

## Enhancing Passenger Screening through Collaborative Intelligence

The basic flaw I see with today's screening system is that we are looking for bad things instead of bad people. Our focus is on innate items, which in and of themselves are not likely to pose a threat to airliners. The terrorists of 9/11 did not carry any banned items on their flights. In fact the only illegal thing they carried was the intent to do grave bodily harm.

Our reaction in the aftermath of 9/11 was to immediately ban all manner of sharp instruments and to begin an ever changing and escalating prohibition of various items from passengers. In order to attempt to keep the newly banned items from the sterile airside of airports many new workarounds had to be invented to keep airport vendors functioning. One of the best ones I saw was a sandwich shop in the concourse; they had a knife chained to the cutting block so that they could cut up sandwiches after making them. Needless to say, this was promptly determined to be unsatisfactory by the fledgling TSA and removed.

Next came **Richard Reed** and his shoe bombs and we all were required to remove our shoes for separate screening. This gave rise to the never-ending stream of jokes about how glad we were that he had not had an underwear bomb. Do you suppose our adversaries watch Jay Leno? Did they then start working on the Christmas 2009 underwear bomb attempt?

The summer of 2006 the liquid explosive bomb plot that was interdicted in the UK gave us another whole list of prohibited items: liquids, gels, and sprays.

Going back and looking at these incidents raises the question of how did we miss the connections between all the indicators and warnings, which in hindsight seem quite clear.

If I were restructuring the passenger screening system it would become an intelligence-based technology-supported operation. For the intelligence aspect is the all-powerful concept of information sharing. In a crisis, information will not spontaneously flow across systems as needed unless organizations plan ahead and create actionable information sharing procedures. We must alter the old intelligence adage of need-to-know to need-to-share, all involved must be held accountable for enabling their sharing.

Intelligence based, by definition entails a great deal of human-in-the-loop interaction. HITL requires the participation of the entire aviation and government enterprise, as every stakeholder has a requirement and a vested interest in being an active participant. Secretary Napolitano in meeting with the International Air Transport Association – IATA- in Geneva last January demonstrated a clear new initiative to establish a joint public-private relationship to share operational experience, passenger data, and harmonize policies and procedures for cross border air travel. The IATA Director General summarized it in his remarks by saying:

*I think that this new administration has brought a sea change to aviation security by proactively engaging the industry to combine government*

*intelligence with airline operational expertise. This is the way forward in which we will be able to battle and win the battle against terrorists in aviation.*

To gain on this initiative I would design an information-sharing network in which every individual that has contact with a passenger is obliged to note positive or negative security notes on a Wiki based form attached to the travelers PNR – passenger name record. For clarification, I use the term Wiki to describe a web-based collaborative environment allowing with attribution, anyone authorized to, create, contribute, modify, organize or comment upon a given topic, which for this application is the PNR. In the case of **Abdul Mutallab**, the Christmas 2009 bomber, the individual taking the reservation would have had the first opportunity to make an entry on the file associated with his PNR. When he purchased the ticket in Ghana on Dec 16, 2009 paying cash for essentially a one-way ticket, because it originated in Ghana went on to Detroit and ended in Lagos. To everyone in the developed world airline business, cash one-way became a flag for potential problems back in the 1970's rash of highjackings. But we must recognize the cultural differences in African air travel where cash is not an unusual and indeed more the norm in making purchases of this sort. Nonetheless, in harmonizing procedures across the global industry, ticketing & reservation personnel would be educated to highlight this fact and other indicators & warnings at the time they took place. This becomes the starting point of a Wikirecord associated with a PNR, which becomes available to everyone who interacts with the traveler.

This newly created data rich information is continuously made available to the intelligence professionals at TSA for their evaluation and sharing. Utilizing newly focused computer algorithms to continuously scan all the travel data and Wiki pages associated with it, looking for potential anomalies or increasing threat factors from other seemingly unrelated sources, creates a threat index associated with any given individual, flight, or airport.

The Wikirecord remains active until such time as the traveler has completed their journeys or in cases of regular travelers or heightened threat indices associated with an individual, the record remains operative for longer periods. The Wikirecord and PNR is constantly machine reviewed by the TSA and NCTC- the National Counter-Terrorism Center as they administer the watchlists and monitor other external threats and vulnerabilities.

Cash, one way, does not in itself create a great risk, rather it begins the compilation of a threat index. This may only generate the lowest level on the index scale. However, by utilizing the massive computing power of the US government the threat indices of all travelers are correlated to establish a visualization of the overall risk picture. A couple of disassociated low level threat indices on a particular flight may not be determined to be a great hazard until they build to a critical mass.

