Malwina Dankiewicz

Methods of detecting potential terrorists at airports

Security Dimensions and Socio-Legal Studies nr 7, 33-46

2012

Malwina Dankiewicz,MA
Institute of Psychology, Department of Behavioural Sciences
of the Jagiellonian University

METHODS OF DETECTING POTENTIAL TERRORISTS AT AIRPORTS

Abstract:
In recent years the interest to improve the reliability of deception and hostile intentions detection techniques is related to the need of increasing the safety of citizens threatened with terrorist attacks. In particular, the United States government through its security agencies is looking for and financing research on modern lie detection techniques[1].
There are different opinions on whether we can determine who is planning a hostile act, merely by observing behavior. Some researchers are convinced that scientific methods of detecting hostile intentions, among others by detecting deception, can help to catch terrorists and provide security. This article focuses on behavioral methods of detecting potential terrorists.

Keywords: *Terrorist, safety, detection, crime, attack.*

Rising crime and a high risk of terrorist attacks cause that predicting aggressive behavior nowadays is the ability that can not be underestimated, and identifying individuals who very likely could have hostile intentions, has become a necessity. In order to protect the security of citizens, including the requirement of eliminating direct attacks on life, health or property of individuals, the methods based on scientific research are applied[2.]

Systems used at airports are the examples of utilizing research findings to

[1] W. Froncisz, *Jak wykryć kłamstwo czy prawdomówność podglądając mózg*, „Wszechświat", 2007, no.1, p. 18-23.

[2] J. Czapska, *Bezpieczeństwo obywateli. Studium z zakresu polityki prawa*, Polpress, Kraków 2004, p. 32.

ppredict aggressive behavior: methods of detecting potential terrorists, based on the analysis of behavior, emotions visible on faces, and physiological indicators.

In recent years the interest to improve the reliability of deception and hostile intentions detection techniques is related to the need of increasing the safety of citizens threatened with terrorist attacks. In particular, the United States government through its security agencies is looking for and financing research on modern lie detection techniques[3].

There are different opinions on whether we can determine who is planning a hostile act, merely by observing behavior. Some researchers are convinced that scientific methods of detecting hostile intentions, among others by detecting deception, can help to catch terrorists and provide security. This article focuses on behavioral methods of detecting potential terrorists.

FACS system

In 1978, Ekman and colleagues developed the Facial Action Coding System (FACS), which supported by measurements of voice and speech allows to increase the accuracy of lie detection (lying defined as “a deliberate choice to mislead a target without giving any notification of the intent to do so”[4]), to 90%.

FACS is a method of describing and measuring facial behavior, based on observable components of facial movement called action units (AU) and the combinations of action units are forming a facial expression. FACS describes the contraction of various muscles, leading to different facial expressions by which we are able to recognize emotions. Involuntary facial expressions (microexpressions) are brief (they last less than one second) and are characteristic for experiencing one of the seven basic, universal emotions: anger,

[3] W. Froncisz, *Jak wykryć kłamstwo czy prawdomówność podglądając mózg*, „Wszechświat”, 2007, no. 1, p. 18-23.

[4] P. Ekman, *Self-Deception and Detection of Misinformation*, [in:] *Self-Deception: An Adaptive Mechanism?*, (ed.) J.S. Lockhard, D.L. Paulhus, Prentice-Hall, Englewood Cliffs, NJ 1988, p. 230.

fear, pdisgust, contempt, sadness, surprise or happiness. Microexpressions are evolutionarily acquired reactions occurring in the entire human species, regardless of socialization, culture and age. In the course of socialization, people learn to control their facial expressions, and therefore it is possible to pretend experiencing specific emotions. However, even with an ability to control any facial expressions, the current emotional state is revealed by other nonverbal messages, more difficult to control consciously[5]. A number of studies indicate that also important is the appearance of eyes (especially the pupillary reflex), whole body posture, way of speaking (tone of voice and speaking rate), spatial behavior and keeping personal distance[6]. In addition, the first reaction of the face, which later can be masked, for example by putting on a fake smile, is usually real. Intentional (fake) expressions differ from the spontaneous ones: fake expressions are usually held for too long, moreover it is not possible to control all the muscles associated with specific facial expressions[7].

