Polish Political Science Yearbook, **vol. 51(2) (2022), pp. 69–87**
DOI: https://doi.org/10.15804/ppsy202148 PL ISSN 0208-7375
www.czasopisma.marszalek.com.pl/10-15804/ppsy

Gabriel Nowacki
Military University of Technology (Poland)
ORCID: 0000-0001-5357-8824
e-mail: gabriel.nowacki@wat.edu.pl

Bohdan Paszukow
Aviation Security and CBRN, EDD, EU COM Working Group (Poland)
ORCID: 0000-0003-3142-7624
e-mail: bohdan.paszukow@gmail.com

Selected Problems of Security Control in Civil Aviation Based on Own Empirical Research

Abstract: The paper refers to the evolution of methods, new technologies, and devices in security control processes in light of civil aviation requirements, procedures, and increased flow of passengers. The research problem has been defined as follows: How shall the international airport security controls function in the context of regulatory and operational conditions and current and future threats? In reference to the problem, the research hypothesis was defined as follows: Security control in civil aviation consists of screening persons and detecting prohibited articles and mainly depends on the professional competence of security staff and the proper selection and maintenance of electronic assistive devices. Professional competences refer to personnel's knowledge, experience, qualification, monitoring, operational supervision, and quality control as part of their tasks. The development of new technologies requires the appropriate selection, commensurate with risk analysis, of electronic assistive devices, including equipment, methods, technical means, and their maintenance in a proper technical condition. The paper presents the results of empirical research conducted amongst experienced aviation security forums. Because of its complexity and unpredictability, this problem still leaves a wide margin for improvement and efficiency. The following research methods were used to solve the research problem: theoretical methods and empirical methods: diagnostic survey and expert interview.

Keywords: *security control, terrorism, civil aviation, new technology*

Introduction

Before approaching the screening position, it must be ensured that there are no prohibited or dangerous articles in cabin baggage. All metal objects with which passenger or airport personnel enters such as keys, watches, belts, mobile phones, coins, etc. and larger electronic devices such as laptops (depending on the type of x-ray equipment used) should be placed in special trays and placed on the belt of the X-ray machine together with the cabin baggage. The airport staff performing the screening will also ask us to put the outer garment such as jackets, blazers, jackets in the plastic trays. In addition, security personnel might ask a passenger to remove shoes to be subject to additional screening. All liquids, gels, and aerosols that we want to bring on board should be placed in containers with a maximum volume of 100 ml/100 g and should fit into one transparent, resealable plastic bag not exceeding one liter (aforementioned depends on the type of x-ray equipment used).

According to ICAO and IATA data, 4.4 billion passengers were checked in at international airports in 2018 and 4.5 billion passengers in 2019.

ICAO has confirmed that international passenger traffic suffered a dramatic 60% drop over 2020, bringing air travel totals back to 2003 levels (ICAO, 2021). ICAO reports that as seat capacity fell by 50% last year, passenger totals dropped by 60%, with just 1.8 billion passengers taking to the air during the first year of the pandemic, compared to 4.5 billion in 2019. Its numbers also point to airline financial losses of 370 billion dollars resulting from the COVID-19 impacts, with airports and air navigation services providers (ANSPs) losing a further 115 billion and 13 billion, respectively.

In 2020, Polish airports handled 14.5 million passengers, i.e., by 70% less than the previous year. The last time a smaller number of passengers was handled was 15 years ago (ULC, 2021).

Security incidents impact travelers, especially when they cause injuries and fatalities, and significantly reduce confidence in air travel and related commercial exchanges. The current threat and risk environment require that aviation security remains one of the highest priorities for states and the global international community.

During 2011-2016, 69 acts of unlawful interference were recorded in air transport. Fatalities were in 21 cases (884 people). The highest number of attacks on-air facilities were incidents – 24 (32%), followed by attacks – 18 (26%), sabotage – 15 (22%), and other acts – 12 (17%). Improvised explosive devices (IEDs) are most commonly used to attempt attacks on civil aviation infrastructure and airports, and therefore security control systems play a key role in deterring and detecting threats in the aviation security system. In addition, attacks against areas adjacent to airports (public areas) have highlighted the growing threat to the very places where passengers gather before departure.

Moreover, in order to cope with the challenges posed by increased security regulations and the growing number of passengers and to keep abreast of the latest terrorist

threats, airports in Europe and worldwide are increasingly seeking new technological solutions tailored to the individual needs of both themselves and their customers, i.e., passengers.

Airports and other actors actively involved in building a secure airport ecosystem must always consider the human factor and state-of-the-art technology solutions. Therefore, airports are an ideal testing ground for integrating new technologies to reap the benefits of global passenger traffic growth and attract further direct or indirect investment.

In order to solve the main research problem of the paper and verify the research hypothesis, qualitative and quantitative research methods were used:

- system analysis enabled the solution of the complex problem of the airport security controls,
- analogy, it was used to formulate a research hypothesis and search for similarities between issues in the field of aviation security,
- the statistical method allowed for the acquisition, presentation, and analysis of data describing incidents in civil aviation,
- the analytical method allowed for the consideration of the organization of airport security controls,
- a comparative method, based on which basic mechanisms of safety implementation in the field of airport control,
- behavioral method, which made it possible to recognize and explain by observing the behavior of passengers,
- empirical methods: a diagnostic survey was carried out to collect the data based on an anonymous questionnaire prepared for the study and expert interviews.

