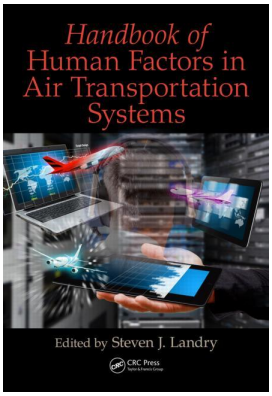

Handbook of Human Factors in Air Transportation Systems

Steven J. Landry

Security

Publication details
https://test.routledgehandbooks.com/doi/10.1201/9781315116549-10
Douglas Harris
Published online on: 15 Nov 2017

10 Security

Douglas Harris

CONTENTS

INTRODUCTION

The current chapter addresses the ever more critical human factors in aviation security, a subject in which human factors have played and will continue play a significant role. A historical background of human factors issues is presented, emphasizing research approaches and findings, and their resulting operational applications. In addition, the findings of periodic critical assessments of aviation security are summarized and their implications for human factors discussed. The chapter also looks ahead to the continuing problems that remain to be solved, predicting the changing mix of threats that will need to be addressed and anticipating the types of new procedures and technologies that will need to be assessed.

As we address the methods and concerns of aviation security, it may be helpful to keep in mind the magnitude and scope of the enterprise. To this end, some helpful statistics have been compiled by the Department of Homeland Security (DHS), the Transportation Security Administration (TSA), the General Accountability Office (GAO), and other organizations. For example, more than 650 million passengers and 700 million items of baggage undergo security screening each year at 450 airports in the United States. The TSA employs the full-time equivalent of 55,600 personnel to conduct passenger and baggage screening at these airports. Moreover, the total cost of these aviation security efforts is an estimated $8 billion per year.

Aviation security was addressed by Gibb and Lofaro in their chapter of the Handbook of *Aviation Human Factors*, second edition, which was published in 2009. It is the intent of this chapter to focus on findings and developments that have taken place since the publication of this earlier handbook, with the exception of the background information that follows. We start, then, with a brief history of aviation security, an accounting and description of threats to aviation security, the roles that have been assigned to human operators, and a description and assessment of factors that influence operator performance.

BACKGROUND

A Brief History of Aviation Security

Threat-detection systems were first implemented at airports in the early 1970s in response to increased hijackings of commercial aircraft. Since the introduction of these systems, human operators have played a key role in the detection of threats, such as guns, explosives, and possible terrorists, by examining X-ray images, resolving metal detector alarms, conducting body scans with metal detection wands, observing passenger's behavior, conducting physical searches of baggage, and maintaining order at screening checkpoints.

Ensuring the safety of air travel was soon recognized as a monumental task, and the effectiveness of the systems implemented to detect and deter threats was soon called into question and has been of concern ever since. In 1994, for example, at the request of the Federal Aviation Administration (FAA), the National Research Council formed a panel that assessed and reported on airline passenger security screening (NRC, 1996). The panel determined that the analytical and decision-making performance of security personnel was critical to the successful implementation of any security system, and that the allocation of functions between machine and operator is likely to have significant influence on the effectiveness of future systems. The panel stated that an ideal passenger screening system "would be capable of detecting both metallic and nonmetallic threat items in less than six seconds, with a high degree of accuracy (including a high detection rate and a low false-alarm rate). In addition, an ideal system would give the operator enough information, in an appropriate format, to allow for the speedy and accurate resolution of alarms."

The panel also determined that the screening systems could be made more effective by integrating the human operator completely into the system. The inability to maintain the needed level of operator performance was considered a major weakness of existing screening systems and a potential weakness of future systems. Moreover, improving operator performance should be considered as critical as technical improvements for enhancing current systems and ensuring the success of new systems.

Concerns for security were then greatly intensified after the terrorist attacks of September 11, 2001 in which four commercial aircraft were hijacked and used as weapons to destroy the World Trade Center twin towers and inflict severe damage to the Pentagon; moreover, these concerns have not diminished as evidence of worldwide terrorism continues to accumulate. In his review and assessment of aviation security at that time, Harris (2002) proposed a much broader and more flexible perspective for addressing the problem than was then in place. He proposed that instead of applying the same procedure to every passenger and item of baggage, the system should be adaptable so as to meet the full range of anticipated security threats with timely and appropriate responses based on the nature and extent of the potential threat. "Such a system would consist of the following integrated and coordinated components:

- Security teams of selected, cross-trained, motivated personnel performing tasks appropriate to the threats, with continuing measurement and feedback of their performance;
- An arsenal of technologies and procedures that can be quickly reconfigured and deployed to meet probable threats; and
- Timely intelligence continually disseminated to security teams on probable adversaries and threat scenarios."

Others also proposed alternative approaches to replace that of screening all passengers in the same manner. For example, Poole and Passantino (2003) suggested employing multiple levels of security involving the screening of passengers and baggage in accordance to assessments of their perceived risk.

As reported by the Congressional Research Service (Elias, 2014), the TSA, after having applied relatively inflexible methods to aviation security over the years, is now shifting away from this approach to what is being called a *risk-based* approach. Thus far, the development of this approach has focused on identification of high-risk passengers and expediting the processing of low-risk passengers. Issues yet to be tested are the efficacy of the specific program elements and the extent to which they complement each other and enhance the effectiveness of the overall security process.

Threats to Aviation Security

The Aviation and Transportation Security Act of 2001 established TSA as the federal agency with primary responsibility for securing the nation's civil aviation system including the screening of all passengers and properties transported by commercial passenger aircraft. TSA relies upon multiple

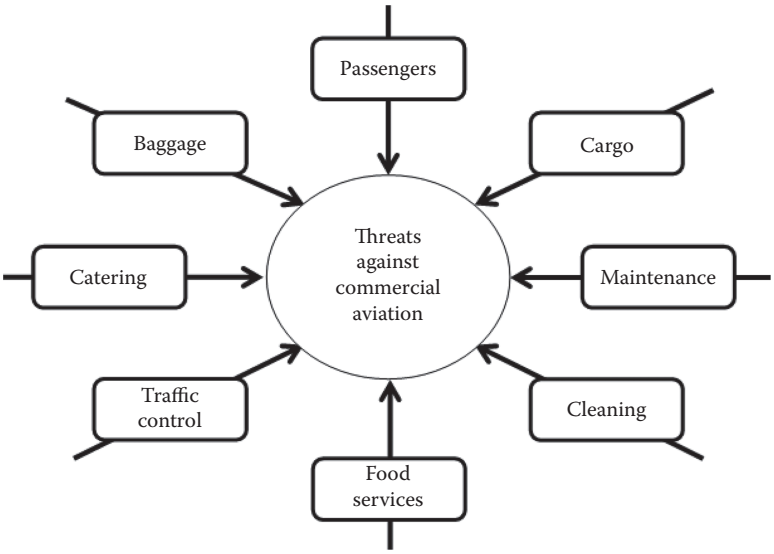

FIGURE 10.1 Potential avenues for threats against commercial aviation.

layers of security to deter, detect, and disrupt persons posing a potential risk to aviation security. The subsequent Act of 2007 further mandates the screening of 100% of cargo transported on passenger aircraft to determine whether cargo poses a threat to transportation security.

Although passengers, baggage, and cargo are the primary focus of security efforts, they are not the only sources of threats to aviation security (see Figure 10.1). Threats can also come from many processes that support airport operations: catering, maintenance, cleaning, baggage handling, air traffic control, retail, food services, and others. For example, members of the cleaning staff stashed guns and grenades in the plane's washroom to support the hijacking of TWA Flight 847, which led to 17 days of terror in 1985 (Gladwell, 2001). Thus, even perfect threat detection applied only to passengers, and their baggage would not necessarily result in acceptable levels of security.

According to Richard W. Bloom (2011), Chair of the Transportation Research Board Aviation Security and Emergency Management Committee, the most appropriate and comprehensive approach to assessing the sources of threat would be a comparative analysis of threats from people (passengers) versus things (cargo). His assessment is that the security threat from passengers or baggage or cargo changes from moment to moment depending on the continuous coupling of threat with vulnerability, qualified by the impact and probability of a successful terrorist attack. In addition, over time, the nature and extent of threats from passengers and cargo will change as the world changes.

The Roles of Human Operators

Aviation security, particularly checkpoint screening, places extensive reliance on human perception, decision-making, and judgment to detect and resolve potential threats. Assuring and enhancing the performance of human operators in their assigned roles will continue to be one of the major challenges in future efforts to incorporate improved security technologies and procedures (Elias, 2009).

For most of the history of aviation security operations, human operators have been called upon to perform tasks for which humans are poorly equipped—such as the monitoring and detection of rarely occurring, low-signal-to-noise-ratio signals embedded in the context of varying background configurations. This has been principally by default because technology has not been available to perform these tasks. An extensive body of research on human vigilance, for example, has led to the unavoidable conclusion that humans are poor monitors and that a variety of interventions

and countermeasures directed toward improving detection performance in different settings and tasks over many years have demonstrated little benefit (Davies & Parsuraman, 1982; Mackie, 1987). Consequently, a primary objective in the design of security systems should be to remove the operator from this monitoring role. Emphasis should be given to developing and implementing screening technology designed to monitor, detect, and alert operators to potential anomalies and to the development of procedures to enable operators to determine whether or not the anomaly is a threat. That is, the monitoring/detection/alarm function should be allocated to machines, and the alarm resolution function to human operators.

Human operators have special unique capabilities needed for alarm resolution, such as pattern recognition, abstract reasoning, spatial visualization, and cognitive flexibility. As a consequence, an appropriate (even necessary) role for human operators is in the resolution of detected signals. However, even in this role, the combined effects of the design of the specific operator tasks, the environment in which the tasks are performed, and the selection and training of operators are critical to the realization of effective performance. Using human operators appropriately in threat-detection systems requires systematic efforts to match their capabilities with the requirements of the system and to minimize the effects of human limitations (Parasuraman, Molloy, Mouloua, & Hilburn, 1996; Rasmussen, 1986; Reason, 1990; Wiener, 1988).

Paradoxically, as threat-detection systems become more automated, human integration issues are likely to become even more important to their successful implementation. Human operators will be performing the more difficult and complex tasks that defy automation, such as alarm resolution. Moreover, the increased automation will introduce new performance issues that will need to be addressed. For example, an operator directly involved in X-ray signal detection necessarily monitors the performance of the X-ray machine. Degradation of images, easily detected by the operator, leads to appropriate equipment calibration or maintenance. If detection is automatic, on the other hand, the operator will need to have some other means of monitoring and ensuring that the technology is operating properly. Such problems introduced by automation can be resolved if they are recognized and addressed during system design and development.