Ekman holds to a view, that nonverbal indicators are the most accurate and promising indicators of lies, in terms of possible practical applications. He concludes, basing on the results of his own research, that people overly rely on verbal communication and are inclined to ignore or misinterpret the most explicit mimic, movement and voice indicators. The researcher also proves that training in recognizing nonverbal indicators of deception, described by him, improves the accuracy in identifying lies. Another argument in favor of this position by Ekman are the contradictions in reports of research on verbal indicators of lie – for example, it appears that the answers given only by some people are indirect, evasive, and contain more information than the question required. Microexpressions are used to detect lies, and it makes possible to detect hostile intentions of the other person. To facilitate this process, Ekman suggests using a tool such as FACS, to enable assessment of facial expression, but mastering it requires a lot of time. Fa-

[5] P. Ekman, *Telling Lies. Clues to deceit in the marketplace, politics and marriage*, W. W. Norton & Company, New York-London 1992.

[6] I. Kurcz, *Język i komunikacja*, [in:] *Psychologia. Podręcznik akademicki*, *t. 2*, (ed.) J. Strelau, GWP, Gdańsk 2004, p. 231-274.

[7] P. Ekman, *Telling*..., *op. cit.*

cial Action Coding System, which has so far been used mainly in laboratory tests, proved to be a reliable and effective method of detecting lies, because the ability to detect microexpressions is positively correlated with the ability to detect lies[8].

Recognizing signs of emotion on the face can be trained through a designed by Ekman computer program called F.A.C.E. Training. The program is composed of two types of training: METT (Micro Expression Training Tool) and SETT (The Subtle Expression Training Tool). F.A.C.E. Training has been scientifically proven and field tested and is now the basis of a new television show on Fox TV: Lie To Me, of which Dr. Paul Ekman is the scientific consultant.[9]

Ekman is currently working on the project of new methods for rapid and mass identification of people whose facial expressions and physiological correlates of emotions may show deception or hostile intentions. He continues to work on the identification of facial expressions of immediate deadly intent, covering both premeditated and loss of control attacks. The study will include persons who have recently survived a physical assault, to restore the expression they saw on the face of the perpetrator. The project is called D-cube (Dangerous Demeanor Detector) and is designed to develop the skills in detecting the subtle signs of aggression[10].

Ekman's recent scientific research is also focused on imaging facial physiology as a method of detecting changes in the level of stress. He and his colleagues conducted a study to prove the accuracy of estimates of the computer system, which uses a thermal camera monitoring the real-time changes in blood flow in the orbital muscles, pointed out correctly in 83% of participants experiencing tension (lying) or not experiencing tension (truth-telling). Researchers believe that this is a result which opens way for the automated detection of deceit in natural conditions, which is the need increasingly being declared from the security systems industry. The threat of terrorist attacks

[8] W. Wypler, *Aktualne trendy w psychologicznych badaniach nad kłamstwem*, [in:] *Profilaktyka społeczna i resocjalizacja*, (ed.) J. Kwaśniewski, Wydawnictwo IPSiR UW, Warszawa 2009, p. 161-181.

[9] *F.A.C.E. Training* [in:] http://www.paulekman.com (04.04.2012).

[10] *Current Projects* [in:] http://www.paulekman.com (04.04.2012).

forces the use of new solutions: technologically advanced systems for quick, efficient and massive monitoring of human behavior and physiology, in order to detect changes in the level of arousal, as well as evaluating in real-time the risk of dangerous behavior, such as terrorist acts[11].

Facial Action Coding System (FACS) underlies the technology used by officers working at American airports under the program implemented by Ekman to detect suspicious passengers. The program is called SPOT (Screening Passengers by Observation Techniques) and is based on training in observation skills to help them identify passengers at an early stage.