As part of the adopted research methodology, the following independent variable was distinguished: the international airport environment and the dependent variable: international airport security status.

1. Characteristics of Security Control

1.1. Terrorist Threats

The terrorist attacks in 2001 (US) opened a new era in air transportation. Airports have become the main focus in implementing security control procedures (De Barros & others, 2010).

The need to more thoroughly screen passengers and baggage, and the consequent increase in processing time, has created the need for more space for security checkpoints and baggage screening inside passenger terminal buildings. Quantification of those impacts is performed with the use of discrete-event simulation and spreadsheet models.

Tab. 1. List of aviation terrorist attacks between 2001 and 2017 (CNN, 2020; Wolniak, 2019)

No	Date	Type of attack	Victims
1.	11.09.2001	Nineteen Al-Qaeda members hijacked four aircraft with passengers: two of them hit the World Trade Center skyscrapers, causing them to fire and collapse, one hit the Pentagon, and the fourth, on which passengers tried to overpower the hijackers, crashed near Pittsburgh.	Over 3,000 were killed people, and several thousand were injured.
2.	07.05.2002	A McDonnell Douglas MD-80 nearing its destination of Dalian, China, reported fire in the cabin. The investigation determined that the passenger used gasoline to set fire to the cabin after purchasing several life insurance policies. Most passengers died from carbon monoxide inhalation. None survived the crash.	112 people were killed.
3.	05.03.2003	5 March – Abu Sayyaf claimed responsibility for the bombings in Davao International Airport in the southern Philippines,	21 people were killed and 148 injured.
4.	24.08.2004	Two domestic Russian passenger flights, a Tu-134 and Tu-154 airliner, crashed within minutes of each other. An investigation found traces of RDX high explosive at both crashes and determined Chechen suicide bombers to be responsible.	44 people were killed from first and 46 from second.
5.	30.12.2006	An explosion of a bomb planted by ETA at Barajas airport near Madrid.	Two missing persons, 26 wounded.
6.	30.06.2007	A bombing at Glasgow airport.	Five people were injured.
7.	24.01.2011	A bombing at the Domodedovo airport near Moscow (Russia).	36 people were killed, 180 people were injured.
8.	18.07.2012	A bombing at Burgas airport, caused by a suicide bomber.	Seven people were killed, and 32 were injured.
9.	17.07.2014	Plane Crash - Malaysia Airlines MH17. He was probably struck by an air-to-air rocket by separatists.	298 people were killed, including 15 crew members.
10.	31.10.2015	An Airbus 321 flying from Egypt to Saint Petersburg broke up above the Sinai, killing everyone on board, becoming the deadliest air disaster in Russian history. ISIL claimed responsibility. Russian investigators found explosive residue, and Egyptian authorities agreed it was a terrorist act.	224 were killed.
11.	22.03.2016	three coordinated suicide bombings were in Zaventem Airport in Brussels. ISIL claimed responsibility for the attack	16 people were killed and 83 300 injured.
12.	28.06.2016	The attack, consisting of shootings and suicide bombings, occurred at Istanbul Airport. Shooters armed with automatic weapons and explosive belts staged a simultaneous attack.	45 people were killed and over 230 injured.

The need to more thoroughly screen passengers and baggage, and the consequent increase in processing time, has created the need for more space for security checkpoints and baggage screening inside passenger terminal buildings. Quantification of those impacts is performed with the use of discrete-event simulation and spreadsheet models.

In 2018, terrorism continued to pose a severe security threat to the EU Member States. Terrible attacks by jihadists such as those from Trèbes, Paris, Liège, and Strasbourg resulted in thirteen deaths and many other injuries. Terrorists aim not only to kill and mutilate but also to divide our societies and spread hatred. The forces responsible for security must remain vigilant to protect citizens and values in the face of attempts to use violence for political purposes.

As regards airport ecosystems, action is needed to divert attention from checkpoints toward public areas at airports to adapt to the changing threat, as illustrated by many recent attacks. The essence of the new approach should no longer be to focus only on preventing dangerous goods from entering critical areas of airports, but also on both sides of the checkpoint, i.e., in de facto public places where air and ground transport systems intersect, such as high-speed trains, subways, and passenger handling points for surface transport such as buses and cars.

Since the attacks of 11 September, countries and airports around the world have strengthened airport security measures. However, over the last few years, terrorist attacks have increasingly focused on areas where people are not screened, such as baggage collection or check-in areas.

Airport security measures from 2001 have been grouped into two types: standardized screening techniques, which all passengers must undergo (e.g., baggage X-rays, metal detecting scans); and elevated-risk screening (including pat-downs, strip searches) for which only a sub-set of passengers are selected.

The results of the research made by ACI and IATA indicated that while both are similarly considered by travelers, high-security measures introduce added concerns regarding personal privacy and the heightened potential for humiliation; this caused the perceived dignity threat for elevated procedures to exhibit much stronger negative relationships with perceived safety and with enplanement intentions (Alards-Tomalin et al., 2014).

The double attacks at Brussels airports and train stations in March 2016 using this tactic killed 32 people and three attackers. It shows that we are facing ambitious opponents who are constantly looking for a place to attack in both the real world and cyberspace and are only waiting for the opportunity to strike again (Shapiro, 2016).