In 2007, the TSA implemented the screening of passengers by observation techniques (SPOT) program that utilized operators in a very different manner from that previously discussed. The program employed behavior detection officers (BDOs) to observe passenger behavior to detect potential high-risk travelers. The assumption of the SPOT program was that cues observed from passenger behaviors might be indicative of the stress, fear, or deception likely to accompany destructive actions. According to TSA, as of 2012, more than 3,000 BDOs were authorized for deployment to 176 U.S. airports (DHS, 2012a).

BDOs, working in pairs, primarily conduct behavioral observations at airport screening checkpoints and by having brief verbal exchanges with passengers while they are waiting in line. A BDO identifies passengers for additional screening based on an evaluation system of previously identified behaviors; the BDO may involve a law enforcement officer to determine if legal intervention is needed. If determined to be a possible threat, the passenger may not be permitted to board the aircraft. According to TSA, SPOT referrals made during the year from October 2011 to September 2012 resulted in 199 arrests for having outstanding warrants, suspected transport of drugs, and being illegal aliens. The passenger throughput during that year was 657,000,000.

Factors Influencing Operator Performance

Operator performance is a continuing concern as covert testing results have repeatedly demonstrated existing weaknesses in screening procedures and capabilities, weaknesses that could be exploited by terrorists or criminals seeking to attack the aviation system. These weaknesses can stem from policies, procedures, technology, and/or operator performance. But according to the Congressional Research Service (Elias, 2009), weaknesses in operator performance are

the principal concern. A wide range of human factors considerations pertaining to operator performance were identified in this assessment as having potentially significant effects on operator performance, including procedures, training, fatigue, perception, detection, judgment, and decision-making.

The humans who operate the system have long been regarded as a potentially highly fallible and vulnerable element of the aviation security system. This should not be construed as a reflection on the dedication, commitment, or motivation of individual operators in performing their critical job functions. Rather, it reflects the combination of complex challenges faced by operators, such as limitations in the required capabilities, resourceful adversaries employing artful concealment methods, and time pressures to perform well while maintaining an efficient flow of passengers through security checkpoints.

In such a system, measurement and feedback of operator performance would seem essential to the development and maintenance of proficiency. Consider, for example, how little people would improve their bowling performance, and how soon they would stop bowling altogether if there was no system of keeping score and no feedback on how many and which pins were knocked down with each roll of the ball. The huge sports industry—players, teams, leagues, fans, tournaments, records, statistics, and magazines—is based on measuring performance and providing feedback (scores, standings, winners, and champions). The power of this process to enhance performance in military and industrial jobs has been known for decades; when it is absent, performance deteriorates (Harris & Chaney, 1969; Howell & Cooke, 1989; Ilgen & Klein, 1988; Swezey & Salas, 1992).

Airport security operators cannot be expected to maintain high levels of performance day after day, month after month without consistent, regular, realistic, accurate measurement, and feedback of their performance. In addition to providing a continuing basis for motivating and improving operators, performance measurement and feedback can also serve to enhance proficiency of the overall threat-detection system by the following:

- Diagnosing performance weaknesses and tailoring performance-based training to overcome the weaknesses identified
- Assessing the impact of new detection technologies and procedures and
- Providing criteria for validating the design and organization of the security processes

According to the TSA (2014b), threat image projection technology is now being employed on a daily basis to measure and provide feedback on operator proficiency in the X-ray detection of weapons and explosives. Potential threats, including guns and explosives, are projected onto X-ray images of carry-on bags passing through screening, thus permitting the testing of detection capabilities. These data permit the evaluation and feedback of individual detection performance and, also, help one formulate operator training programs. As the X-ray equipment is part of a network, every airport and X-ray monitor is able to receive automatic image updates from the TSA technology lab based on the latest intelligence on potential threats.

The ultimate success of on-line performance measurement for improving operator performance will have as much to do with the manner in which systems are introduced and employed as with the effectiveness of the systems themselves. Critical considerations include the detailed procedures needed for collecting and analyzing data, the extent to which the measurement system intrudes into operator screening tasks and the degree of understanding by operators of how the measures are to be obtained and used. Rarely, for example, should the results obtained from any on-line performance measurement be employed as the basis for punitive actions, such as fines, penalties, reprimands, or other punishments. Punitive actions based on performance measures will inevitably lead to subversion of the measurement process, contamination of the results obtained, and resistance to remedial measures that might be introduced to enhance performance.

ASSESSMENTS OF AVIATION SECURITY

Over the past 10 years, systematic, independent assessments of aviation security have been made by oversight organizations such as the Heritage Foundation, the GAO, the RAND Corporation, the Reason Foundation, and the 2015 Aviation Security International Summit. The results of these assessments serve to provide a varied perspective of the issues confronting aviation security and to identify a host of human factors problems and issues that need to be addressed.

Heritage Foundation Assessment

The Heritage Foundation is an American conservative think tank based in Washington, D.C. The foundation's stated mission is to "formulate and promote conservative public policies based on the principles of free enterprise, limited government, individual freedom, traditional American values, and a strong national defense."

In its assessment of aviation security, the Heritage Foundation (2006) stated that "although well-intentioned, much of the effort to enhance aviation security since September 11, 2001, has done little to make the skies significantly safer." The assessment is critical of the Congress having vested both regulatory and operational responsibilities in the same agency, the TSA. According to the assessment, TSA's dual role of being both regulator and operator of baggage and passenger screening creates a serious conflict of interest.

The assessment points out that beginning in the 1980s, European airports began to develop a performance-contracting model under which the government set and enforced high performance standards, which airports then carried out by hiring security companies or occasionally using their own staff. Now, most countries in the world use this model, leaving the United States pretty much alone in having the national government actually operate its aviation security system. As a result, the Heritage Foundation report states that the prospects for any significant improvement in passenger and baggage security are grim.

RAND Corporation Assessment

The 2012 assessment by the RAND Corporation (Jenkins, 2012) starts with a historical perspective, taking the reader down the 40-year path of terrorist threats and aviation security responses and concluding that, over the long run, increasing security has made terrorist operations more difficult and pointing out that the effectiveness of security should be measured not in the number of weapons or explosive devices discovered at airport checkpoints but in the steadily declining number of attempted terrorist hijackings and sabotage attempts. The reason for this positive trend is in both the decline in the number of terrorist groups focusing on aviation and in the improvement in security. In addition, although some critics think airline security is a joke, terrorists take it very seriously because risks of betrayal and failure are just too great.

The RAND assessment observes that airport security personnel is under increasing stress because each terrorist innovation has added another security procedure and each added procedure complicates the search, slows down the screening process, and further stretches human resources. At the same time, passenger loads are increasing, whereas security budgets appear likely to decline. If the same number of operators is expected to perform more procedures on more passengers without letting the lines back up at checkpoints, performance can be expected to suffer. Meanwhile, public tolerance and cooperation are likely to fray.

Americans have come to hold unreasonable expectations that government should provide 100% security, and they quail when there is any failure. At the same time, they have little tolerance for inconvenience and react with outrage to intrusions into their privacy, and the safer people feel, the less tolerance they have for what they see as increasingly intrusive security.

Thus, the review concludes that aviation security is costly, controversial, and contentious; moreover, no other security measures directly affect such a large portion of the country's population. On account of the nature of the threat, aviation security is the most intrusive form of security and, as a consequence, is often at conflict with issues of civil liberties. But, the threat is real and not likely to go away soon; terrorists remain obsessed with attacking airplanes.

The RAND assessment proposed a sweeping review of aviation security and recommended that nongovernment research institutions undertake the task, and that each reviewer independently design an optimal aviation security system beginning with a clean slate. The competing models would be reviewed, and the best ideas, or combination of ideas, would be put forward. RAND justifies this effort by stating that even if the results resemble what is already in place, the process would offer some comfort that we are close to the best that we can do.

GAO Assessments of 2012, 2013, and 2014

The GAO is an independent, nonpartisan agency that supports the U.S. Congress in meeting its constitutional responsibilities by helping to improve the performance and ensure the accountability of the federal government. The stated objective of GAO evaluations is to provide Congress with timely information that is objective, fact based, nonpartisan, nonideological, fair, and balanced.

In 2012, the GAO assessed TSA's SPOT program and TSA's efforts to enhance cargo security on inbound aircraft. In its report (GAO, 2012), the GAO acknowledged that the TSA had not only taken actions to validate the science underlying its behavior-based passenger screening (SPOT program) but also stated that more work remains. GAO had reported earlier, in 2010, that TSA had deployed SPOT before first determining whether there was any scientifically valid basis for using behavior and appearance indicators to reliably identify passengers who might pose a risk. The GAO also had reported then that it was unlikely that the SPOT program had ever resulted in the arrest of anyone who is a terrorist, or who was planning to engage in terrorist related activity, even though there was evidence that terrorists had transited through SPOT airports.

The GAO also reported that the TSA has taken actions to enhance the security of cargo on inbound aircraft, but that challenges remain. In its June 2010 assessment, GAO had recommended that TSA develop a mechanism to verify the accuracy of all screening data. TSA concurred in part and required air carriers to report inbound cargo screening data but has not yet fully addressed the recommendation. In June 2012, TSA required air carriers to screen 100% of inbound air cargo transported on passenger aircraft by December 3, 2012. However, air carriers and TSA have faced challenges in implementing this requirement and in providing reasonable assurance that screening is being conducted at reported levels.

The 2013 assessment (GAO, 2013) concluded that the SPOT program does not meet its objectives and recommended that future funding for behavioral detection activities be limited. According to this assessment, available evidence does not support the use of behavioral indicators, such as those employed in the TSA's SPOT program to identify persons who may pose a risk to aviation security. GAO reviewed four meta-analyses of over 400 studies from the past 60 years and found that the human ability to accurately identify deceptive behavior based on behavioral indicators is the same as or only slightly better than chance. The GAO warned that until TSA can provide scientifically validated evidence demonstrating that behavioral indicators can be used to identify passengers who may pose a threat to aviation security, the agency risks funding an aviation security approach that has not been determined to be effective.