Now think back to 9/11, had we a system that reviewed Wikirecords for all travelers that day might we have seen; similar people with similar tickets, similar seating locations, purchased through similar means boarding 4 flights

at similar times? With the benefit of hindsight could we fine tune the analysis to factor in other seemingly non associated facts, like the relative passenger loads of the flights or the number of reservations for those flights which no-showed their ticketing and check-in; and a host of other data so disparate that only a robust computer system will discover a remarkable alignment of similarities.

This system has the potential to move from a data-poor to a data-rich environment generating a newly refined threat index for a given individual, flight or airport. **Abdul Mutallab** changed planes in Amsterdam, might he have had contact with support team members in the transit lounge, could they have independently brought portions of his device and passed them along within the sterile environment? We may therefore wish to extend the computer search to include nodes where certain threat indices intersect.

On creating the threat index, part of the concept is that through the use of Wiki, individuals are free to put up their thoughts and perceptions on a topic, this is then open for others to refine, correct or elaborate upon.

Over a 27-year career flying for a major US airline I was often amazed at the level of intuitive understanding of human behavior patterns possessed by the experienced gate agents and flight attendants. These folks with years of public contact experience would very often be able to see problems or difficulties long before they had a chance to manifest themselves. A flight attendant would turn to me during a boarding process pointing out an

individual that would later be an issue. Sure enough during the flight I would get the call, "remember the guy I told you about, well he is now a problem". There is great value in sharing the operational expertise of our professional employees. The Wiki tool gives these people the ability to input and review others input. It allows the intelligence professionals and the computer systems to translate and leverage the combined wisdom of mass collaboration to create the threat index. Of course there must be partitions within the records as everyone does not have a need-to-know and many facts are confidential.

The tremendous potential of the DHS / IATA meeting is that IATA represents 230 airlines – the vast majority of all air carriers around the world. IATA is the clearinghouse for essentially all air tickets and until eTickets became operational they were organization that produced and controlled ticket stock used by airlines and travel agents worldwide. This ticket stock was a financial instrument, printed and controlled much as treasury departments manage currency. The result of this is that IATA has a fantastic database of information on travelers, method of payment, travel itineraries and some very sensitive data. Founded in 1945 - on principles including- *promoting safe secure air travel for the benefit of the world's consumers* – IATA is the epitome of discretion and security when it comes to the data they hold sacred. It is a very significant step forward to see this level of public-private cooperation taking place.

What we do with our newly conceived Wiki data package is as important as the process, which created it. A large expense will be incurred up to this point and it needs to be acted upon. Within this new system of intelligence-based technology-supported screening, I would add a simple barcode reader combined with video facial capture function for every passenger when they pass through identity verification or passport control. This is for a dual purpose, one to determine and maintain a record of where and when an individual entered the secure active traveler environment and secondly as the time to initiate actions based on the entire data evaluation process associated with that person up to that point.

Now, in order to gain on the cost benefit equation for these increased procedures I would deconstruct our current checkpoint into three separate lanes: A, B, and C. Where Lane A is the line for people about whom we have a great deal of favorable information. For instance US persons holding US security clearances, or frequent flyers with long established and validated identities. For these people the screening process could be expedited to exclude the need to remove shoes and jackets, computers, and small liquid containers from bags, thus increasing the throughput for this group.

Lane B would be the standard, which we have today and would apply to all those folks at or below some level on the threat index or infrequent flyers about whom there is a small body of information and lesser reason to suspect a risk.

Lane C now becomes the potentially more intrusive and thorough procedure. At this point the Wikirecord is humanly reviewed, behavior detection officers are actively engaged with the traveler, full body imaging is the norm and various other procedures applied on an as required basis.

Through the process of identity check, scanning the boarding pass, and real-time video image capture at the start of the screening protocol; travelers are segregated- either electronically or by the TSOs determination- into the various lanes. This also creates a positive record of the fact of where and when they entered the active traveler secure environment. Under today's procedures a traveler may check-in online, print a boarding pass from a remote location up to 24 hours before a flight and there is currently no means to positively identify when or where they enter the sterile environment through screening.