Given the current catalog of threats against airports, there is a continuing need to update and strengthen security solutions by using a new assessment of today's threats and speeding up the modification of security strategies in airport areas. Below, the authors present several key challenges and trends related to developing new technologies for airport security and their ecosystems and checkpoint infrastructure.

1.2. Legal Bases for Security Control

According to Regulation 300/2008/EC, all departing, transfer, and transit passengers and their cabin baggage shall be screened to prevent prohibited articles from being introduced into restricted security areas and on board an aircraft.

Transfer passengers and their cabin baggage may be exempted from screening if they:

- arrive from a Member State, unless the Commission or that Member State has provided information that those passengers and their cabin baggage cannot be considered as having been screened to the common basic standards,
- arrive from a third country where the security standards applied are recognized as equivalent to the common basic standards under the regulatory procedure.

Transit passengers and their cabin baggage may be exempted from screening if they:

- remain on board an aircraft, have no contact with screened departing passengers other than those who board the same aircraft,
- they arrive from a Member State unless the Commission or that Member State has provided information that those passengers and their cabin baggage cannot be considered as having been screened to the common basic standards,
- they arrive from a third country where the security standards applied are recognized as equivalent to the common basic standards under the regulatory procedure.

The following Parties are responsible for carrying out the tasks related to screening (Regulation EC, No 300/2008):

- The manager of the airport in relation to:
  - persons other than passengers and items carried by them,
  - passengers and cabin baggage,
  - hold baggage,
  - air cargo and mail, air carrier mail and air carrier materials, in-flight supplies, and airport supplies before being granted access to the restricted security area, unless the airport operator, air carrier, known consignor of airport supplies, or regulated supplier of in-flight supplies has applied the required security controls within the meaning of Regulation (EC) No 300/2008,
- a regulated agent within the meaning of Regulation No 300/2008/EC in respect of freight and mail,
- a regulated supplier of in-flight supplies within the meaning of Regulation (EC) No 300/2008 in respect of in-flight supplies or an air carrier that delivers supplies to its aircraft. The tasks in Poland are performed under the President of the Office, who cooperates with the Border Guard. The airport manager performs the tasks in cooperation with security services operating at the airport.
- The Airport Security Service shall perform the tasks of the managing body of the aerodrome regarding

- carry out security checks,
- access control to restricted security areas,
- checks on passes issued by the airport managing body,
- capture and transfer to the Police or the Border Guard of a person (violating airport security conditions and a passenger violating transport conditions, a person who without authorization obtained or attempted to obtain access to the restricted area of the airport, a person who committed or attempted to commit an act of unlawful interference, a person who otherwise violates public order),
- security of restricted areas and other areas within the meaning of Regulation 300/2008/EC.

If it is necessary to perform tasks exceeding the competence of airport security services, the airport manager shall notify the Border Guard or the Police.

The President of the Civil Aviation Authority may recognize a certificate of a security control operator issued in another Member State of the European Union, the Swiss Confederation or a Member State of the European Free Trade Association (EFTA) – a party to the Agreement on the European Economic Area or by the International Civil Aviation Organization or another international aviation organization – as valid on an equal footing with a Polish certificate of a security control operator, unless the requirements for its issue were less stringent than those imposed in the Republic of Poland, after applying to the commanding officer of the Border Guard Division for information on the lack of negative premises for performing security control in civil aviation by that person.

Recently, the Convention for the Suppression of Unlawful Acts Relating to International Civil Aviation (Beijing Convention) and the Protocol to the Convention for the Suppression of Unlawful Seizure of Aircraft (Beijing Protocol) have strengthened the global legal framework for dealing with cyber-attacks against international civil aviation.

Cyber-security is a priority in the EU's global foreign and security strategy. In the cyber security chapter, the EU global strategy mentions the EU's willingness to increase the focus on cyber security, equipping the EU and helping Member States protect against cyber threats while maintaining an open, free and secure cyberspace (EU Global Strategy, 2016).

In 2013, the Council welcomed the European Union Cyber Security Strategy and underlined the need and urgency to develop and implement a comprehensive approach to EU cyberspace policy. In 2014, The Council adopted the Cyber Defense Policy Framework (CDPF), setting out priority areas for promoting civil-military cooperation and synergies with broader EU cyber security policies, relevant EU institutions, agencies, and the private sector. These areas have recently been reviewed to adapt to the changing environment of cyberspace and EU security and defense initiatives related to the implementation of the EU global strategy (EDA, 2013).

In September 2017, The Commission launched an updated package of cyber security initiatives through a Joint Communication on "Resilience, deterrence, and defense". It concluded that the threat landscape had grown significantly with progressive digitization and

the associated benefits of linking the economy and society to related objects via the Internet of Things.

1.3. Security Control Process

After the Spanair 5022 aircraft crash in 2008, which occurred shortly after take-off from the runway, it was discovered that the central computer system used to monitor technical problems in the aircraft was infected with malware. An internal report issued by the airline revealed that the infected computer had not detected three technical problems with the aircraft, which, if detected, could have prevented the aircraft from taking off. The malware was found to be a Trojan horse (CAA Spain, 2008).