The efforts of TSA to introduce expedited passenger screening were addressed by the GAO in its 2014 assessment (GAO, 2014). This program, sometimes referred to by the TSA as *Managed Inclusion*, was implemented in 2011 and involves selecting passengers for expedited screening based on layers of risk assessments of all passengers. Testing of the system is scheduled to be completed by mid-2016. The number of passengers receiving expedited screening grew slowly at first but has increased more rapidly since late 2013 when the TSA expanded its employment of

automated risk assessments of all passengers, in which a risk score was assigned to each passenger based upon available information.

TSA determines a passenger's risk score, and thus eligibility for expedited screening at the airport, using one of three risk assessment criteria: inclusion on a TSA precheck list of preapproved low-risk travelers, identification of passengers as low risk by TSA's risk assessment algorithm, or a real-time threat assessment at the airport using the managed inclusion process. To be on the TSA precheck list of approved travelers requires the completion and approval of an application and payment of a processing fee.

The GAO had previously examined several of the layers of passenger risk assessment employed in the managed inclusion process, raising concerns regarding its effectiveness, and recommending actions to TSA to strengthen them. In late 2014, TSA planned to begin testing managed inclusion as an overall system but could not provide specifics or a plan or documentation showing how the testing was to be conducted, the locations where it is to occur, how these locations are to be selected, or the timeframes for conducting testing at each location. GAO emphasized the need to employ established methodological practices for evaluation such as adequate sample size and random selection of participants to ensure the generalizability of results.

Reason Foundation Assessment

In their 2013 report, "Overhauling U.S. Airport Security Screening," the Reason Foundation addressed what they see as a conflict of interest of the TSA (Poole & Ybarra, 2013). That is, as specified by the Aviation and Transportation Security Act of 2001, the TSA establishes security policy and regulates those that provide airport security while, at the same time, is itself the operator of the largest component of airport security: passenger and baggage screening. The recommendation is for the airport and not TSA to select the security contractor and to manage the contract under TSA regulatory oversight. This position is essentially the same as that taken by the Heritage Foundation in 2006 that was discussed earlier in this section of the chapter.

In their assessment, the Reason Foundation pointed out that separation of aviation security regulation from the provision of security services is called for by the International Civil Aviation Organization (ICAO), to which the United States (along with 189 other countries) is a signatory. Under the Chicago Convention that created ICAO, "contracting states are required to notify ICAO of any differences between their national regulations and practices" and ICAO's international standards. The United States has failed to notify ICAO that it does not comply.

The Foundation report further specified that under a performance contracting approach, with screening devolved to the airport, TSA would continue to certify screening companies that met its requirements (e.g., security experience, financial strength, screener qualifications, training, etc.). It would also spell out the screening performance measures (outcomes) that companies or airports would be required to meet. Airports would be free to either provide screening themselves or to competitively contract for a TSA-certified screening company. Companies bidding in response to the airport's RFP would propose their approach to meet the performance requirements, in terms of staff, procedures, and technology. This could include, for example, cross-training screeners to carry out other airport security duties, such as access and perimeter control. The airport would select the proposal that offered the best value, subject to TSA approval. TSA, in its role as regulator, would oversee all aspects of the airport's security operations, including adherence to federal laws and screening.

The Aviation Security International Assessment

In their report, "Security Screening: Improving Human Performance for Greater Reliability," Aviation Security International (2015) stated that they were encouraged by the innovative designs and security solutions tested recently at larger airports. Specifically mentioned were the improved

capabilities of detection equipment resulting from the introduction of new technologies. On the other hand, the assessment concluded that innovation in detection capabilities must extend beyond the introduction of new technologies alone. It must encompass improvements in capability, which can result from the effective alignment of people, procedures, and equipment, and where the role of technology is one of assisting human operators to better perform their detection tasks.

The Aviation Security International assessment references the results of research on airport security estimating that about 80% of all error events can be attributed to deficient human performance and, of these, the majority stem from organizational weaknesses. Their assessment states that the findings from analyses such as these can provide the basis for enhanced operator performance by sharing the results with operators. Feedback of this type, providing an opportunity to learn from performance results, has long been known and practiced by top-performing organizations.

RESEARCH ON OPERATOR CAPABILITIES AND PERFORMANCE

Factors Affecting Visual Search and Detection

Research has been conducted for decades to assess visual skills in search and detection for a variety of applications and, more recently, as they relate to performance in airport-security screening. In this section, we identify, describe, and assess those factors that have been identified as affecting the visual search and detection tasks employed to meet aviation security objectives.

Two-Component Model of Visual Search and Detection

Elements of the aviation security inspection task can be seen as being similar to inspection tasks found generally in other applications. They rely on the component of repetitive visual search of multiple target items on multiple images, and on the component of detection—the classification of a target either as acceptable or requiring further investigation. However, aviation security inspection has the added challenge of requiring operators to recognize each of the changing catalogue of potential threats whose general nature is known (i.e., guns, knives, etc.), but whose actual size, shape, and other characteristics are likely to change over time. In addition, threats are likely to be deliberately concealed, to rarely occur, and to lead to severe consequences if undetected (Schwaninger & Hofer, 2004).

In a study employing 416 experienced X-ray screeners, Ghylin, Drury, and Schwaninger (2006) tested the applicability of this two-component model as the basis for computer-based training of operators in aviation security X-ray screening. Application of the two-component inspection model was shown to result in large increases in detection performance and substantial reductions in response times. It also allowed the individual parts of the inspection process to be further analyzed and modeled to provide a better idea of what steps within the inspection processes have been changed by the training and why. The authors conclude that by having knowledge of the individual components within inspection, the technologies, methods, and procedures that current security inspectors utilize can be better honed to enhance the strengths of the human–system interface and correct their weaknesses.

Object Recognition

The detection of prohibited objects in passenger's bags using X-ray screening equipment requires the matching of X-ray images with object representations stored in visual memory. Visual knowledge of which objects are forbidden and what they look like is therefore critical to their successful detection. In studying the visual abilities and visual knowledge required of screeners to perform this task, Schwaninger, Hardmeier, and Hofer (2005) developed and applied tests of these capabilities.

The prohibited items test was developed to measure the extent to which a screener has acquired the necessary visual knowledge. The test contains a sample of different forbidden items from the

international prohibited items lists placed in X-ray images of passenger bags to clearly reveal object shapes. As each image in the test can be inspected for 10 seconds, failing to recognize a threat item can be mainly attributed to a lack of visual knowledge.

The object recognition test was developed to measure visual processing and encoding. Three image-based factors can be distinguished that challenge different visual processing abilities. First, depending on the rotation within a bag, an object can be more or less difficult to recognize (effect of viewpoint). Second, other objects can be superimposed over prohibited items, which can impair detection performance (effect of superposition). Third, the number and type of other objects in a bag can challenge visual search and processing capacity (effect of bag complexity).

To examine the role of object recognition in the detection of threat objects in X-ray images of passenger baggage, a total of 134 aviation security screeners and 134 novices participated in a study. The criticality of the three image-based factors measured by the object recognition test was validated. The effect of view, superposition, and bag complexity was all highly significant. Regarding the effect of visual knowledge, as measured by the prohibited items test, detection performance of screeners was significantly superior to that of novices, consistent with the assumption that visual knowledge is also important to screener performance. Reliability was found to be high for both participant groups and tests, indicating that they can be used for measuring performance on an individual basis. The results confirm that X-ray detection performance relies on visual abilities necessary for coping with image-based effects such as view perspective, bag complexity, and superposition. Visual experience and training are necessary to know which items are prohibited, and what they look like in X-ray images of passenger bags.

Target Prevalence

Target prevalence is calculated as the ratio of the number of target events (target present) to the number of nontarget events (target absent) over a period of time. For example, if the number of opportunities for a target to be present were 100 and only one target appeared during this time, the target prevalence would be 1%.

Visual search for infrequently appearing targets (low-target prevalence) is characterized by a marked elevation of miss errors accompanied by a corresponding decrease in reaction times (Wolfe, Horowitz, & Kenner, 2005). A likely explanation might be that observers simply become faster and more careless when targets seldom appear. However, follow-up research by Wolfe and his associates (Wolfe et al., 2007) demonstrated that this target prevalence effect is more complex than just a simple speed-accuracy tradeoff. When two observers view the same sequence of stimuli, if prevalence errors were simply careless lapses, they should occur randomly and not be correlated between observers. However, their research showed that errors were strongly correlated. Rather than the product of carelessness, then, errors appear to be caused by shifts in decision criteria that lead operators to miss most of the same targets; when targets rarely appear, operators shift their criteria to a strongly conservative position resulting in the nondetection of infrequently appearing targets.

This pattern of results has been well known for years in other settings (Green & Swets, 1967; Mackworth, 1970; Maddox, 2002). Mackworth stated that one of the most important findings in vigilance research was the discovery that the probability that a signal will be detected is considerably reduced when the rate of target events is very small relative to the rate of nontarget events (often referred to as the background rate). The effect of reducing target prevalence is to make the decision criterion more conservative. The operator performing X-ray screening of passenger baggage will be less likely to call something a target if the *a priori* probability of the target is low.

Target prevalence, then, powerfully influences the results of visual search behavior. In most visual search experiments, in which targets are rare (such as in medical or airport screening), observers shift response criteria, leading to elevated target miss rates. Operators also speed target-absent responses and may make more motor errors. This could result from a simple speed/accuracy tradeoff with fast, frequent absent responses producing more miss errors. However, research completed by Wolfe and Van Wert (2010) showed that although very high target prevalence (98%)

shifted response criteria in the opposite direction, leading to elevated false alarms in a simulated baggage search, the very frequent target-present responses were not speeded and the rare target-absent responses were greatly slowed. This effect was further studied by varying target prevalence systematically more than 1,000 trials; detection accuracy and reaction times were measured for each trial. Observers' criterion and target absent response times closely tracked prevalence. These results support a model in which prevalence influences two parameters: the decision criterion governing the detection decision for each attended item, and the quitting threshold that governs the timing of target-absent responses.

Correctable Target-Detection Decisions

Fleck and Mitroff (2007) also addressed the problem of low detection rates for infrequently appearing targets in baggage screening by examining the mechanisms that hinder visual search and detection for these targets. As shown in the previous research, when targets are rarely present, observers respond more quickly, resulting in higher miss rates. Their research showed that when searching arrays similar to those viewed by airport baggage screeners, observers missed only 7% of the targets when target frequency was high (target present on 50% of trials) but missed an alarming 30% when target frequency was low (target present on 1% of trials).

