Inflight Entertainment and Aviation Security . . . Is There a Connection?

By Robert M. Peterson

The events of September 11, 2001, sent shock waves throughout the commercial aviation industry. Six years later, the effects are still lingering. Although the industry has been fortunate in the fact that the terrorists have been unsuccessful in launching any new attacks against commercial aviation, our industry remains a primary target of terrorism. This was clearly evidenced by the events on August 10, 2006, as the British government apparently took down a plot to attack commercial airliners over the Atlantic Ocean.

So what does this have to do with IFE? Besides the resulting crimp in the revenue stream of IFE providers resulting from the 9/11 events, IFE and Aviation Security are unrelated, right? Wrong!

Just the opposite, in fact. To some extent, each and every person involved in IFE is involved in the war on terror and in protecting commercial aviation from the threats of another 9/11, a hijacking, or some other attack on the international Airline industry. The truth is, we are all involved in this war on terror. We are all on the front line of this war.

Before the business development staffs get carried away with potential new product opportunities, it needs to be clear that this link between IFE providers and aviation security is not focused on new products, new technology, or new business opportunities. There are business opportunities, and there are IFE providers pursuing that business. The issue of aviation security is considerably more pervasive than technology opportunities. To fully understand the links between aviation security and IFE, we must understand the nature of terrorism, as the war on terrorism must be fought on multiple levels.

The first known aircraft hijacking occurred in Peru in 1930. We had airplane hijackings in the '60s, but for many years, a hijacking, although disconcerting, was little more than an unscheduled side trip to Cuba. In 1969 the incidents turned more ominous when Arab extremists hijacked a TWA flight bound for Israel and diverted it to Syria. Then, in September 1970, terrorists blew up four commercial airliners in the desert of the Middle East, prompting President Richard Nixon to announce a comprehensive federal antiterrorist program, including the initiation of the Federal Air Marshall program. Ironically, this action was taken on September 11, 1970.

Between 1970 and September 11, 2001, multiple hijackings or inflight bombings occurred. During this period, many enhanced security measures were proposed or promulgated, and several minor procedural improvements for security were implemented. A little-noticed incident in January 1995 foretold the future, but went virtually unnoticed. A plot to blow up 10 US airliners over the Pacific Ocean by a fundamentalist terrorist organization with Al Qaeda connections using liquid explosives was thwarted when one of the bombs blew up in the apartment of the bomb maker before the attack could be launched.

The official September 11 Commission report identified several other harbingers of the events of 9/11 that went unnoticed, enabling the Al Qaeda plot to proceed under the radar

screen of our intelligence agencies. As has been reported numerous times, one of the biggest mistakes made during this period was our collective unwillingness or inability to imagine the possible. In the nearly six years following the terrible events of that day, many steps have been taken to enhance aviation security, and the intelligence services around the world have substantially enhanced their attention and focus on rooting out these plots before they can be consummated. The worldwide installation of reinforced flight deck doors has been recognized as a significant deterrent to further hijacking with the intent to use the aircraft as a weapon of mass destruction.

Richard Reid, the "shoe bomber"; the bombings of the two Russian airliners by Chechnyan rebels; and the thwarted attacks of August 10, 2006, provide ample evidence that our ongoing effort to promote and enhance aviation security must continue unabated. Unfortunately, the debate over how to enhance aviation security has provided more confusion than it has a real improvement in security.

Many billions of US dollars are being spent around the world on aviation security, both for real-time screening and protection of daily operations of the worldwide fleet of commercial airplanes and for research and development into current and new technologies focused on prevention of any more incidents. Within the United States, proposals for aviation security over the past four years, if fully implemented, would have added over US$8 to10 billion in annual security costs to the industry (an industry whose total revenue is around US$135 billion – with annual profits, in a good year, of under US$2 billion). Unfortunately, neither industry nor government has demonstrated the ability to assess the efficacy of any of these proposed measures at reducing the likelihood of another attack on commercial aviation.