In 2010, the FAA (Federal Aviation Administration) published a notice indicating that some Boeing 747-8 and 747-8F computer systems may be vulnerable to external attacks due to the nature of their communications (Kirby, 2010). Therefore, solutions have been taken to move some processes into the so-called virtual space (cloud operations) to improve efficiency, reduce initial capital investment and offer flexibility to adapt to passenger flows.

In 2014, ICAO explored how innovative technologies might enhance efficiency and threat detection and examine policy and operational challenges stemming from the combination of equipment, privacy and health concerns, operating concepts, human factors, and airport environments (ICAO, 2014). Among the technological areas to be addressed are advanced screening equipment, access control systems, surveillance, and the use of security barriers. Next-generation security checkpoints, for example, might integrate technology with intelligence, behavioral analysis, and passenger data. Biometric data could help verify a passenger's identity and determine the appropriate level of screening. Enhanced screening technology may allow passengers to keep personal electronics and liquids in their bags and eliminate the requirement to remove coats and shoes.

According to Commission Implementing Regulation of 5 November 2015 (EU, 2015/1998), the airport operator will conduct security checks at the entrance to the restricted security area of the airport at least of the following: liquids, aerosols, and gels purchased at the airport or on board an aircraft, which are enclosed in tamper-evident bags, clearly displaying appropriate evidence of their purchase in the airside of the airport or on board an aircraft, as well as liquids, aerosols, and gels intended for use during travel for medical treatment or due to special dietary requirements, including baby food.

In 2017, the UK government introduced a ban on the in-flight transportation of electronic devices for flights from certain countries in the Middle East and North Africa. As a result, passengers flying from certain airports in Tunisia, Turkey, Egypt, Lebanon, Jordan, and Saudi Arabia to Europe were banned from transporting items such as phones, laptops, and tablets to prevent potential terrorist threats. The ban was lifted in August 2018, but it was an impulse for technology companies to start finding new technologies for detecting explosives in electronic devices (UK Lifts, 2018).

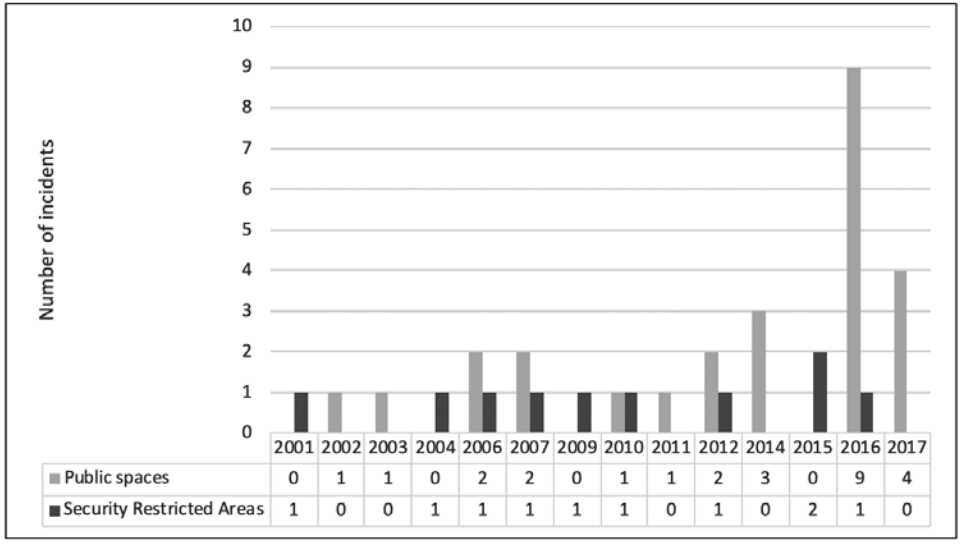
Hybrid threats are becoming evident, and cybercrime is expected to continue to grow until 2021, costing businesses worldwide more than €5 trillion per year (CSIS, 2017).

An automated border control system that allows travelers to be tested using lie detector avatars may soon become a reality. The aim is to speed up queues and increase security at the EU's external borders. The "IBORDERCONTRI" project aims to develop intelligent border control systems by developing a series of questions via animated border guards on screen before they reach the border, whether on land, air, or sea, using questions adapted to gender, ethnicity, and travel language (IPCS, 2016).

In 2015, the European Union issued standards for explosive detection systems in cabin baggage (EDS CB). The European Civil Aviation Conference (ECAC) is the main body behind equipment testing and performance management. It has resulted in the deployment of CT technology at checkpoints. However, the regulatory authorities have ensured that airports can implement these standards according to their circumstances, priorities, and resources.

As a result of airports using EDS CB certified equipment under ECAC regulations, a certain percentage of all items belonging to passengers are no longer required to be screened randomly. If it is a certified C1 security system, passengers must remove electronics and liquids from their cabin baggage.

If it is a C2-certified system under the authority of the national regulatory authority, passengers may leave electronic items in their bags to remove liquids from their bags. In case when the scanner complies with the C3 standard, nothing needs to be removed from



	2001	2002	2003	2004	2006	2007	2009	2010	2011	2012	2014	2015	2016	2017
Public spaces	0	1	1	0	2	2	0	1	1	2	3	0	9	4
Security Restricted Areas	1	0	0	1	1	1	1	1	0	1	0	2	1	0

Fig. 1. Visualization of a comparative analysis of aviation incidents between 2001 and 2017 divided into public and restricted areas of an airport (Own elaboration)

the bag. It can change the divestment process, making it less complex and quicker, thus improving passenger comfort.