They hypothesized that when targets are rarely present, observers adapt by responding too quickly, resulting in reporting errors and high miss rates. They proposed that misses are often due to response-execution errors rather than perceptual or identification errors. That is, airport screeners might actually have sufficient information to determine that a target is present but just respond too quickly indicating it is not. The investigators further hypothesized that when provided with the opportunity to correct their response, the operator would often be able to catch and correct the mistake. If so, low-target prevalence may not be a generalizable cause of high miss rates in visual search.

They tested this hypothesis with 1,400 target-detection trials divided into three blocks determined by the frequency with which targets were present. The experimental design was similar to that of Wolfe, Horowitz, and Kenner (2005); the critical difference was that half of the participants were given the opportunity to correct each response. The high-target-prevalence block consisted of 200 trials, 50% of which contained a target; the medium-prevalence block consisted of 200 trials, 10% of which contained a target: and the low-prevalence block consisted of 1,000 trials, 2% of which contained a target. Presentation of the blocks was counterbalanced among the 20 participants in the research and no order effects were noted. Half of the operators, the correction condition, were given the opportunity to correct their response before going on to the next trial.

Results for the no-correction condition replicated the prevalence effects of the Wolfe, Horowiz, and Kenner study. Miss rates were 10%, 19%, and 31% for the high-, medium-, and low-target-prevalence blocks, respectively. In contrast, the correction condition showed no significant effect of prevalence, with miss rates of 4%, 10%, and 10% for the high-, medium-, and low-prevalence blocks.

In summary, target prevalence did not influence the error rate in the correctable searches in this study. The option to correct mistakes appeared to parse out response-execution errors, thus minimizing the rise in miss rates previously found in searches for rare targets. Ultimately, improving real-world search and detection performance might be served by separately addressing errors of action and errors of perception. However, these conclusions need to be verified by studies conducted in actual aviation security screening operations.

Sleep Deprivation

Fatigue may be caused by a variety of factors, including intrinsic and extrinsic sleep disorders, as well as work and lifestyle-related changes in sleep schedules. Impairments from sleep loss have been found, in general, to produce increased variability in alertness and compensatory effort, resulting in increased rates of errors of omission (i.e., lapses) and errors of commission (i.e., incorrect responses). To what extent do night work and sleep loss impair target detection performance in

aviation security tasks? Is the impact on visual detection sooner and more dramatically than other cognitive functions?

In a study to determine the effects on screener performance of fatigue induced by night work, sleep loss, repeated performance shifts, and time-on-task, screener performance was assessed by measuring the speed and accuracy of threat detection during a simulated luggage screening task (Basner et al., 2008). The study tested the implications of previous research that night work and sleep loss would increase both errors of omission (missed threats) and errors of commission (false alarms) in threat-detection performance.

The results confirmed that night work and sleep loss adversely affect performance of tasks performed by airport baggage screeners. Thus, fatigue induced by sleep deprivation in luggage screening personnel could potentially pose a threat for air traffic safety. In the future, methods could be developed to predict signal detection performance based on brief fitness-for-duty tests or objective monitoring of screener alertness during the screening task, and countermeasures developed and deployed in an effort to assure high levels of vigilance and detection performance.

Image-Based Factors

Among the factors that are likely to affect X-ray screener performance in the detection of threat objects in passenger baggage are view difficulty and threat item superposition. The nature and extent of image interpretation training received by screeners is also likely to interact with these image-based factors. The objective of an experimental study completed by Bolfing, Halbherr, and Schwaninger (2008) was to determine the relative importance of these image factors and the possible influences of screener training on them. The study employed 90 professional aviation security X-ray screening operators and 2,048 test images created automatically employing a set of image measurement algorithms.

Bivariate correlations between detection performance and image factors were analyzed to estimate the isolated impact of each single factor independently of any other. Multiple linear regression analyses were applied for estimating the overall impact of both image-based factors and computer-based training, respectively. Analyses of covariance were applied in to check for possible interaction effects between all variables. All analyses were applied separately for the four threat item categories: guns, knives, improvised explosive devices (IED), and others.

The findings from these analyses led to the conclusion that view difficulty can be addressed effectively with computer-based training of X-ray screening operators; training improved detection performance significantly, particularly for the more difficult views. The results for image superposition, however, were not so promising under the limitations of the screening technology employed in which only one image was presented per bag. The solution for superimposed images is likely to require more recent technology capable of providing multiple views for each bag.

This study showed, once again, that in addition to stable human abilities, there are also trainable skills that play a very important role in mediating detection performance. Knowledge-based factors such as knowing which objects are prohibited and what they look like in X-ray images can be effectively learned by screeners through computer-based training, a powerful tool to improve X-ray image interpretation competency of screeners.

Single versus Multiple Target Search

Research on industrial inspection tasks long ago determined that visual search for one type of possible defect (target) at a time, employing multiple searches, was more effective than searching for all possible defects (targets) at a time during a single search. When applied to aviation security searches of passenger bags, this finding would indicate that searching an X-ray image of a bag for one threat item (knife, gun, and bomb) at a time would result in a higher detection rate than searching for all three items at the same time. In industrial inspection, defect-by-defect searches of complex items of electronic equipment containing many types of potential defects were found to be about twice as effective as area-by-area searches of the items (Harris & Chaney, 1969).

Recent research has confirmed that the superiority of single-target searches also applies to X-ray screening of passenger baggage for purposes of aviation security. Menneer, Donnelly, Godwin, and Cave (2010) investigated the relationship between the search for one and the search for two targets and found that performance was lower in dual-target search compared with the combined performance for two independent single-target searches, and that the added response time required by the two searches disappeared with practice, but the reduced accuracy of single searches remained. Thus, the two searches, one for each type of target, produced better detection performance and, ultimately, did not require more search time.

Sensitivity was lower and the decision criterion more conservative in dual-target searches than in single-target searches, suggesting that the mental representation of the target was less effective in dual-target search than in single-target search. In addition, target-present responses were excessive under high target prevalence, and target-absent responses were excessive under low-target prevalence. These findings are important for aviation security screening tasks in which targets appear rarely and can differ from each other. For example, the low-target prevalence in X-ray security searches may magnify the dual-target deficiencies implicated in previous research with X-ray images. Such a result would increase the need for security personnel to consider alternatives to dual-target search, such as specialization in detecting one target type or training to encourage independent searches for each target.

Assignment of Security Tasks

Depending on the country in which the airport is located, there are typically several parties responsible for aviation security activities at an airport: the government department responsible for civil aviation, the police, the airport operator, and aircraft operators who have contracts with security companies. There are also several categories of security tasks at airports such as passenger security screening, checked baggage security control, access control to restricted areas, cargo and mail security, and crisis management. An important human factors consideration in aviation security, and the object of some study, is the rationale and manner in which responsibility for each security task is assigned.

The ICAO, a specialized agency of the United Nations, provides the standards for defining and allocating aviation security tasks for its 190 member states that include the United States. It specifies that each state shall require the appropriate authority to define and allocate tasks and coordinate activities between the departments, agencies, and other organizations of the state, the airport and aircraft operators, and of the entities assigned with the responsibility for implementation of the national aviation security program.

The structure and assignment of security tasks has been the subject of study by several researchers. Feng (2003) reviewed the aviation security structures in various countries such as the United States of America, Canada, the United Kingdom, Australia, New Zealand, Singapore, and Japan. He found that only the United States had created a new national organization, the TSA, charged with overseeing transportation security under the DHS. The other countries place their security organizations under their respective ministries of transport. Yoo and Lee (2004) studied the responsibility structure of security tasks at international airports in several countries and compared the advantages and disadvantages of each system. They pointed out that systems emphasizing a governmental role, such as those in the United States of America, have better security performance, whereas systems that place the responsibility for security tasks on the airport operator have an advantage in maintaining the efficiency of overall airport operations. Askew (2004) researched passenger screening and argued that significant improvements in security screening outcomes and check point performance result from the implementation of comprehensive recruitment and training with recurrent training to remedy deficiencies, along with continuing assessment and modification of processes and procedures.

Yoo (2009) surveyed a sample of experienced aviation security practitioners to assess the relative importance of five principal aviation security tasks. Passenger screening was considered to be the most important among the five security tasks and the most in need of enhancement. Checked baggage control was assessed as being the second most important followed, in order, by access control, cargo security, and crisis management. According to Yoo, these results probably reflected respondents' awareness that there have been numerous major security incidents at their facilities, such as hijackings and sabotages caused by the failures of passenger or baggage security control.

Human Factors in Layers of Defense in Airport Security

Airport security systems have been built up over the years out of layers of defense based on the security-in-depth model. As discussed in this section, the TSA has now defined a staggering 20 layers of defense to control security risks. This means that many others have security responsibilities beyond the more visible security personnel that we see at the airport when catching a flight. Human factors play a significant role in most of these layers of defense and in possible future improvements.

According to the TSA (2015), multiple layers of security are employed to ensure that the traveling public and the nation's transportation systems are adequately protected. Security is most often associated with the airport checkpoints operated by transportation security officers; however, checkpoints represent just one layer of security among the many in place to protect the various forms of transportation. There are different measures of security utilized within the aviation system including intelligence gathering and analysis, cross-checking passenger manifests against watch lists, random canine team screening at airports, and federal air marshals and federal flight deck officers that provide armed protection to the aircraft. According to the TSA, there are also additional security measures undisclosed to the public.

According to the TSA, each layer serves as a counterterrorism measure. In combination, these layers provide enhanced security creating a much stronger and protected transportation system to deter, detect, and prevent an attack from happening. Each of the 20 layers is described briefly in the following.

1. Intelligence: Intelligence officers work with government and international partners to identify threats and to determine current and future issues affecting aviation security.
2. Customs and Border Protection**:** As one of the largest and most complex security operations, its objective is to keep terrorists and their weapons out of the United States while also facilitating trading and passenger travel.
3. Joint Terrorism Task Force: The Joint Terrorism Task Force consists of personnel from local and national agencies brought together to protect regional airports by assuring that the security measures taken are up to national standards.
4. No Fly List and Passenger Prescreening: The no-fly list is developed by means of passenger prescreening and monitored to ban people considered potential threats from traveling in or out the United States on any commercial aircraft.
5. Crew Vetting: In the process of assuming flight duties, airline crew members submit identification details such as name, country of residence, date of birth, and, in the case of pilots and engineers, license numbers.
6. Visible Intermodal Prevention and Response Teams: Visible Intermodal Prevention and Response teams work with regional security and police departments to maximize the capabilities for the detection of terrorism plans.
7. Canine Teams: The TSA has an estimated 500 canine teams working with the local law enforcement agencies and operating in 70 airports and 14 mass transit systems to detect possible explosive substances at the airports perimeter and interior.