Had a barcode reader, facial video capture in conjunction with identity check been in effect May 2010 when **Faisal Shahzad** attempted his Times Square bombing, it could have been quickly used to narrow the search area for him. The media was quick to criticize the airlines for not having a method of checking the watchlist within two hours of his flight departure, when in point of fact, **Faisal Shahzad** could conceivably have checked-in and entered screening at JFK early Monday morning of May 3 or even late the evening before. He was not captured onboard his flight until Monday evening. With a positive identity check and a real-time picture a simple computer search would determine whether he had entered the active traveler secure

environment. If needed that current image would be transmittable to authorities in the airport facilitating his apprehension. In a more technologically effective procedure the image could be quickly uploaded to a facial recognition surveillance system if such was operable within the airport. Or as Commissioner Ray Kelly said last Thursday, 24 June, NYPD has launched its ambitious plan for a network of surveillance cameras to combat terrorism and detect suspicious behavior in lower and Midtown Manhattan. Certainly this new system, as an integral part- will have state-of-the-practice facial recognition applications.

A major step in the new paradigm of passenger screening was announced last Thursday, 24 June by the TSA:

*Secretary Napolitano announced that 100 percent of passengers flying domestically and internationally on U.S. airlines are now being checked against government watchlists through the Transportation Security Administration (TSA) Secure Flight program, the second major step in fulfilling a key 9/11 Commission recommendation achieved this month.*

This is a significant step forward in taking the cost and responsibility off the shoulders of industry and it greatly facilitates the connectivity of identity matching into the system I advocate.

Additionally, there are other criminal watchlists and activities where having a good facial recognition video picture tied to an positive identity check would

be a value added; of course there are privacy concerns and regulations, which need to be addressed and compliance issues met.

Now suppose we have this threat index system and the sorting process at screening taking place; travelers are still free to check-in and enter the active traveler phase many hours early and spend up to several days within the system on complicated and/or delayed long journeys. The threat index procedure is a continuing living process always updating itself through human and machine evaluation. I would expect, as in the case of the Times Square bomber, developing intelligence quickly changes the threat index of a given traveler or a combination of travelers raises the threat index of a particular flight or airport. At this point agents may be dispatched within the airport to either apprehend or require certain travelers be returned to lane C for a thorough screening and evaluation. As it is certainly possible to miss threatening travelers within any system, an entire flight manifest of travelers could be re-screened at a pre-determined threat level.

As I mentioned this threat indexing of traveler, flight or airport is a living process. Had the watchlist evaluation on **Abdul Mutallab** been accomplished after he had departed Ghana the threat index would have greatly increased, this data with picture attached could have been quickly passed to the airlines and authorities in Amsterdam where they could have applied appropriate screening measures.

Secretary Napolitano and IATA have started a grand quest to build information sharing across international and corporate borders. From IATA's public testimony last March before the House Homeland Security Committee:

*IATA believes that the key to this future (passenger screening) is leveraging all of the passenger information currently collected by a government before the start of the trip. Data collected in the name of customs and immigration needs to be merged with that collected for security. Then it should be analyzed by government intelligence agencies before a "cleared to board" decision is issued. The general results of this vetting would be made known to the screener at the checkpoint who would decide if a more thorough physical search is warranted. This process combined with advanced behavior detection would make for a stronger and more efficient checkpoint.*

True public – private partnerships are the mainstays for creating a holistic AvSec system; 85% of all critical infrastructures are in the private sector, likewise much of the critical data is held by the private sector. We must learn to share access to this data while maintaining the privacy and discretion demanded by our worldwide stakeholders. To this final end I make yet again an endorsement for establishing at least within the US, a functioning Sector Coordinating Council or ISAC- information sharing and analysis center- including our stakeholders and acting as an honest broker to manage the public-private interface.

Breaking development. Saturday morning 26 June, Dr Tom Cellucci, First Chief Commercialization Officer, DHS announced that the department just released the 7th book on innovative public-private partnerships; it will be posted on various pages on [www.dhs.gov](http://www.dhs.gov) in the next two weeks. Perhaps there are grounds for true collaboration on the horizon.

Finally, we often hear that in meeting the terrorist threat we need to be right 100% of the time while they must only be right once. Yes and no. Aviation security is a system of systems; layers built one upon the other and the terrorist has to be right time after time in order to navigate through these complex layers we have built. The architecture of intelligence-based technology-supported screening is one, which is constantly growing and maturing. No single piece of fancy high tech gear is going to be the grand answer or solution. As new technology comes along it is plugged into the system until the next best invention is available. Likewise the human side of the process is an ever-evolving professional endeavor. Every person with access to the traveler Wiki-record has an obligation to constructively add to the overall body of knowledge. Some people like to say that we are looking for a needle in a haystack when referring to the potential terrorists in our midst. More accurately I submit ... we are looking for a needle in a needle stack, a pile where there is great deal of similarity with just the slightest indicators & warnings of who needs closer examination.

Working together in collaboration is the key to protecting the aviation industry and indeed our nation.