SPOT program

At 161 airports in the United States there are working about 3,000 of Behaviour Detection Officers (BDOs). They are employees of Transportation Security Administration (TSA), which is branch of Department of Homeland Security (DHS): government agency watching over the safety of the traveling citizens in the United States. BDOs are part of a four-year-old program called Screening Passengers by Observation Technique (SPOT), which is designed to identify people who could pose a threat to airline passengers. The program utilizes noninvasive behavior observation and behavioral analysis techniques to identify potentially high-risk passengers. BDO officers are intended to detect persons exhibiting behavior that indicates that they may constitute a threat to aviation and air transport security.

The program is a derivative of other successful behavioral analysis programs which have been implemented by law enforcement and security personnel, both in the U.S. and around the world. TSA's BDO-trained security officers are screening travelers for involuntary physical and physiological reactions which people exhibit in response to fear of being discovered. Manifestation of some of these behaviors does not automatically mean that an in-

[11] P. Tsiamyrtzis, J. Dowdall, D. Shastri, I.T. Pavlidis, M.G. Frank, P. Ekman, *Imaging Facial Physiology for the Detection of Deceit*, „International Journal of Computer Vision", 2007, no. 71 (2), p. 197-214.

dividual has terrorist or criminal intent, but this knowledge helps to determine whether a person presents a higher risk or whether the observed behavior has a nonthreatening origin[12].

BDO officers are trained to detect suspicious or unusual behavior in passengers: they determine whether the passengers are a threat, basing on their responses to a set of routine questions. Security officers ask three to four questions (e.g., „Where have you been?”, „Where are you traveling?”, „What is the purpose of your trip?”, „Do you have a business card?”), while looking for minute facial cues that may indicate deception or malicious intent. The primary responsibility of the BDO officers is to observe the behavior of passengers going through the security checkpoint.[13] Individuals exhibiting specific observable behaviors may be referred for additional screening at the checkpoint, including personal and one's carry-on baggage physical inspection. Referrals are based on specific observed behaviors only, not on one's appearance, race, ethnicity or religion.

BDO officers add an element of unpredictability to the security screening process which is easy for passengers to navigate but difficult to manipulate by terrorists. It serves as an important additional level of security in the airport environment, requires no additional specialized screening equipment, can be easily deployed to other modes of transportation and presents yet another challenge the terrorists need to overcome in attempt to defeat the security system.

To 2011 Ekman has taught about 1,000 BDO experts and continues to consult on the program. The methodology used in SPOT has never been subjected to controlled scientific tests, because neither Ekman nor TSA have disclosed the specific cues used to identify potential threats, citing security reasons. Ekman has largely stopped publishing, not to provide any help to terrorists trying to cheat the system.

[12] *Behavior Detection Officers (BDO). Layers of Security* [in:] http://www.tsa.gov (date of reading 04.04.2012).

[13] C. J. Ciaramella, *I spy with my little eye: TSA rolling out new 'behavior detection officers'* [in:] http://dailycaller.com (04.04.2012).

Evidence of the SPOT program effectiveness provides statistics: in the first phase of the program, from January 2006 to November 2009, according to the TSA agency, behaviour-detection officers referred more than 232,000 people for re-inspection, which involves closer control of bags and testing for explosives. The vast majority of those subjected to another inspection continued on their travels with no further delays, but 1,710 were arrested[14].

Similar safety programs are implemented in many other airports around the world. At Heathrow Airport in London, the British government is implementing behavior detection officers in a program modeled in part on the SPOT, while Department of Homeland Security in the United States leads the FAST program, which uses sensors to look at nonverbal behavior, and thereby detects the potential terrorists, walking down the hall. United States Department of Defense (DOD) and intelligence agencies have expressed interest in similar programs[15].

FAST technique

TSA SPOT program was in its first year, when the Science and Technology Directorate of the U.S. Department of Homeland Security began searching for new methods and started to sponsor research aimed at developing and testing tools and methodologies for identifying and assessing potential threat (deception and hostile intent) in real time, on the spot and noninvasively, and at better understanding of the phenomenon of terrorism, improving national security, and accelerating movement of people through checkpoints. This technology would be similar to or exceeding the capabilities of present screening techniques without impeding the flow of travelers.