8. Behavior Detection Officers: Behavior detection officers operate at security checkpoints in an attempt to detect passengers who exhibit suspicious behavior.
9. Travel Document Checker: Passengers are required to hand or show their boarding pass and identification to a TSA document checker when entering the departure areas.
10. Checkpoint Transportation Security Officers: TSA agents are stationed at airport security checkpoints to assure that passengers are properly screened before entering the aircraft.
11. Checked Luggage Screening: All checked luggage that will go into the cargo compartment is required to undergo X-ray and explosive-trace screening.
12. Transportation security inspectors: Transportation security inspectors observe security operations to assess the TSA personnel, the jobs they are performing, and the effectiveness of TSA procedures.
13. Random Employee Screening: Any individual with access to the airport's secure areas is subject to random screening and thorough background checking.
14. Bomb Appraisal Officers: These officers provide guidance and education to other security personnel to enhance their capabilities at checkpoints. They typically have had operational experience in military or law enforcement bomb squads.
15. Federal Air Marshal Service: Air marshals typically work undercover and armed in passenger aircraft to address any problems that might occur in flight.
16. Federal Flight Deck officers: Selected pilots and other approved flight crews are, after being trained, permitted by the TSA to carry a firearm during flight operations.
17. Trained Flight Crew: All cabin crews are encouraged to complete self-defense training offered by the TSA to deal with assaults that might occur during flight.
18. Law Enforcement Officers: Armed law enforcement officers may be called upon to assist with security on an airplane or at an airport by arresting or suppressing individuals exhibiting problem behavior.
19. Hardened Cockpit Door: The three aircraft cockpit doors are hardened to prevent entry, thus providing an extra layer of threat prevention.
20. Passengers: Passengers are required to undergo a number of screening processes as they pass through the security checkpoint, possibly including X ray, metal detector, trace explosive detector, and a pat-down search under suspicious circumstances.

In their study of human factors in layers of defense in airport security (Andriessen, Gulijk, and Ale 2012), 177 security personnel and 180 passengers completed survey questionnaires. The objective of the study was to obtain the perspectives of both security personnel and passengers toward the various elements that constitute the layers of defense in aviation security. The results identified several themes that the authors considered important to understand the effectiveness of the layers of defense model.

Security staff feel their responsibility most strongly when their responsibilities are compared with those of other airport employees. The type and amount of training received appears to contribute to this effect.

Frequent flyers are the most informed about security procedures but also feel the least responsibility for the security of other passengers.

A passenger's level of education was found to influence his or her perception of security; passengers with higher levels of education were found to know more about the security elements and processes. Among airport security staff, on the other hand, systematic differences were not found. It was hypothesized that this was a result of the common elements in the training that security staff had received.

The technology employed in airport security was found to be little trusted by both passengers and staff. This is a remarkable finding considering that technology plays such a large role in many of the layers of defense employed by the TSA. It seems that security staff, although feeling responsible for doing their job right, cannot trust the tools they use to do this job.

Airport security staff considered their airport to be less safe than did the passengers. Whether this is caused by the specific knowledge of the process that they possess or because of their distrust of the technology employed was not clear from the results of this study.

Human Factors in Cargo Screening

Air cargo varies in content, how the content is packaged and situated, and the configuration and other characteristics of the aircraft. Content may be categorized by density, weight, size, economic value, signatures of explosives, weapons, and weapons components. The associated screening challenges include the following: possible electrostatic discharge, physical damage related to the method of screening, levels of specificity and sensitivity related to the cargo content, and terrorist knowledge of screening methods, which can lead to the development of countermeasures or to other means of exploitation. The determination as to whether or not a cargo container is acceptable is difficult because the inspected containers can be very large, whereas the prohibited items can be comparably small (e.g., an IED or contraband goods). Taking human factors into account is therefore of utmost importance for assuring effective cargo security screening.

According to the results of a review of human factors in cargo screening (Mendes, Michel, & Schwaninger, 2013), security measures have been strengthened substantially in recent years for passenger screening, but not so much for cargo screening. Most airports now use X-ray security screening for containers and unit load devices (a pallet or container used to load cargo on aircraft, permitting a large quantity of cargo to be bundled into a single unit) providing an image of the contents without the need for physical interference. Yet it is still the human operator (security officer) who needs to identify prohibited items in the X-ray image and make the decision on whether the inspected unit can be regarded as harmless or not. Consequently, methods must continue to be explored for enhancing operators' ability to identify threats.

Knowledge-Based and Image-Based Factors

From previous research results and observations of the performance of security personnel, both knowledge-based and image-based factors appear to have a significant impact on human detection performance (Michel, Mendes, de Ruiter, Koomen, & Schwaninger, 2014). Knowledge-based factors relate to knowing which items are prohibited, what they look like in X-ray images, and how they can be distinguished visually. They are particularly relevant for objects, such as IEDs, that are rarely seen in everyday life and that look quite different in an X-ray image. Image-based factors are characteristics of the X-ray images of the objects. For example, objects are more difficult to recognize if shown from an unusual viewpoint or when superimposed by other objects. Recognition is also affected by the complexity of the image, which depends on the number and types of other objects.

Addition of Color to X-Ray Images

Recent X-ray technologies have material discrimination capability that employs color to aid the threat-detection process. Material types (such as organic, inorganic, and metal) are rendered in different colors that overlay the original gray image. According to Michel et al. (2014), although this technology holds the potential to improve the screening process, additional human factors evaluations are necessary because the introduction of color images has not demonstrated an improvement in comparison with the grayscale images in experimental tests to date. For example, colors introduced into the cognition and perception processes might serve as distractors during target detection and resolution.

Computer-Based Training for Cargo Screening

Research conducted by Mendes, Michel, and Schwaninger (2013) demonstrated that customized computer-based training can significantly improve operator performance in cargo X-ray image interpretation. During a three month study, one group of experienced cargo screeners received a minimum of 20 minutes of training per week, whereas a control group from the same population received no training over the same period. Both groups were tested before and after the training with a computer-administered test consisting of 240 X-ray images, half of which contained prohibited items relevant for customs concerns (e.g., drugs, weapons) as well as for security screening (e.g., explosives, IEDs). The X-ray images were provided in both grayscale and with color enhancement. The task of the screeners was to distinguish between clear images (nothing of concern) and images containing prohibited items (something to report). The results of the study revealed significant increases in detection performance for screeners having received the weekly training, whereas the control group showed no change. The effect of training was particularly high for the detection of IEDs. Moreover, the larger the number of training hours received by a screener, the better the test performance.

During training, the screener received an immediate response feedback as to whether the response was correct or not. When a prohibited item was contained in the image, information on this item was also provided. Test performance of individual participants correlated positively with the number of training hours they received; these results were similar for displays presented in grayscale and those with color enhancement. Further, a general decrease in the inspection time per image was found for the group that received training. It is noteworthy that the baseline detection performance of both groups measured before training was very low for certain prohibited items, further underlining the significance of training for cargo X-ray screening.

Detection of Deception

The majority of published research on detecting deception has set out to identify indicators of human behavior that can discriminate deceivers from truth-tellers. Behavioral indicators of deception relate to observable demeanor and/or actions such as nervousness, aggression, eye contact, fidgeting, and verbal hesitations. Although the effectiveness of behavioral indicator approaches has never been tested in a large-scale field trial, a meta-analysis of laboratory studies that used behavioral indicators to discriminate deceivers from truth-tellers revealed a mean rate for correct identification at only slightly above chance (Bond & DePaulo, 2006), inspiring little confidence that the approach would be effective for detecting a deceiver from among the large numbers of truth-tellers among airline passengers. Even so, as discussed earlier, the TSA initiated the use of behavioral indicators in 2007 in their SPOT program through the employment of behavioral detection officers. That program eventually came under considerable criticism for its cost and ineffectiveness and, as discussed earlier, in 2013, the GAO recommended that future funding for this program be limited.

Ormerod and Dando (2014) have proposed veracity testing for detecting deception, focusing on the verbal exchange between the sender (the individual attempting to deceive) and the receiver (the individual attempting to detect deception). (This approach, based on verbal interactions, differs from the deception indicators employed in the SPOT program that were based on observation of the nonverbal behavioral indicators discussed earlier.) Ormerod and Dando reviewed a number of research studies and identified six aspects of dyadic verbal exchanges that appear to have the potential for discriminating between deceivers and truth-tellers. These are summarized as follows:

1. Interviews that use tactical and strategic information-gathering methods. The receiver first explores the sender's accounts, guided by information known to them before the interview, but without revealing to the sender what is known. The sender's responses are then compared with the known information and challenged when inconsistencies arise by revealing the information (Dando, Bull, Ormerod, & Sandham, 2015).

2. Questioning styles that elicit rich verbal accounts, such as open questions that do not constrain responses, require expansive answers and commit passengers to an account of the truth concerning issues such as identity, background, and previous, current, or future activities. (Oxburgh, Myklebust, & Grant, 2010).
3. Tests of expected knowledge, which compare the content of what someone says with information already known (Blair, Levine, & Shaw, 2010).
4. Interviewing methods that restrict the verbal maneuvering, the strategic manipulation by deceivers of verbal content, and delivery to control a conversation to avoid detection (Taylor et al., 2013).
5. Procedures that raise the cognitive load faced by an interviewee, such asking a question unlikely to be anticipated (Walczyk, Igou, Dixon, & Tcholakian, 2013).
6. The length of responses—truth-tellers speak longer, say more, and use more unique words than deceivers (Morgan, Rabinowitz, Hilts, Weller, & Coric, 2013).

Ormerod and Dando (2014) developed a method for applying the veracity concept to deception detection and conducted a double-blind randomized-control study involving 165 security agents and 204 mock passengers at international airports. Each mock passenger was provided with a valid ticket, an itinerary of flights, and a deceptive cover story to be maintained during the security interview and queued with other passengers to pass through the security process. Security agents detected 66% of the deceptive passengers using the veracity testing methodology. This compared with the detection of less than 5% using behavioral indicator recognition methodology described earlier in this section.