Many industry players are leveraging their core competencies to demonstrate how their products or services could be used to enhance aviation security. Estimates of the worldwide business potential for "homeland security" range from US$10B to US$100B annually, although not all of that necessarily focuses on commercial aviation. The marketing of these new capabilities often lean on the "fear" factor induced by the images of 9/11 to make the case for the value of their proposals. After all, no one wants a repeat of those events, right?

The process of determining what technologies do, in fact, enhance aviation security is called "risk management" by many. This process, which is supported by complex math modeling, combined with available intelligence, is used to determine relative values of various counter-measure technologies for enhancing aviation security. To do so requires a consideration of three primary elements: risk, threat, and vulnerability.

Risk is technically evaluated by a statistical analysis of a set of historical events to determine the probability of a future event (e.g., the probability of being hit by lightning represents a quantifiable risk). "Threat" represents the concern associated with the negative consequences of something happening that does not have an analyzable history of occurrence. The threat may be real or imagined and may have a range of probability of occurrence from 0 to 1 (i.e., It will never happen, to It will definitely happen.). "Vulnerability" is defined as a perceived weakness in one's defenses (e.g., An unlocked door is a vulnerability.).

Aviation security can only be enhanced when either the likelihood of a terrorist attack is reduced, or when the impact of a terrorist event can be mitigated.

One must first understand the character of the threat. An analysis of terrorist events around the world reveals that there is no singular characteristic to describe a terrorist, terrorist behavior, or a terrorist threat. The diversity of terrorist threats requires that we distinguish between the various types of terrorist threats. At one extreme lies what is commonly called "state-supported terrorism." Al Qaeda is one of several extremist organizations that would fall into this category. Generally, state-sponsored terrorist organizations have the most resources and are more organized. At the other extreme is the local terrorist cell, not affiliated with any international organization and often motivated by local issues, or merely a group of social misfits intent on fomenting chaos in the society surrounding them—and everything in between. Across all of the different types of terrorists is one common thread—they are focused on causing death, destruction, chaos, and fear within modern society. To be clear, commercial aviation is not the primary target; modern civilization as we know it is the target. Commercial aviation is merely a very high visibility industry that makes it a very visible target for fomenting fear and chaos.

(continued on page 42)

Second, one must understand and embrace the strategy of protecting modern society and, more specifically, commercial aviation from the threats of terrorism. The strategy of countering terrorism, as espoused by the United States Department of Homeland Security and supported by most governments around the world, is one of providing a multilayer defense against terrorists and terrorism. This multilayer approach does not just focus on physically defending the aviation system. It is focused on all aspects of the threat and all of the stages necessary in the development of a terrorist plot. This multilayer approach is focused primarily on the state-sponsored terrorist, the one capable of financing and developing a plot akin to September 11. It also works well against the less capable terrorist cells.

Terrorism experts often describe the terrorist plot development as a series of stages: marking, surveying, planning, testing, execution, or some variety thereof. In the marking stage, the terrorist cell selects a target. In the surveillance step, the terrorist cell learns everything they can about the target and its defenses. Planning focuses on developing the implementation steps and determining the weapon materials and methods of delivery. Testing is used to probe the defenses and determine the optimum attack path to achieve the objective. Finally, execution represents the culmination of the plot. In many cases, the time frame for a plot from marking to execution may be several years.

Immediately after 9/11, most the United States' visible efforts in aviation security were focused on the last two stages, as considerable effort and monies were focused on substantially enhancing the last-stage defenses against a terrorist attack. Development and mandated implementation of the flight deck door and the standup of the Transportation Security Agency's screening corps are two very visible examples of this last-stage defense. While necessary, these steps are not sufficient. Similar to the Maginot Line*, these steps are critical in the prevention of another 9/11 style attack.

But, as was the case with the Maginot Line, the enemy will modify their planning to minimize the defensive value of the action. Many have approached aviation security as we have approached aviation safety. While the intent is the same—minimizing deaths and damages done to the industry and society—the fundamentals are different. Accidents are the result of a set of random events that culminate in an airplane accident or incident. Terrorism is planned by intelligent agents, who constantly adapt their strategy, tactics, and plans, maximizing their likelihood for success in light of their knowledge of the defenses against terrorism. As such, the threat is changing continuously.