Achieved in effect is the FAST technique (Future Attribute Screening Technology), developed under the DHS program called Social and Behavioral Research (SBR), in addition to previously used methods of screen-

[14] S. Weinberger, *Airport security: Intent to deceive?*, „Nature", 2010, no. 465, p 412-415.

[15] S. Weinberger, *Airport..., op. cit.,* p. 412-415.

ing, such as SPOT. It consists in the fact that passengers passing through a security gate are monitored in terms of nonverbal signals of intent to harm others. This technology is designed to catch suspicious behavior, and thereby potential terrorists, with cameras and sensors measuring subtle physiologic changes that can be assessed remotely and in real time, including eye movement, width of the pupil, heart rate, skin electrical resistance, respiration rate, sweating, and possibly brain scans, while a passenger is asked a series of specific questions. FAST also draws attention to visual signals, such as blinking rate and body movements (restless behavior). The procedures and technologies necessary to receive these signals, are noninvasive and easy to integrate into crowded operating area, such as airports. In addition to detecting signals of hostile intentions, under the program was conducted research on the possibility of automating this process using sensors and detection algorithms, and integrating the system with other technologies aimed at identifying individuals who pose a threat to United States aviation, such as biometric tools and databases.[16]

The device, just as technology Pre-Crime in the movie „Minority Report", is designed to read the intentions of potential terrorists, for example at airports. It reminds polygraph, but there is no need of direct contact with a potential perpetrator – FAST's sensors do not come in direct contact with monitored individual, and their action does not depend on direct questioning. Contact sensors were replaced with stand-off systems (optical sensors and radars), such as infrared cameras to measure subtle changes in facial temperature and BioLIDAR, a laser radar that measures heart rate and respiration. That allows the assessment of travelers walking down the hall, standing in line, or passing through the control gate.

According to DHS, the device worked properly in 70 percent, 30 percent were false alarms. This result is much higher than random, and also higher than those achieved by specially trained persons. Daniel and Jennifer Martin's malintent theory underlying the FAST technique is based on the assumption derived from the behavioral sciences, that the hostile intentions translate

[16] *Deception Detection* [in:] http://www.dhs.gov (04.04.2012).

into specific physiological responses and behavior. Scientists have proven the relationship between psychophysiological indicators and intentions. The study consisted of 40 Arabic-speaking men, and led to the conclusion, that there is a relationship between the intent to deceive and heart rate variability, known as respiratory sinus arrhythmia (RSA)[17].

The FAST project consists of two elements: first, necessary are the models of hostile intent and deception, focusing on behavioral and verbal cues, and second, an automated suite of non-invasive sensors and algorithms. Integrated, these sensors automatically detect and track the input cues to the models. According to the developers of this technology it has the potential to revolutionize the screening and interviewing process, by supporting access control for strategic infrastructure, such as airports[18].

While existing screening technologies, such as biometrics, offer the potential to detect already known terrorists, the FAST technology focuses only on real-time, psychophysiological and behavioral patterns in an attempt to stop an unknown terrorist from obtaining access to his desired location. Simply put, comparing the behavior of individuals with established patterns of behavior, in relation to the situational context and appropriateness of behavior, allows the prediction of human actions. That was achieved through mobile and multimodal technologies, using behavioral and physiological sensors which provide culturally neutral indicators of hostile intent. By creating the FAST technology, DHS hopes to simplify the control of the airport by using recent advances in the development of screening techniques focused on behavior[19.]

[17] S. Weinberger, *Airport…, op. cit.,* p. 412-415.

[18] *Deception..., op. cit*.

[19] Privacy Impact Assessment Update for the Future Attribute Screening Technology (FAST)/ Passive Methods for Precision Behavioral Screening, DHS/S&T/PIA-012(a), 21 December 2011.