Performance of Full Body X-Ray Scanners

Full-body X-ray scanners started replacing metal detectors at airports in many countries in 2007. A full-body scanner is a device that detects both metallic and nonmetallic objects on a person's body for security screening purposes, without the need to physically remove clothes or make physical contact. Depending on the specific technology, the operator may see an image of the person's naked body, or just a cartoon-like representation of the person, with indicators showing the location of any suspicious items. Full body X-ray scanners were faster than previous scanning methods (taking only about 15 seconds) and did not require passengers to physically remove clothing. In the United States, pursuant to the FAA Modernization and Reform Act of 2012, all full-body scanners operated in airports by the TSA now must use automated target recognition software, which replaces the picture of a nude body with the cartoon-like representation to show the screener the location of suspicious items. According to the TSA, there are now, in 2015, as many as 740 of these units employing the advanced imaging technology at 160 airports nationwide.

At this time, there have been no evaluation studies completed on the effectiveness of the recently employed full-body X-ray scanners. On the other hand, a number of studies were completed on the Rapiscan Secure 1000, the full-body scanner that was deployed at U.S. airports between 2009 and 2013. Most of these studies revealed vulnerabilities in passenger screening employing these scanners. A representative sample of this research was that completed by a team of researchers from the University of California, San Diego, the University of Michigan, and John Hopkins University (Mowery et al., 2014) that claimed theirs' was the first analysis and laboratory testing that was independent of the device's manufacturer and its customers, and the first to consider software as well as hardware.

The researchers concluded that the system was ineffective in reliably detecting concealed knives, guns, and explosives against an adaptive adversary who has access to a device for study and to use for testing and refining attacks. They also concluded that the flaws identified could be partly remediated through changes to procedures such as performing side scans in addition to front and back

scans, and by screening subjects with magnetometers as well as a backscatter scanner. But they also concluded that these procedural changes would significantly lengthen screening times, thus eliminating one of the key advantages of the system.

Despite the flaws identified in the Rapiscan Secure 1000, the researchers did not categorically reject TSA's claim that advanced image technology represents the best available tradeoff for airport passenger screening. The millimeter-wave scanners that are currently deployed to airports are likely to behave differently from the system that was studied. However, it was recommended that these full-body scanners be subjected to independent, adversarial testing, and that this testing specifically consider software security.

LOOKING AHEAD

Solving Continuing Problems

Air Line Pilots Association Perspective

As the representative of more than 53,000 pilots who fly for airlines in the United States and Canada and with its 80-year history, Air Line Pilots Association provides a unique and important perspective for analyzing the current state of aviation security and identifying the continuing problems that need to be solved. It provides regular analyses of issues of importance to air line pilots, employees, and passengers on the internet at www.alpa.org. In a recent analysis, it identified and reported the following proposed improvements in aviation security that are most in need of additional research and development with attention to human factors considerations.

- Implementation of Threat-Based Security. Although TSA has publicly committed to pursuing a threat-based approach to aviation security and some steps have been taken, threat-based security should be adopted across the board as a foundational philosophy and as a plan of action to address today's threats. A threat-based approach will ultimately enhance passenger privacy, create a more efficient and effective screening system, and make better use of limited screening resources.
- Enhanced Security of All-Cargo Flight Operations. Continuing efforts need to be expended in closing the gaps in security requirements for all-cargo flight operations. In particular, improvements are needed in the background vetting of individuals with unescorted access to cargo aircraft and cargo, hardened flight deck door requirements, and perimeter security protocols that clearly define entry and exit procedures and dictate specific identification display and ramp security procedures.
- Introduction of Threatened Airspace Management. A prioritized plan for control of the national airspace system during a major security event is needed to provide pilots in command of airborne aircraft, or those about to take off, with real-time notification of significant and ongoing security concerns.
- Aircraft Protection from Laser Attacks. FAA statistics show that the threat to aviation safety from laser attacks is growing and real, with an exponential increase in reported laser attacks against aviation. Efforts are needed to develop and test possible countermeasures that will minimize both the likelihood of these attacks and their possible impact.

Department of Homeland Security Perspective

The long-range research and development test and evaluation plan prepared by DHS (2012b) provided strategic objectives for the continuing development and enhancement of aviation security. A brief summary of each of the objectives that have implication for future human factors research and development is provided here.

- Enhanced detection performance of security systems. The principal areas of research identified for meeting this goal are developing more reliable methods for characterizing the signatures and indicators of emerging threats, developing tools and procedures for more effective alarm resolution, and increasing the efficiency and certainty of the testing conducted to evaluate the implementation of new technologies.
- Improved passenger experience in the screening process. Research conducted to help meet this goal would focus on solutions, technological, and procedural, which might decrease the physical invasiveness of screening modes and increase the efficiency with which passengers proceed through the screening processes. Possible solutions include the development and evaluation of procedures that do not involve direct contact with or actions required by passengers.
- Enabled risk-based and intelligence-driven screening processes. It is hypothesized that risk-based screening would allow the TSA to focus resources on high-risk individuals or threat objects, increasing the overall effectiveness and efficiency of passenger aviation screening. Research would address the development and evaluation of systems that would provide for a rapid adjustment of risk posture, enhancement of behavior-based targeting, and improved data processing and decision-making.
- Enhanced threat response capability with more flexible security solutions. The concern is that present security structures and procedures are not sufficiently flexible to respond to changing or emerging threats. Research is required for the development security systems that are more easily and quickly adaptable to changing threats.
- Other desired improvements in technology and procedures. A variety of other desired improvements must be derived from the application of science to specific problems identified by the DHS. They include improvements in the following: blast mitigation capabilities, behavior detection and biometric identification, anomaly detection, high throughput threat detection, system resilience and recovery, and freight tamper prevention and detection.

Security Topics Identified at the 2014 Aviation Security Summit

The 14th Annual Security Summit was hosted on November 17, 2014 by the American Association of Airport Executives (AAAE) in cooperation with the DHS and TSA. A product of the summit was identification of the principal aviation security concerns of those in attendance, as summarized in the following.

Risk-Based Security: Constantly assessing the operating environment and being able to discern new threats as they present themselves is a capability being developed in the industry. Learning how to adapt under different conditions and to apply the appropriate security measures is an essential component of a risk-based security program. TSA is working hard to adapt its security protocols to this philosophy, finding that it allows for greater flexibility for both its own personnel and all those affected.

TSA Precheck Program: Approximately 30% of the flying public is now taking advantage of the TSA's Precheck program with efforts in place working to expand the program to include aviation employees such as flight crew members, fueling personnel, and ramp workers who have already undergone background checks to obtain airport access. New innovations in the program could allow better matching between program participants and their luggage should an associated security protocol be activated in baggage handling.

Addressing the Changing Mix of Future Threats

Ideally, new threats are met with fast, nonintrusive, and flawless passenger screening that is 100% effective against the latest terrorist devices and concealment methods, while anticipating

and thwarting new threats. The system must effectively screen every passenger and every piece of checked and hand-carried luggage nearly 800 million times a year. At the same time, passenger screening should be discerning but democratic. Intelligence must keep terrorist suspects off flights but without errors that affect innocent travelers, and it must accomplish this without government-held databases that appear to threaten civil liberties. Although attaining all of these objectives would be considered by most involved in aviation security to be impossible, it is clear that knowing and understanding the changing mix of threats faced by aviation security is critical and worthy of an increasing level of effort.

The Combatting Terrorism Center (CTC) at the United States Military Academy in West Point, New York, in their 2011 assessment of terrorist threats to commercial aviation (Brandt, 2011) anticipated the critical future threats to be addressed by aviation security. The CTC focused on insider threats, threats from ranged weapons, evolving threats from explosive devices, and threats against airline facilities and airports. The reports from the TSA and others added threats from thermite-based incendiary devices, threats in the form of cyber-attacks, and threats from drones.

Insider Threats

Examples of insider threats that have been discovered during the past 10 years include a man seeking to become a flight attendant to stage a suicide attack and attempts by terrorists to recruit airport employees such as baggage handlers, security staff, and mechanics to participate in various plots. Although TSA and airport investigators currently conduct criminal and terrorist database checks on potential airport, airline, and vendor employees who are to be granted access to secure areas, there are apparently vulnerabilities in their approach. For example, according to the CTC, street gangs have gained employment and carried out criminal activities such as narcotics trafficking, baggage theft, and prostitution at airports nationwide. The magnitude of this vulnerability is compounded because most airport employees working in secure areas do not undergo security screening prior to entering their workspace due to practical constraints

Threats from Explosive Devices

IEDs are likely to remain a significant threat to commercial aviation due to limitations in current screening technology. According to the CTC, even the latest enhancements in bomb detection technology can be defeated by surgically implanting a device or secreting it within a body cavity. Moreover, IEDs concealed within complex electronic devices are likely to defeat all but the most thorough visual inspection.

Threats against Airline Facilities and Airports

Airport facilities, such as fuel lines, arrival halls, and curbside drop-off points, are likely to continue to be tempting targets, as are aircraft that can be reached by breaching the airport perimeter fencing to assault aircraft on runways, taxiing areas, and at gates. Airport facilities are likely to be more vulnerable in the future, particularly if terrorists continue their emphasis on making smaller scale attacks on targets of opportunity.

Threats from Ranged Weapons

Ranged weapons are small portable weapons such as rocket-propelled grenades and small surface-to-air missiles that can be launched at a target from a distance. These weapons are becoming more accessible to terrorist groups through thefts from military depots and through gifts from sympathizers.

Threats from Thermite-Based Incendiary Devices

In a bulletin released to its intelligence customers, the TSA (2014c) warned of a thermite-based incendiary device, the ignition of which on an aircraft at altitude could result in catastrophic damage and the death of every person on board. The bulletin stated that the devices are easily assembled

and concealable, and that current TSA screening procedures would likely not recognize thermite-based mixtures. Thermite is made of rust and aluminum powder (both substances are easily obtainable) and, when ignited, burns violently at extremely high temperatures and is capable of spraying molten metal in all directions.

Threats in the Form of Cyber-Attacks

Cyber security was a principal concern raised at the November 17, 2014 Aviation Security Summit hosted by the AAAE in cooperation with the DHS and TSA. Cyber security is growing in importance because aircraft systems are typically not encrypted and therefore vulnerable to hackers. Central to this concern of cyber security is the human factor. In many cases, cyber security faults are caused by staff that click on a malware link or unknowingly breach security in hundreds of small ways.