The events of August 10, 2006, in London, and the recently foiled plot against JFK's fuel pipeline demonstrate this. The terrorists are continuously changing their targets and tactics. They recognize that attempts at hijacking aircraft for use as weapons is considerably more risky now than it was prior to 9/11. They have done the research and know exactly what our screening technologies can identify, and what they can't. Just like the Germans flanked the Maginot Line, these plots flanked our current in-situ defenses.

Aircraft manufacturers around the world have developed secure cockpit doors.

Fortunately, both plots were foiled while still in the planning and surveillance phases. The foiling of these plots was not just luck. Even when one only has access to the publicly available information about these plots, it is evident that our intelligence organizations around the world have stepped up their activity, their attention, and their cooperation. Foiling these plots in the planning, surveillance, and testing phases is obviously a lot better than depending on our final defense of screening at the airport to capture everything that may try to get through. Both plots were based on attack methodologies and weapons that would not be identified with our last layer of defense, demonstrating the ability of the terrorist cells to adapt to any implemented measures of aviation security. The good news is the plots were foiled. The bad news is that the terrorists are still targeting commercial aviation and dreaming up new and different ways to mount the attack.

So what can the IFE industry do to help in this global war on terrorism? Several providers have offered technologies that enhance onboard monitoring of activities in the aircraft cabin. Others are promoting various types of sensors that can be incorporated into onboard hardware. It is quite likely that almost every product development and business development organization is looking at what it can do to enhance aviation security. The literature is rich with proposals, research initiatives, adaptations of military hardware, and more. Sensors, filters, situational enhancement hardware, biometrics, and surveillance are all rich fields for

**Designed as an elaborate series of defensive and impregnable fortresses, the Maginot Line was constructed by the French prior to World War II but proved to be ineffective and was quickly overrun by German forces.*

(continued on page 44)

business development, and many IFE vendors have technologies that are adaptable to the war on terror. With the identified market for Homeland Security products and services estimated to be in the tens of billions of dollars annually, this is not a surprise. This is free enterprise at its best.

But this represents only the tip of the iceberg above the surface. It is glamorous, and in many cases it is where the money is. But IFE's contribution to the war on terror needs to go much further. As is the case with many players in the industry, this focus on product results is a far more insidious threat to commercial aviation than one might surmise. When this author was deeply engaged with the IFE industry 15 years ago, a debate was raging as to the safety risks associated with IFE. Unfortunately, a large passenger airplane equipped with an IFE system installed after initial delivery was subsequently lost, and the investigating agency concluded that IFE wiring was involved in the arcing that initiated the event. The IFE industry is in a similar situation today when it comes to the war on terrorism. One must ask whether or not IFE can be used by terrorists as part of their attack method. Unfortunately, this author, after only minimal contemplation, can identify multiple ways of using the onboard systems to aid and abet a terrorist attack (for security reasons, these methods will not be described here).

The industry lost that MD-11 because insufficient attention was paid to fault analysis at the time of integration design. What happens when we mix into this environment people who have intent to do harm, people who are well educated, people who are well financed, people who have it in for modern civilization? This possibility makes it an imperative that we all ensure that our systems and products do not introduce vulnerabilities that can be exploited by the terrorist.

While many terrorist acts are poorly planned, poorly organized, or poorly resourced, the organized terrorist organizations have demonstrated an ability to mastermind and implement sophisticated attacks on their enemies, demonstrating a strong