CT technology is the only technology likely to meet the EDS CB C3 (and C4 in the future) standards. By taking the detection of explosives in cabin baggage to a whole new level, CT technology will improve the safety and security of air traffic, the operational efficiency of airports and air networks, and significantly improve passenger experience (ACI, 2018).

Security has always been a high priority for airports around the world. However, major developments in the operational and technology environment of airports have transformed their threat landscape. The conventional approach to airport security cannot counter the present threats, both physical and cyber. They are also not able to meet the increasing volume of air passengers and their need for seamless and secure travel.

In the light of the new risks, the International Airport Committee has developed a statement that summarizes the scope for action by individual Member States to address the new risks. In this document, the International Council of Airports (ACI) pointed out that the entry to the terminal and the public domain is no different from other public spaces and is subject to security measures implemented by local authorities. At the same time, the Council pointed out that intelligence sharing is the most practical and realistic means of combating terrorism, rather than additional security checks.

Some authors have proposed the model of a multi-criteria evaluation of the security controls. It is necessary to adopt input variables to apply it. Security controls are evaluated by considering their capacity, efficiency, and level of service, so the following input variables for the system evaluation were adopted: capacity of a security control checkpoint, detection efficiency of prohibited items, passenger's experience. The approach proposed allows for selecting an optimal structure of a security control lane and an optimal structure of the security control process (Kierzkowski, 2017).

The International Air Transport Association (IATA) and the International Airports Council (ACI) have launched the New Experience in Travel and Technologies (NEXTT) initiative to support the use of modern aviation technologies.

The NEXTT initiative is to be a platform where airlines and airports will jointly develop standards for the use of new solutions. Three main pillars of NEXTT:

1. Baggage handling and passport control.
2. Advanced data processing (e.g., passenger and baggage tracking and identification technologies, automation of processes).
3. Interactive decision making (e.g., through better use of data or implementation of artificial intelligence).

British authorities are already testing Heathrow airport 3D scanners for hand luggage control. It will apply to all major UK ports. As highlighted, the use of the new equipment will shorten the time of security checks and save passengers the need to show security services liquids or electronics.

In Poland, the so-called biometric border control gates, called ABC (Automated Border Control) gates, have appeared at two airports serving Warsaw. Ten gates were installed at the main Chopin Airport for passengers arriving from outside the Schengen area and 10 for departing passengers. In Modlin, five gates will be used only by persons flying to Poland.

In some countries, like the USA, Canada uses full-body scanners. The National Transportation Safety Board (NTSB) has approved this possibility, and on the screen for the security guard, all intimate parts are displayed as covered (invisible).

The passenger has the right to receive a full explanation of the technology used to carry out the check. This right is granted by EU legislation which stipulates that passengers have the right to be fully informed about the technology used to scan them.

The airport security control processes in the future will include the latest technologies (IT systems) to improve security, enhance passenger screening and the overall travel experience. The mentioned IT systems would be vendor-neutral, utilize standardized communication protocols and interoperable technologies. Interoperability is called the capacity of IT systems and the underlying business processes to exchange data and share information and knowledge. IT application means an operational instrument for the application through a well-defined organizational and operational framework to contribute toward (passenger) safety, efficiency, comfort, and facilitating or supporting transport and travel operations (Nowacki, 2012).

Airports security controls processes will need to rethink their security procedures with the following in mind: implementation of technology as an enabler to enhance the passenger experience, differentiation focus and resources according to passenger risk profiles, reviewing processes to maximize screening efficiency, collaboration across a large set of stakeholders, integration of data to follow passengers' routes through all steps of their journey.

Security has always been related to people, processes, and technology, and it appears more than ever that advanced technology needs to be applied uniformly across the entire global aviation sector and other vulnerable sectors to detect evolving threats. While current technology is good at detecting explosives, the major concern is that terrorist capabilities challenge our technological capability to detect the latest threats (Nowacki, 2018). In light of the current pandemic scenario, airlines and airports are calling for swift international agreement on health measures to restore passenger confidence. Within the airport and airlines ecosystems, sets of various measures have already been deeply elaborated.

1.4. Security Control in Threats of COVID-19

The COVID-19 outbreak has massively impacted the aviation industry. For airport operators, the main aims are to protect the health and welfare of travelers, staff, and the public and reduce the opportunities for further spreading the virus. National regulators and health authorities have reacted to the spread of the virus by introducing measures directly affecting aviation and, more broadly, across society. Many airports operate at vastly reduced capacity, and almost all have introduced operational measures to deal with the crisis.

The latter naturally create an additional scope of tasks to be performed by various services, not limited to security personnel. For example, measures related to temperature screening and alternative security control measures of passengers and airport personnel, including the whole scope of basic safety precautions related to the obligatory use of personal protection equipment by security personnel, might significantly influence the implementation of new types of security controls.

Concluding, if security teams involved and responsible for the implementation of alternative security control processes will be asked to fulfill additional safety functions beyond their core purpose, it might also create some gaps, especially for those who wish to target aviation for criminal or terroristic purposes.