Threats from Drones

Recent reports from pilots of commercial airliners have identified drones as a potential threat to aviation security. As reported in the Washington Post (Whitlock, 2014), two pilots reported sightings on the same day of large drones operating at high altitudes near their aircraft. One sighting over New York City from a pilot landing at LaGuardia Airport was of a black drone with an estimated 15-foot wingspan flying at about 5,500 feet above Lower Manhattan. The other sighting from two airliners approaching Los Angeles International Airport was of a remote-controlled aircraft the size of a trash can at an altitude of 6,500 feet. A NASA database contains 50 reports over the past 10 years, and the FAA database has 15 reports over just the past two years of close calls or improper flight operations involving drones.

Capitalizing on New Procedures and Technologies

Risk-based approaches to aviation security have been proposed as part of a comprehensive, multilayered approach to aviation security rather than as an alternative approach. Risk-based programs are envisioned to closely interact with physical screening checkpoint measures to allow TSA to focus physical screening resources on unknown and elevated risk passengers. They also inform the protocols that TSA utilizes to modify security postures based on known or perceived threats. The TSA and others have proposed the development and evaluation of specific procedures and technologies to support the implementation of risk-based approaches to aviation security (Elias, 2014; Pistole, 2014; TSA, 2014a). These are presented and discussed in this final section of the chapter; each is subject to human factors considerations, concerns, and implications for research and testing.

Checkpoint of the Future

In its Press Release Number 35 of June 7, 2011, the International Air Transport Association discussed its vision for the *checkpoint of the future*, a series of neon-lit tunnels, each equipped with an array of eye-scanners, X-ray machines, and metal and liquid detectors. Heralding an end to *one size fits all screening*, the association says that passengers will be assigned a *travel profile* and ushered into one of three corridors accordingly. Thermal lie detection has been proposed to be implemented with a camera that can detect variations in facial temperature in response to questioning. Human factors are likely to play a significant role in the design of the tunnels and the passenger interaction with the various screening technologies and equipment.

Credential Authentication Technology

The TSA envisions the development of technology that would automatically authenticate identity documents presented to TSA screeners by passengers during the security checkpoint screening process. Assuming an optimal interaction between passengers, screeners, and the authentication technology, the system would both enhance security and increase screening efficiency by automatically verifying passenger's identification and obtaining their vetting status.

Paperless Boarding Pass

The paperless boarding pass, an encrypted bar code along with passenger identification and flight information, enables passengers to download their boarding pass to their cell phones or personal digital assistants. The objective of this approach is to streamline the boarding process at the checkpoint while also increasing the ability to detect fraudulent boarding passes. Passengers would continue to be required to show photo identification so officers can validate that the name on the boarding pass matches that of the passenger's identification. Critical issues to assuring the successful employment of paperless boarding passes are the user friendly design of the cell phone software, the handling of passengers without cell phones, and the expeditious handling of problem cases.

Biometric Identification

Biometric identification is being explored because it permits verification of a person's identity by employing his or her own unique set of biological identifiers—fingerprints, iris scans, or a combination of the two. The TSA is testing this technology at airports across the country. The success of this approach would seem to depend on the efficient, minimally intrusive, and error-proof manner in which passengers provide their fingerprints and iris scans.

Bottled Liquids Scanners

Bottled liquids screening systems are being considered by TSA to detect potential liquid or gel threats, which may be contained in a passenger's property. The technology employed must be capable of differentiating liquid explosives from other liquids in amounts that are permitted. Potentially applicable technology includes laser, infrared, and electromagnetic resonance. A critical consideration would appear to be the manner in which this screening component is incorporated into the overall passenger screening process to maintain adequate passenger flow.

Explosives Trace Detection

Explosives trace detection (ETD) is technology used at security checkpoints around the country to screen baggage and passengers for traces of explosives. Officers may swab a piece of carry-on or checked baggage or a passenger's hands and then place the swab inside the ETD unit to analyze it for the presence of potential explosive residue. This is an awkward and relatively time-consuming process for passengers; one that seems ripe for technological innovation. A recent problem, somewhat similar to this one that has been solved by technology, is that of measuring body temperature. The most common approach, employed for years, has required shaking a small thermometer, after it has been sanitized with alcohol, to lower the liquid below the level of the expected body temperature, inserting the bulb end of the thermometer in an oral cavity for approximately three minutes, and then reading the liquid level to determine the temperature. The new temporal artery thermometer simply requires a swipe across the forehead.

Airport Scanner Game as a Research Tool

Data collected from the video game, airport scanner, and analyzed by researchers at the Duke Institute for Brain Sciences, indicate the possible potential of such games as research tools. In the Airport Scanner game, players earn points by tapping on illegal items as simulated X-ray images of airport passenger bags roll across their screens. The game collects anonymous data on how players perform, providing researchers the results from about a million trials a day, far more information than could possibly be obtained in a more traditional laboratory setting. By analyzing these gameplay data, researchers have been able to identify some of the common mistakes the human brain makes while searching for things (Mitroff et al., 2015).

SUMMARY AND CONCLUSIONS

As stated in the introduction, the objective of this chapter is to address the ever more critical and significant role that human factors play in aviation security. A historical background of important security events and the associated human factors issues was presented, focusing mainly on those dating from publication of the previous *Handbook of Human Factors in Aviation* published in 2009. The chapter reviewed human factors research approaches and findings, and their resulting operational applications to elements of aviation security. An important part of this review was the findings of the periodic critical assessments of aviation security by the GAO and others, which were summarized and their implications for human factors research and development discussed. The chapter also looked ahead to the continuing human factors problems that remain to be solved, predicting the changing mix of threats that will need to be addressed by human factors research, and anticipating the types of new procedures and technologies for which human factors issues will need to be identified and resolved.

This handbook is being published at the time of a major turning point in aviation security. The TSA, after having applied relatively inflexible methods to aviation security since its inception, is now shifting away from this *one size fits all* approach to what is being called a *risk-based* approach. Thus far, the development of this approach has emphasized identifying and focusing on high-risk passengers, while expediting the processing of passengers predetermined to be of low risk. Issues yet to be tested are the efficacy of the specific program elements and the extent to which they complement each other and enhance the effectiveness of the overall security process. Discussion of the many human factors issues to be addressed, as elements of risk-based approaches are introduced and tested, constitutes an important part of this chapter.

Operator capabilities and performance are critical to the effectiveness of systems developed and installed to assure aviation security. Human visual search and detection skills, in particular, have played a critical and central role since the initiation of passenger and baggage screening at airports. The application of operator skills requires a repetitive visual search of multiple target items on multiple images, and on the detection and classification of a target as either acceptable or requiring further investigation. The results of research studies have shown that successful visual search and detection requires the application of a number of specific human skills and technologies while also overcoming factors likely to degrade performance. Human factors were found to play a significant role in aviation security beyond that of visual search and detection during passenger screening including the assignment of security tasks, establishment of layers of defense in airport security, screening of air cargo, detection of passenger deception, and the operation and performance of screening with full-body X-ray scanners.

Looking ahead, the chapter identified and discussed the following as continuing problems that will require human factors research and development from the perspective of the organizations most concerned with aviation security. From the perspective of the Air Line Pilots Association, the major continuing problems are the implementation of threat-based security, enhancement of the security of all-cargo flight operations, institution of airspace management, and aircraft protection from laser attack. From the perspective of the DHS, the following continuing problems should be given priority: enhancing the detection performance of security systems, improving the passenger experience in screening process, enabling risk-based and intelligence-driven screening processes, and enhancing threat response capability with more flexible screening solutions. The AAAE at their 2014 Annual Security Summit focused on risk-based security and enhancement and expansion of the TSA Precheck Program as their highest priorities for further development.

The changing mix of threats likely to be faced by aviation security in the future was addressed by the CTC. The CTC identified insider threats, threats from ranged weapons (small portable weapons such as rocket-propelled grenades and small surface-to-air missiles), evolving threats from explosive devices, and threats against airline facilities and airports. Reports from the TSA and others

added threats from thermite-based incendiary devices, threats in the form of cyber-attacks, and threats from drones.

Risk-based approaches to aviation security have been proposed as part of a comprehensive, multilayered approach to aviation security rather than as an alternative approach. Risk-based programs are envisioned to closely interact with physical screening checkpoint measures to allow TSA to focus physical screening resources on unknown and elevated risk passengers. The anticipated new procedures and technologies to be employed in support of this approach are as follows: checkpoint reconfiguration, credential authentication technology, paperless boarding passes, biometric identification, bottled liquids scanners, enhanced explosives trace detection, enhanced explosives trace detection, and video games as research and training tools.

REFERENCES

Andriessen, H., Gulijk, C., & Ale, B. (2012). Human factors in layers of defense in airport security. In *11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference* (pp. 4325–4332). Red Hook, NY: Curran Associates.

Askew, G. (2004, November). *Who is the screening boss? Does it really matter?* Aviation Security (AVSEC) 2004 World Conference Proceedings, Vancouver, British Columbia, Canada.

Aviation Security International (2015, January). Security screening: Improving human performance for greater reliability. Retrieved March 8, 2015, from: http://www.asi-mag.com/security-screening-improving-human-performance-greater-reliability/

Basner, M., Rubinstein, J., Fomberstein, K. M., Coble, M.C, Ecker, A., Avinas, D., & Dinges, D.F. (2008). Effects of night work, sleep loss and time on task on simulated threat detection performance. *Sleep*, *19*, 1251–1259.

Blair, J. P., Levine, T. R., & Shaw, A. S. (2010). Content in context improves deception detection accuracy. *Human Communication Research, 36*(3), 423–442.

Bloom, R. W. (2011, July–August). Airport security: Which poses the greatest threat—passengers or air cargo? *TR News*, pp. 21–27.

Bolfing, A., Halbherr, T., & Schwaninger, A. (2008). How image based factors and human factors contribute to threat detection performance in X-ray aviation security screening. *HCI and Usability for Education and Work*, *Lecture Notes in Computer Science, 5298*, 419–438.

Bond, C. F. Jr., & DePaulo, B. M. (2006). Accuracy of deception judgements. *Personality and Social Psychology Review, 10*(3), 214–234.

Brandt, B. (2011, November). Terrorist threats to commercial aviation: A contemporary assessment. *Combating Terrorism Center at West Point Military Academy.* Retrieved March 9, 2015, from: https://www.ctc.usma.edu/posts/terrorist-threats-to-commercial-aviation-a-contemporary-assessment

Dando, C. J., Bull, R., Ormerod, T. C., & Sandham, A. L. (2015). Helping to sort the liars from the truth-tellers: The gradual revelation of information during investigative interviews. *Legal and Criminological Psychology, 20*(1), 114–128.

Davies, D., & Parasuraman, R. (1982). *The psychology of vigilance*. London, UK: Academic Press.