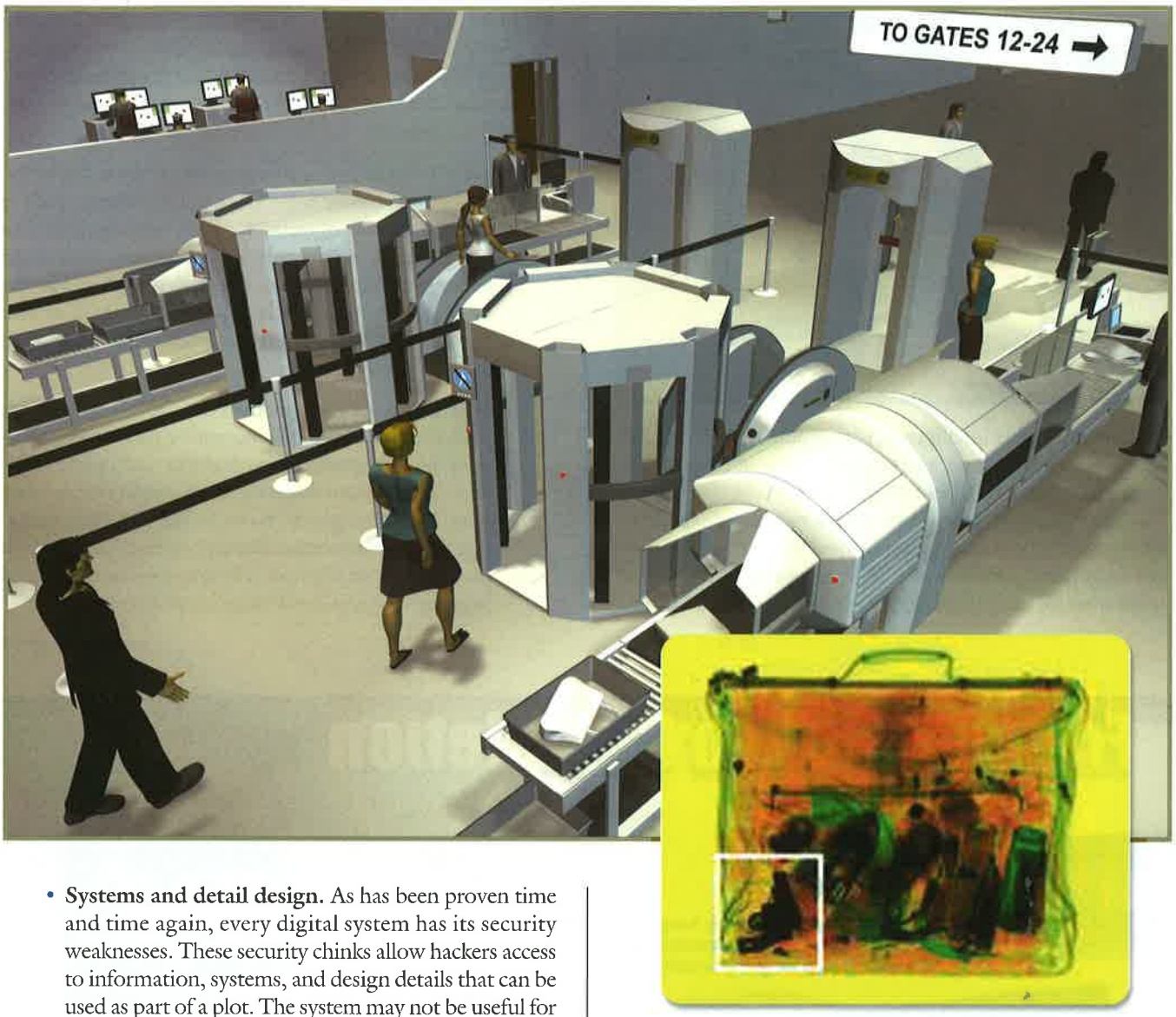
capability to gather intelligence, recruit, and train the suicide bombers, develop plans, and take advantage of our vulnerabilities to orchestrate devastating attacks.

So what can we do to counter this continuing threat? Each and every one of us may be confronted with an opportunity to actively participate in this war. Who among us hasn't thought about what we would have done if we had been aboard United Flight 93 on that fateful day when a few passengers thwarted the fourth of the 9/11 hijackings, giving their lives as heroes. But there are many more ways we may find ourselves involved. To that end, here are ways that you may become involved, perhaps unwittingly.