SAFEE system

The SAFEE system (Security of Aircraft in the Future European Environment) is a large integrated project, developed by scientists from research centers in the UK and Germany, which aims to restore full confidence in air transport. The vision of this project is to build an advanced system of aviation safety, working under the threat of terrorist attack on the aircraft. The main objective of this system is to provide a completely safe flight from departure to arrival destination, whatever the identified threats are. The basis of the project is past experience, which has shown that people with hostile intentions may go through the different airport controls and security measures, access an aircraft and initiate a hostile action. Therefore there is a need to secure the plane, as the last barrier of attack[20]

The project is focused on the implementation of a wide range of onboard systems detecting threats and providing reliable information about the threat to the flight crew. The monitoring system of air passengers called Onboard Threat Detection System, designed to prevent the abduction of the aircraft, tracks passengers with miniature cameras installed in every seat in the plane, and analyzes their behavior. This technology has to distinguish the ordinary passengers from those, who may threaten others and themselves. Applied eye blinking frequency monitors were borrowed from the work on lie detectors: increased frequency suggests higher level of stress. Cameras have to continually monitor and record every movement of the passenger, to analyze the expression of the face, the frequency of blinking, eye movements, wetting the lips with tongue, and even the state of hair, meaning all indicators suggesting increased level of stress, which in turn is indicative of passenger's intent to deceive. In addition to the cameras in the seats, installed microphones might be installed, which may pick up even softly spoken words. Analysis of each passenger behavior will be available to the crew and will be a warning signal of the possibility of a terrorist attack, such that took place on 11 September.

[20] *Security of Aircraft in the Future European Environment* [in:] http://www.safee.reading.ac.uk (04.04.2012).

All audio and video materials about the behavior of passengers are to be reset after each flight to protect passenger rights[21].

An important aspect of behavior analysis is the issue of avoiding discriminatory ethnic profiling, such as recognizing any person of Arab origin as a potential terrorist. Presented below are case studies of training offered to officers in order to develop their abilities to perceive and analyze suspicious behavior, diverting attention from the characteristics that may refer to prejudice, such as race, ethnicity or religion.

In the Netherlands there is a training program called Search, Detect and React (SDR), created by International Security and Counter-Terrorism Academy for Police and Security Entities. The SDR is used as a tool to identify cases of potential violence, disrupting public order, illegal activity and fatal attacks. It is intended to protect public space and mass events and to increase security skills for the analysis of behavior: directs attention to behavior that might require police action, and diverts attention from the immutable characteristics, such as skin color. During the training, officers learn how people usually behave in specific places and situations and how to detect in a best way suspicious behavior which differs from the norm. When they detect such behavior, the officers must act in a certain way, for example, refer to the suspect in a careful, informal way without use of formal police powers. The program includes theoretical, practical and job training. SDR is now applied at Schiphol airport and in various units of the Dutch police.

In the United Kingdom, police training is conducted under the Behavior Assessment Screening System (BASS). The system was created by Massachusetts State Police in the United States and adapted for use by the British Transport Police. The training is based on profiling of the behavior of people who are under stress at airports and transport hubs. Massachusetts State Police along with criminologists has reviewed the recordings of the hijackers in the September 11 attacks, departing from Boston's Logan International Airport and arriving at the airport before the attacks. They created a set of criteria with which it is possible to identify the behavior of people under stress

[21] *Security…, op. cit.*

in the crowd, when checking in at the airport or during security check. These criteria have been adapted to British conditions using information gathered from the 7 July bomb attacks on the London Underground. The mandatory training of BASS passed all the officers of British Transport Police, working in the London Underground, and it is now also applied to officers working on the railroad across the country. The two-day course includes lectures, discussions and practical exercises, both in class, as well as in the transport hubs. The training emphasizes that there is no racial or religious profile of terrorist, because the attacks are carried out by the people of all ethnic groups[22].

In Poland the year 2011 brought changes to the Polish Aviation Law. New legislation is being adapted to the requirements of the European Union and introduces a coherent system of civil aviation security. According to new recommendations, security control at airports is to be conducted by private security companies, working as Airport Security Service (SOL) and no longer has to be done by Polish Border Guard, as it was before. SOL will take such tasks as controlling people and luggage. The duties will include providing security at the airport, among others by observing passengers and searching in a crowd for those people, who behave in a suspicious manner, namely through the use of behavioral analysis techniques that have worked so far in many countries[23].

In this way, science can help to predict, prevent, prepare for and raise after a terrorist attack[24], and also to understand the causes of terrorism and how to resist it[25]. The introduced amendments are aimed at improving aviation safety and streamlining the process of airport management.