Department of Homeland Security (DHS), Office of Inspector General (2013a, May). *Transportation Security Administration's Screening of Passengers by Observation Techniques.* (Report OIG-13-91.)

Department of Homeland Security (DHS) (2013b, August). Strategic plan for fiscal years (FY) 2012–2016. Retrieved March 9, 2015, from: http://www.dhs.gov/strategic-plan-fiscal-years-fy-2012-2016

Elias, B. (2009). *Airport passenger screening: Background and issues for Congress.* Congressional Research Service Report R40543.

Elias, B. (2014). *Risk-based approaches to airline passenger screening.* Congressional Research Service Report R43456.

Feng, C. (2003). A review of aviation security organization. In L. W. Lan (Ed.), *The new challenge of international transportation security* (pp. 73–84). Institute of Traffic and Transportation, National Chiao Tung University, Taiwan.

Fleck, M. S., & Mitroff, S. R. (2007). Rare targets rarely missed in correctable search. *Psychological Science, 18*(11), 943–947.

Ghylin, K., Drury, C., & Schwaninger, A. (2006, July). Two-component model of security inspection: Application and findings. *16th World Congress of Ergonomics*, *IEA 2006*, Maastricht, the Netherlands, July, 10–14, 2006.

Gibb, G., & Lofaro, R. (2009). Human factors in civil aviation security. In J. A., Wise, V. D. Hopkin, & D. J. Garland (Eds.), *Handbook of aviation human factors* (2nd Ed.), 27-1–27-30. Boca Raton, FL: CRC Press.

Gladwell, M. (2001). Safety in the skies. *New Yorker*, 50–53, October 1, 2001.

Government Accountability Office (GAO) (2012, September). *9/11 Anniversary observations on TSA's progress and challenges in strengthening aviation security*. General Accountability Office Publication GAO-12-1024T.

Government Accountability Office (GAO) (2013, November). *Aviation security: TSA should limit future funding for behavior detection activities*. General Accountability Office Publication GAO-14-159.

Government Accountability Office (GAO) (2014, December). *Rapid growth in expedited passenger screening highlights needs to plan effective security assessments*. General Accountability Office Publication GAO-15-150.

Green D. M., & Swets, J. A. (1967). *Signal detection theory and psychophysics*. New York: John Wiley & Sons.

Harris, D. H. (2002). How to really improve airport security. *Ergonomics in Design, 10*, 17–22.

Harris, D. H., & Chaney, F. B. (1969). *Human factors in quality assurance*. New York: John Wiley & Sons.

Howell, W. C., & Cooke, N. J. (1989). Training the human information processor: A review of cognitive models. In I. Goldstein (Ed.), *Training and development in organizations* (pp. 121–182). San Francisco, CA: Jossey-Bass.

Ilgen, D. R., & Klein, H. J. (1988). Individual motivation and performance: Cognitive influences on effort and choice. In J. P. Campbell & R. J. Campbell (Eds.), *Productivity in organizations* (pp. 143–176). San Francisco, CA: Jossey-Bass.

Jenkins, B. M. (2012). *Aviation security: After four decades, it's time for a fundamental review*. Homeland Security and Defense Center Occasional Paper, RAND Corporation, Santa Monica, CA.

Mackie, R. (1987). Vigilance research –Are we ready for countermeasures? *Human Factors, 29*, 707–724.

Mackworth, J. (1970). *Vigilance and attention*. Harmondsworth, UK: Penguin Books.

Maddox, W. T. (2002). Toward a unified theory of decision criterion learning in perceptual categorization. *Journal of the Experimental Analysis of Behavior, 78*, 567–595.

Mendes, M., Michel, S., & Schwaninger, A. (2013). Cargo screening: Enhancement of human factors. *Aviation Security International*, 29-30, October 2013.

Menneer, T., Donnelly, N., Godwin, H. J., & Cave, K. R. (2010). High or low target prevalence increases the dual-target cost in visual search. *Journal of Experimental Psychology: Applied, 16*(2), 133–144. doi:10.1037/a0019569

Michel, S., Mendes, M., de Ruiter, J., Koomen, G., & Schwaninger, A. (2014). Increasing X-ray image interpretation competency of cargo security screeners. *International Journal of Industrial Ergonomics, 44*, 551–560.

Mitroff, S. R., Biggs, A. T., Adamo, S. H., Dowd, E. W., Winkle, J., & Clark, K. (2015). What can 1 billion trials tell us about visual search? *Journal of Experimental Psychology*: *Human Perception & Performance, 41*(1), 1–5. doi:10.1037/xhp0000012

Morgan, C. A., Rabinowitz, R. G., Hilts, D., Weller, C. E., & Coric, V. (2013). Efficacy of modified cognitive interviewing compared to human judgments in detecting deception related to bio-threat activities. *Journal of Strategic Security, 6*, 100–119. doi:10.5038/1944-0472.6.3.9

Mowery, K., Wustrow, E., Wypych, T., Singleton, C., Comfort, C., Rescorla, E., Checkoway, S., Halderman, A., & Shacham, H. (2014, August), Security analysis of a full-body scanner. Proceedings of the 23rd USENIX Security Symposium, San Diego. Retrieved March 9, 2015, from https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/mowery

National Research Council (NRC). (1996). *Airline passenger security screening: New technologies and implementation issues* (Publication NMAB-482-1). Washington, DC: National Academy Press.

Ormerod, T. C., & Dando, C. J. (2014). Finding a needle in a haystack: Towards a psychologically informed method for aviation security screening. *Journal of Experimental Psychology*: *General, 144*(1), *78*–84.

Oxburgh, G. E., Myklebust, T., & Grant, T. (2010). The question of question types in police interviews: A review of the literature from a psychological and linguistic perspective. *International Journal of Speech Language and the Law, 17*(1), 45–66.

Parasuraman, R., Molloy, R., Mouloua, M., & Hilburn, B. (1996). Monitoring of automated systems. In R. Parasuraman & M. Mouloua (Eds.), *Automation and human performance*: *Theory and applications* (pp. 91–115). Mahwah, NJ: Erlbaum.

Pistole, J. S. (2014, April 30). Statement of John S. Pistole, Administrator, Transportation Security Administration, U. S. Department of Homeland Security, before the United States Senate, Committee on Commerce, Science, and Transportation. Retrieved March 9, 2015, from https://www.tsa.gov/sites/default/files/assets/pdf/SenateCommerce_jsp.pdf

Poole, R. W., & Passantino, G. M. (2003, May). *Risk-based airport security policy.* Reason Foundation. Reason Public Policy Institute, Policy Study 308.

Poole, R. W., & Ybarra, S. (2013, July). *Overhauling U. S. airport security screening.* Reason Foundation. Reason Public Policy Institute. Retrieved March 8, 2015, from http://reason.org/news/show/overhauling-us-airport-security-scr

Rasmussen, J. (1986). *Information processing and human-machine interaction: An approach to cognitive engineering*. New York: North-Holland.

Reason, J. (1990). *Human error.* Cambridge, MA: Cambridge University Press.

Schwaninger, A., Hardmeier, D., & Hofer, F. (2005). Aviation security screener's visual abilities & visual knowledge measurement. *IEEE Aerospace and Electronic Systems, 20*(6), 29–35.

Schwaninger, A., & Hofer, F. (2004). Evaluation of CBT for increasing threat detection performance in X-ray screening. In K. Morgan & M. J. Spector (Eds.), *The Internet society 2004*, *advances in learning*, *commerce and security* (pp. 147–156) Wessex, UK: WIT Press.

Swezey, R. W., & Salas, E. (1992). Guidelines for use in team-training development. In R. W. Swezey & E. Salas (Eds.), *Teams: Their training and performance* (pp. 219–245). Norwood, NJ: Ablex.

Taylor, P. J., Dando, C. J., Ormerod, T. C., Ball, L. J., Jenkins, M. C., Sandham, A., & Menacere, T. (2013). Detecting insider threats through language change. *Law and Human Behavior, 37*, 267–275. doi:10.1037/lhb0000032

Transportation Security Administration (TSA) (2014a, February). Risk-based security initiatives. Retrieved March 9, 2015, from http://www.tsa.gov/traveler-information/risk-based- security-initiatives

Transportation Security Administration (TSA) (2014b, October). Security technologies: Threat image projection. Retrieved March 7, 2015, from http://www.tsa.gov/about-tsa/security-technologies

Transportation Security Administration (TSA), Office of Intelligence and Analysis (2014c, December). Other agency product of interest (OA-PoI). Retrieved March 9, 2015, from https://prod01-cdn00.cdn.firstlook.org/wp-uploads/sites/1/2015/02/TSA-Bulletin.pdf

Transportation Security Administration (TSA) (2015, February). Layers of U.S. aviation security. Retrieved March 9, 2015, from http://www.tsa.gov/about-tsa/layers-security

Walczyk, J. J., Igou, F. P., Dixon, A. P., & Tcholakian, T. (2013). Advancing lie detection by inducing cognitive load on liars: A review of relevant theories and techniques guided by lessons from polygraph-based approaches. *Frontiers in Psychology, 4*(14), 4–14.

Whitlock, C. (2014). Close encounters on rise as small drones gain in popularity. *Washington Post*, June 23, 2014.

Wiener, E. L. (1988). Cockpit automation. In E. L. Wiener & D. C. Nagel (Eds.), *Human factors in aviation* (pp. 433–461). San Diego, CA: Academic Press.

Wolfe, J. M., & Van Wert, M. (2010). Varying target prevalence reveals two dissociable decision criteria in visual search. *Current Biology, 20*, 121–124.

Wolfe, J. M., Horowitz, T. S., & Kenner, N. M. (2005). Rare items often missed in visual searches. *Nature, 435*, 439–440.

Wolfe, J. M., Horowitz, T. S., Van Wert, M. J., Kenner, N. M., Place, S. S., & Kibbi, N. (2007). Low target prevalence is a stubborn source of errors in visual search tasks. *Journal of Experimental Psychology*: *General, 136*(4), 623–638. doi:10.1037/0096-3445.136.4.623

Yoo, K. (2009). A study on factors influencing the performance of airport security and on responsibility assignment of security task at international airports. *Journal of Aviation/Aerospace Education & Research, 19*(1), 37–50.

Yoo, K., & Lee, J. (2004). *Airport security: Establishing a clear chain of command*. Aviation Security (AVSEC) 2004 World Conference Proceeding, Vancouver, British Columbia, Canada.