Airports need to be secured to minimize the risk of spreading the virus and maintain trust and confidence in air transportation again. In order to support a safe and smooth recovery from COVID-19 lockdown, the study, due to be released later in August 2021, was commissioned by EUROCONTROL and carried out by the Airport Research Center (ARC) with input from 6 partners, including ACI Europe, IATA, Charles-de-Gaulle, London Heathrow, Stuttgart and Swedavia Airports (EUROCONTROL, 2020).

The risk for air traffic leading to recurring local outbreaks is inherent as soon as airlines carry infected passengers, which are hard to identify when they are asymptomatic. It adds uncertainties for all aviation stakeholders regarding travel restrictions or quarantine measures taken by local governments. Therefore, the focus is on implementing risk-based measures that amongst physical distancing and enhanced sanitation may include health checks for arriving and/or departing passengers.

Thermal temperature screening was implemented at several airports in the initial phase of the pandemic but has been identified by EASA as a high-cost but low-efficiency measure because passengers without symptoms (up to 75%) are not detected.

PCR testing before departure could be done off-airport before traveling or at the airport, with results provided 2 to 3h after the test. Some countries have implemented requirements for recent negative PCR tests (e.g., 48-72 hours before departure).

PCR testing on arrival has been implemented, in particular from defined "risk areas". National authorities put rules into place but currently have difficulties with local testing capacities to ensure timely results.

Health self-declaration is requested by some governments as a further measure. Airlines had to ask health questions related to COVID. That was initially performed during check-in by agents, but most airlines have now integrated this into the online check-in. Some governments request this information online before travel.

Passenger locator cards / online health forms have been established by some national authorities (e.g., Spain or Greece) to ask self-declaration health questions and enable contact tracing more efficiently, request passengers to fill in online forms. With an online system, a QR code can be generated that passengers show during the check-in and eventually on arrival to prove that they provided the required.

2. Results of Own Empirical Research

2.1. Research Group

The research was conducted in the form of anonymous interviews and questionnaires in English, German, Spanish, and Polish within the major national and international stakeholders such as ICAO, IATA, European Commission, as well as amongst selected Civil Aviation Authorities and Airport Security Authorities in Poland, France, Germany, Sweden, Norway, Belgium, the Netherlands, Portugal, Spain, Austria, Croatia, the United Kingdom, the United States, and Canada. The research also included representatives of services companies responsible for the security and operational supervision at airports (police, border guards, customs, private security companies). The research was conducted using expert selection due to the knowledge and experience of respondents (118 persons) in the field of civil aviation security control.

2.2. Results of Survey

Question results: *how do you assess the following elements of the screening process for passengers at airports in terms of their relevance (significance)?* – as set out in Tables 2 to 5.

The courtesy and helpfulness of the security staff were assessed as good by the respondents (Tab. 2).

Tab. 2. Courtesy and helpfulness of security staff [own elaboration]

Possibility to respond	Quantity	%
1 (minor)	3	2,5
2 (significant)	11	9,3
3 (sufficient)	38	32,2
4 (good)	43	36,4
5 (very good)	23	19,5

It is very important as it indicates that issues relating to the quality of the passenger service itself in the screening process are not insignificant. Positive passenger experience stands key element during the security control process, simultaneously significantly influencing its overall perception.

The screening accuracy was assessed as the most important element for the overwhelming majority of respondents (Tab. 3). It indicates a high degree of relevance of this parameter for the screening process.

Tab. 3. Accuracy of screening [own elaboration]

Possibility to respond	Quantity	%
1 (minor)	2	1,7
2 (significant)	6	5,1
3 (sufficient)	9	7,6
4 (good)	15	12,7
5 (very good)	86	72,9

The waiting time parameter for screening was also crucial throughout the whole passenger screening process (Tab. 4).

Tab. 4. Waiting time for screening [own elaboration]

Possibility to respond	Quantity	%
1 (minor)	2	1,7
2 (significant)	19	16,1
3 (sufficient)	39	33,1
4 (good)	44	37,3
5 (very good)	14	11,9

A subjective parameter of a general sense of security, assessed at the individual level, was assessed as the most important in the study. This indicator shows that responders positively perceive the security component also recognize its purpose (Tab. 5).

Tab. 5. General feeling of security [own elaboration]

Possibility to respond	Quantity	%
1 (minor)	1	0,8
2 (significant)	5	4,2
3 (sufficient)	11	9,3
4 (good)	41	34,7
5 (very good)	55	46,6
No response	5	4,2

The results of the question: *how you generally assess the adaptation of existing security procedures at airports to the evolving risks associated with terrorist threats* is presented in Tab. 6.

The overwhelming majority of respondents assessed the level of adaptation of existing security procedures at airports to the evolving risks of terrorist threats at a rather good and very good level. On the other hand, the analysis also identified a group that assessed it

at an average level, indicating significant discrepancies among the surveyed expert groups. Considering the results of the analysis of the answers identified in the open questions, the majority of respondents indicated a risk (threat) that changes dynamically.

Tab. 6. Adapting procedures to changing risks [own elaboration]

	Possibility to respond	Quantity	%
1	It is very good	17	14,4
2	It is rather good.	62	52,5
3	It is average, just like that	32	27,1
4	It is rather bad	6	5,1
5	It is very bad	–	–
6	No response	1	0,8

Additionally, the answers were justified by statements about new types of threats and that terrorists usually are one step ahead.