- **New technologies to support aviation security.** Technology can be helpful, but unfortunately, much of the recently touted technology has not contributed to risk reduction. As an example, what good is a biohazard sensor on an airplane, when it takes days to assess whether or not a collected material represents a hazard or not. Before one promotes a technology, the benefit needs to be identified clearly.
- **Discussions of your product or job.** It is well known that considerable intelligence can be gathered through attending symposiums, conferences, and public meetings. Be suspicious when someone you don't know asks questions that seem to be more detailed them necessary for the conversation. Bits and pieces of conversation picked up from multiple conversations can be pieced together to gain considerable inside knowledge.

(continued on page 46)

Airport checkpoints of the future will continue to focus on secutity enhancements.



- **Systems and detail design.** As has been proven time and time again, every digital system has its security weaknesses. These security chinks allow hackers access to information, systems, and design details that can be used as part of a plot. The system may not be useful for bringing an airplane down, but it may provide enough information to allow a terrorist to get into somewhere they shouldn't, either physically or virtually. Everyone involved in the design process should continuously be reviewing their work to make sure no inadvertent vulnerabilities are being built into the system.
- **Logistics and processes.** As our primary frontline defenses get better and better, the terrorists become more nefarious in their methods of penetrating our security. This can include the use of false IDs, getting jobs on the inside, and other criminal-like behavior that often goes unnoticed. Deep and regular vetting of all employees through the use of criminal records checks and background checks should be the norm for all employees having access to systems, software, or aircraft.

Again, review should be done to ensure that vulnerabilities are not being created as we design and improve logistics and processes

- **Abnormal Behavior.** Over the past several years, several terrorist plots have been identified by individuals reporting abnormal behavior to the authorities. While the debate rages on racial profiling, there is no debate about focusing on abnormal behaviors. This is perhaps the most critical of all. Most nonmilitary people, not living in or near a war zone, usually dismiss strange behavior. It is no longer okay to watch someone's luggage for them. Someone traveling on a two-week vacation without luggage should ring alarm bells. A stranger taking pictures of nontourist sites should trigger our curiosity.

(continued on page 48)

The commercial aviation industry has been fortunate since 9/11. We cannot let our vigilance down however. Several recent terrorist plots have been thwarted because individuals observed something strange and reported it to the authorities. These successes can only continue if this vigilance is maintained and enhanced. This vigilance must be focused on our work and on our surroundings, as this is where the war is being fought.

Author Robert M. "Bob" Peterson resides in Newcastle, Washington, and currently serves as Chief Architect and Lead Analyst for the United States Commercial Aviation Partnership (USCAP), a government industry partnership focused on ensuring cost-effective aviation security for Boeing. He holds BS and MS degrees in aeronautical engineering from the Massachusetts Institute of Technology and joined Boeing in September 1973, entering the marketing organization for commercial airplanes. His background includes fleet planning systems development, traffic forecasting, airline analysis, and product strategy before becoming Director of Computing for Commercial Airplane Group Executive Offices. He also performed the duties of Director-Airplane Economics and Director-Air Transport Industry Strategy. Bob left the marketing organization to lead the development of the Boeing Commercial Air Group strategy for dealing with inflight entertainment, and then led the implementation effort for that strategy. Bob's contributions to the IFE industry are recognized by many as being strategic to understanding the dynamics of an industry that combines airlines, airplane manufacturers, electronics, and entertainment. He then moved to the Spares organization as Director-Spares Technical Publications. Bob returned to marketing, working in the European Airline Analysis Group before taking on a previous assignment as DirectorMarket Requirements-New Airplane working on the Sonic Cruiser. He received his current appointment in March 2003. During the past four years, Bob has led an industry group focused on assessing the cost- effective use of technology in the advancement of aviation security. The analytical methods developed by Bob and his team have received international acclaim for high quality policy analysis, and the economic assessments provided by the USCAP team are now used by the US Department of Homeland Security and Transportation Security Administration as they evaluate changes in US security policy. Bob was named a Technical Fellow at Boeing in November 2006 in recognition of this industry-leading effort. The views he expresses are his own.