[22] *Podniesienie skuteczności działań policji. Rozumienie dyskryminującego profilowania etnicznego i zapobieganie mu: przewodnik*, Raport Agencji Praw Podstawowych Unii Europejskiej, Urząd Publikacji Unii Europejskiej, Luksemburg 2010.

[23] *Przyszłość bezpieczeństwa lotnisk w Polsce. Jak będzie wyglądała praca Agencji Ochrony?*, „Safety and Security”, 2011, no. 1, p. 48-52.

[24] *Combating Terrorism: Research Priorities in the Social, Behavioral and Economic Sciences*, Raport NSTC, Washington 2005.

[25] P.E. Rubin, *Behavioral Science and Security*, presentation before the Subcommittee on Investigations and Oversight Committee on Science, Space, and Technology, U.S. House of Representatives 2011.

Bibliography

Behavior Detection Officers (BDO). Layers of Security, [in:] http://www.tsa.gov (04.04.2012).

Ciaramella, C. J., *I spy with my little eye: TSA rolling out new 'behavior detection officers'* [in:] http://dailycaller.com (04.04.2012).

Combating Terrorism: Research Priorities in the Social, Behavioral and Economic Sciences, Raport NSTC, Washington 2005.

Current Projects [in:] http://www.paulekman.com (04.04.2012).

Czapska, J., *Bezpieczeństwo obywateli. Studium z zakresu polityki prawa*, Polpress, Kraków 2004.

Deception Detection [in:] http://www.dhs.gov (04.04.2012).

Ekman, P., *Self-Deception and Detection of Misinformation* [in:] *Self-Deception: An Adaptive Mechanism?*, (ed.) J.S. Lockhard, D.L. Paulhus, Prentice-Hall, Englewood Cliffs, NJ 1988, p. 229- 257.

Ekman, P., *Telling Lies. Clues to deceit in the marketplace, politics and marriage*, W. W. Norton & Company, New York-London 1992.

F.A.C.E. Training [in:] http://www.paulekman.com (04.04.2012).

Froncisz, W., *Jak wykryć kłamstwo czy prawdomówność podglądając mózg*, „Wszechświat", 2007, no. 1, p. 18-23.

Kurcz, I., *Język i komunikacja*, [in:] *Psychologia. Podręcznik akademicki*, t. 2, (ed.) J. Strelau, GWP, Gdańsk 2004, p. 231-274.

Podniesienie skuteczności działań policji. Rozumienie dyskryminującego profilowania etnicznego i zapobieganie mu: przewodnik. Raport Agencji Praw Podstawowych Unii Europejskiej, Urząd Publikacji Unii Europejskiej, Luksemburg 2010.

Privacy Impact Assessment Update for the Future Attribute Screening Technology (FAST)/Passive Methods for Precision Behavioral Screening, DHS/S&T/PIA-012(a), 21 December 2011.

Przyszłość bezpieczeństwa lotnisk w Polsce. Jak będzie wyglądała praca Agencji Ochrony? „Safety and Security", 2011, no. 1, p. 48-52.

Rubin, P.E., *Behavioral Science and Security*, presentation before the Subcommittee on Investigations and Oversight Committee on Science, Space, and Technology, U.S. House of Representatives 2011.

Security of Aircraft in the Future European Environment [in:] http://www.safee.reading.ac.uk (04.04.2012).

Tsiamyrtzis, P., Dowdall, J., Shastri, D., Pavlidis, I.T., Frank, M.G., Ekman, P., *Imaging Facial Physiology for the Detection of Deceit*, „International Journal of Computer Vision", 2007, no. 71 (2), p. 197-214.

Weinberger, S., *Airport security: Intent to deceive?,* „Nature", 2010, no. 465, p. 412-415.

Wypler, W., *Aktualne trendy w psychologicznych badaniach nad kłamstwem* [in:] *Profilaktyka społeczna i resocjalizacja*, (ed.) J. Kwaśniewski*,* Wydawnictwo IPSiR UW, Warszawa 2009, p. 161-181.