Particular attention should be paid to statements stating that reactions to events should be quicker and that the regulations are reactive to the existing threats.

The results of the question: *In your opinion, is the technical equipment of security checkpoints at international airports adequate to today's threats* presented in Tab. 7.

Concerning the technical equipment of screening facilities, most respondents stated that they are equipped in a manner appropriate to the risks involved. When analyzing the responses, five categories of responses were identified, of which as many as three were indicative of shortcomings in the technical equipment. The lack of new equipment and the degree of modernity of the new equipment were largely highlighted. In addition, the comments highlighting the financial aspects of purchasing modern technology that some airports would not be able to cope with were not insignificant.

Tab. 7. Technical equipment for screening points [own elaboration]

	Possibility to respond	Quantity	%
1	It is fully adequate to the risks involved.	11	9,3
2	It is rather adequate to the risks involved	88	74,6
3	It is rather inadequate for the risks involved.	19	16,1
4	It is completely inadequate for the risks involved.	–	–

The results of the question: *how you generally assess the level of knowledge, skills, and competence of international airport security staff in conducting screening activities* are presented in Tab. 8-10.

The level of knowledge of security staff was set at a good and very good level (Tab. 8). A very small percentage described it as insufficient. It can be concluded that the knowledge of security staff is perceived positively.

Tab. 8. Knowledge [own elaboration]

	Possibility to respond	Quantity	%
1	Very good	22	18,6
2	Good	80	67,8
3	Sufficient	14	11,9
4	Insufficient	2	1,7

The skill level of security staff was also mostly set at a good and very good level. It also indicates that general perception of this factor being positively perceived by most of the responders (Tab. 9).

However, the importance of more assessments indicating only a sufficient level of skills compared to knowledge outcomes has emerged. It could indicate some shortcomings in the practical application of the control procedures, despite the knowledge available.

Tab. 9. Skills [own elaboration]

	Possibility to respond	Quantity	%
1	Very good	15	12,7
2	Good.	77	65,3
3	Sufficient	24	20,3
4	Insufficient	2	1,7

The overall assessment of the competence of security staff was made by a group of respondents at a good and very good level (Tab. 10). However, there was no shortage of assessments that defined the competences at a sufficient level.

Tab. 10. Competence [own elaboration]

	Possibility to respond	Quantity	%
1	Very good	14	11,9
2	Good	70	59,3
3	Sufficient	30	25,4
4	Insufficient	4	3,4

The use of modern technologies to detect potential threats is certainly a very important element of an airport security system – Tab. 11.

Analyzing respondents' opinions, the following types of activities were identified, which, according to experts, would help increase security at international airports. In the first place,

the respondents indicated a general tightening of the screening procedures for all persons having access to public areas of an airport, without any specific indication of methods or controls.

Tab. 11. Use of the latest technology [own elaboration]

Possibility to respond 1 is the lowest grade, and 5 for the highest grade	Quantity	%
1	7	5,9
2	7	5,9
3	28	23,7
4	52	44,1
5	20	16,9
No answer	4	3,4

Based on data from the conclusions of the International Civil Aviation Security Forum, a working panel on "Aeronautical Transport Vision 2040 and beyond" organized by the International Air Transport Association (IATA) in June 2019 provided a broad range of aviation experts with a vision of the future of the development of air transport as well as contemporary threats.

In one of the key questions posed by the forum on how the 2040 threat vision is perceived, the participants almost unanimously or in a similar tone identified the following areas of challenge in order of importance and alarm. As a result, they were singled out:

1) threats related to the cybersecurity of aviation ecosystems, including airlines and airports,
2) the increased need for background checks on internal threats,
3) attacks on areas with open access to airport infrastructure,
4) threats of chemical or biological attack both on board an airplane and within the airport infrastructure,
5) the evolution of methods of concealing explosives.

Summary

It is increasingly important for all stakeholders within the aviation ecosystem to look to new technologies, which can help preserve margins and ultimately deliver a better customer experience. Airports are currently increasingly full of modern technologies. Check-in machines, computer tomography in security control, robots that help carry luggage, or self-service automatic baggage check-in, where it is enough to put a suitcase on a belt, and the check-in takes up to 20 seconds. The new solutions are designed to eliminate the need for queues. At some airports, one can make an appointment to check-in for a specific hour; others introduce automatic biometric boarding.

Passenger transport by air has been growing steadily for many years. The increase in the number of passengers, on the one hand, makes it necessary to speed up security control procedures and, on the other hand, to improve the quality of such control. The airport environment will change significantly in the coming years.

Combined with the growing expectations of passengers and the need to improve security performance in the face of a changing global threat, this new ecosystem will change many procedures. Security will become a streamlined process based on cooperation and data exchange. Airports wishing to offer such experience to passengers will need to rethink their security procedures, taking into account issues such as:

- the implementation of technologies to improve the traveler experience,
- the introduction of targeted screening actions depending on the risk profile of the passenger,
- reviewing security processes and procedures to enable screening,
- data integration allowing identification of passengers at all stages of their journey,
- the need for a faster assessment and response of the whole aviation sector to threats, vulnerabilities, and consequences (better risk assessment and management), building cross-border and inter-organizational trust.

