include a full mobilization of all available forces and means to counteract such events, and that those responsible for protecting civilians must wake up every day with the unwavering conviction that there will be an attack that morning. With this approach, for a rational society of people interested in protecting themselves and their loved ones, no price for security is too high.

References:

Blake A. (2017). *TSA failed to detect 95 percent of prohibited items at Minneapolis airport: Report*, in: „The Washington Times", Jul. 6, 2017.

Chehabeddine M., Tvaronavičienė M. (2020). Securing regional development. *Insights into Regional Development*, 2(1), 430-442. http://doi.org/10.9770/IRD.2020.2.1(3)

Chorzępa V. (2015). *Problemy ochrony niewielkich międzynarodowych portów lotniczych przed zagrożeniami terrorystycznymi na przykładzie Portu Lotniczego Rzeszów-Jasionka* [Problems of Small International Airport Protection against Terrorist Threats on the Example of the Rzeszow-Jasionka-Airport], Rzeszow University of Technology (diploma thesis manuscript, in Polish)

Gethmann C.F., Kloepfer M. (1993). *Handeln unter Risiko im Umweltstaat*, Springer, Berlin et al.

Grzywna Z., Limański A., Drabik I. (2018). *Zarządzanie bezpieczeństwem w portach lotniczych* [Airport Safety Management]. *Zeszyty Naukowe Politechniki Śląskiej. Organizacja i Zarządzanie*, 118(1), 181-197.

International Civil Aviation Organization (2014): *Safety Management Manual (SMM)*, ICAO Doc 9859, Montreal

International Civil Aviation Organization (2018), *ICAO Safety Report 2018*, Montreal

Jonas H. (1984). *The imperative of responsibility. In search of an ethics for the technological age*, University of Chicago Press, Chicago&London

Kerley D., Cook J. (2017). *TSA fails most tests in latest undercover operation at US airports*, in: „ABC News", Nov. 9, 2017.
Kohn D. (2002). *The Safest Airline. A Secure Example Set by Israel`s El Al*, in: „CBS News", Jan. 15, 2002.

Kordík M., Kurilovsk, L. (2017). Protection of the national financial system from the money laundering and terrorism financing. *Entrepreneurship and Sustainability Issues,* 5(2), 243-262. http://doi.org/10.9770/jesi.2017.5.2(7)

Kyriazanos D.M., Segou O.E., Zalonis A., Thomopoulos S.C.A. (2016). *FlySec: a risk-based airport security management system based on security as a service concept*, in: SPIE-Proceedings „Signal Processing, Sensor/Information Fusion, and Target Recognition" XXV Vol. 9842, (17 May 2016) https://doi.org/10.1117/12.2224031

Masood O., Javaria, K. Petrenko Y. (2020). Terrorism activities influence on financial stock markets: an empirical evidence from United Kingdom, India, France, Pakistan, Spain and America. *Insights into Regional Development,* 2(1), 443-455. https://doi.org/10.9770/IRD.2020.2.1(4)

Nabożny D. (2019). *System zarządzania bezpieczeństwem i ochrony portu lotniczego Rzeszów-Jasionka* [Safety & security management system of the Rzeszów-Jasionka-Airport], Rzeszów University of Technology (diploma thesis manuskript, in Polish)

Nowacki G., Olejnik K, Woźniak G. (2015): *Analiza zagrożeń terrorystycznych dla sektora transportu lotniczego [Analysis of Terrorist Threats for Air Transportation Sector]*, in: „Logistyka", 4 (CD2), 8063-8071 (in Polish)

Plėta T., Tvaronavičienė M., Della Casa, S. (2020). Cyber effect and security management aspects in critical energy infrastructures. *Insights into Regional Development,* 2(2), 538-548. https://doi.org/10.9770/IRD.2020.2.2(3)

Ruciński A, Madej K. (2016). Polski rynek transportu lotniczego w perspektywie 2030 roku [Polish air transport market in the perspective of the year 2030]. *Studia Oeconomica Posnaniensia*, 4(7), 7-38. (in Polish)

Skorupski J., Uchroński P. (2016). Dostosowanie systemu kontroli bezpieczeństwa bagażu rejestrowanego do wielkości ruchu [Adjustment of the hold baggage screening system to the traffic volume]. *Prace Naukowe Politechniki Warszawskiej. Transport*, 114, 303-314 (in Polish)

Thomopoulos S.C.A., Kyriazanos D.M., Zalonis A. (2018). *FLYSEC: A comprehensive control, command and Information (C2I) system for risk-based security*, in: SPIE-Proceedings „Signal Processing, Sensor/Information Fusion, and Target Recognition" XXVII Vol. 10646 (25 June 2018) https://doi.org/10.1117/12.2500144

Krzysztof MICHALSKI is a doctor in the Department of Security Sciences at the Faculty of Management at Rzeszów University of Technology. Research interests: philosophy of science, safety theory, technology assessment.
ORCID ID: 0000-0002-2089-2160

Marcin JURGILEWICZ is the Professor at Rzeszów University of Technology, PL. Head of the Department of Safety Sciences. Research interests: internal security, law, mediation.
ORCID ID: 0000-0003-2243-2165

Mariusz KUBIAK is the Professor at University of Natural Sciences and Humanities in Siedlce. Research interests: cultural security, issues of contemporary wars and armed conflicts.
ORCID ID: 0000-0002-6757-5509

Anna GRĄDZKA is the master at Johns Hopkins University in USA. Research interests: national security with a focus on Eastern Europe. **ORCID ID:** 0000-0002-7096-947X