The presented conclusions confirm that the research problem of the article has been solved and the research hypothesis has been positively verified.

In the era of the global COVID-19 crisis, which is severely affecting the aviation sector, both operationally and financially, it is required to further assess new regulatory and operational changes. There should be appropriate measures in place (in consultation with health authorities) to ensure screening is carried as required and the implementation of ICAO baseline standards is ensured. Security checkpoint operations and design should be reviewed and, where necessary, rearranged to reduce queues and crowds to the extent possible. In addition, security personnel responsible for implementing security control shall be trained adequately to perform their tasks in a new operational environment considering alternative security control measures and strict safety precautions.

References:

Aktürk, S. (2019). Five Faces of Russia's Soft Power. *PONARS Eurasia Policy Memo, 623*.

ACI report 6.4% growth in global passenger traffic. (2019, September 17). *Airport Technology*. https://www.airport-technology.com/news/global-passenger-traffic-aci-report

Airport Council International World Report. Fraport's digital strategy – Focusing on projects that make a difference. *Airport Council International*. https://issuu.com/aciworld/docs/aci_october_world_report

Alards-Tomalin, D., Ansons, T.L., Reich, T., Sakamoto, Y., Davie, R., Leboe-McGowan, J.P., & Leboe-McGowan, L.C. (2014). Airport security measures and their influence on enplanement intentions: Responses from leisure travelers attending a Canadian University. *Journal of Air Transport Management, 37*, 60-68.

CAA Spain. (2008, August 20). Report A-032/2008, Accident Involving a Mcdonnell Douglas Dc-9-82 (Md-82) Aircraft Operated by Spanair, At Madrid-Barajas Airport.

Center for Strategic and International Studies. (2017). *Global costs of cybercrime*.

Commission Implementing Regulation (EU) 2015/1998 of 5 November 2015, laying down detailed measures for the implementation of the common basic standards on aviation security. OJ L 299, 14.11.2015, 1–142.

Cyber Security Strategy for the European Union (2013). *European Defence Agency*. www.eda.europa.eu

De Barros, A.G., & Tomber, D. Quantitative analysis of passenger and baggage security screening at airports. *Journal of Advanced Transportation, 41*(2), 171–193.

EUROCONTROL. Impact of COVID-19 Measures on Airport Capacity. https://www.eurocontrol.int/event/covid-19-impact-airport-operations-and-capacity

Future of Air Transport Security. (2014, October 21-23). *ICAO HQ*. http://www.icao.int/Meetings/SIAS/Pages/default.aspx

Global Strategy for the European Union's Foreign and Security Policy. http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf

ICAO. *Effects of Novel Coronavirus (COVID-19) on Civil Aviation: Economic Impact Analysis*. https://www.icao.int/sustainability/Documents/COVID-19/ICAO_Coronavirus_Econ_Impact.pdf

ICAO. (2020). *Passenger totals drop 60 percent as COVID-19 assault on international mobility continues*. https://www.icao.int/Newsroom/Pages/2020-passenger-totals-drop-60-percent-as-COVID19-assault-on-international-mobility-continues.aspx

IATA Report. (2019). *Air Transport Security 2040 and Beyond*.

Intelligent Portable Control System, iBorderCtR. https://www.iborderctrl.eu/The-project

Kierzkowski, A., & Kisiel, T. (2017). Evaluation of a Security Control Lane with the Application of Fuzzy Logic. *Elsevier Limited, Procedia Engineering,* 187, 656–663

Kirby, M. FAA imposes special conditions on 747-8 to prevent hacking. *FAA*. https://www.flightglobal.com/news/articles/faa-imposes-special-conditions-on-747-8-to-prevent-h-337368

More Connectivity and Improved Efficiency - 2018 Airline Industry Statistics Released. *IATA*. https://www.iata.org/pressroom/pr/Pages/2019-07-31-01.aspx#__prclt=zTkSP6TZ

Nowacki, G. (2018). Development and Standardization of Intelligent Transport Systems. *The International Journal on Marine Navigation and Safety of Sea Transportation, 6*(3), 403–411. DOI: 10.1201/B11347-9

Nowacki, G., & Paszukow, B. (2018). Security Requirements for New Threats at International Airports. *The International Journal on Marine Navigation and Safety of Sea Transportation, 12*(1). DOI: 10.12716/1001.12.01.22

Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No. 2320/2002. OJ L 97, 9.4.2008, 72–84.

Shapiro, D. (2016). *How did security measures fail in Brussels*. John Jay College of Criminal Justice.

Terrorism and War-Related Airplane Crashes Fast Facts. (2020, January 20). *CNN Editorial Research*. https://edition.cnn.com/world/terrorism-and-war-related-airplane-crashes-fast-facts/index.html

UK Lifts ban carrying phones laptops tablets aircraft cabin. (2018, August 31). *Airport Technology*.

ULC. (2021, June, 2). Przewozy pasażerskie w transporcie lotniczym w 2020 roku. https://www.ulc.gov.pl/pl/aktualnosci/5632-przewozy-pasazerskie-w-transporcie-lotniczym-w-2020-roku

Wolniak, R. (2019). Aviation terrorism and its impact on the aviation industry. *Scientific Papers of the Silesian University of Technology,* 134.