Case study

John W. Halinski, Former Deputy Administrator/Deputy Assistant Secretary, Transportation Security Administration

In the period leading up to the Christmas Day 2009 Underwear Bombing attempt, the Transportation Security Administration (TSA) was following multiple threat streams focused on aviation. The majority of these involved the terrorist group Al Qaeda in the Arabian Peninsula (AQAP), who had been fixated with attacking the commercial aviation sector. AQAP was emboldened by the significance of the attacks of 9/11, and thus believed that continued attacks in this domain would significantly terrorize the West by causing significant loss of life and serious economic damage.

The TSA is a component of the Department of Homeland Security, and thus is the Federal entity charged with protecting the transportation sector of the United States. On any given day, the TSA screens almost 2 million people, thousands of tons of cargo, and more than 5 million bags. This system is one part of many layers of security, both seen and unseen, for the travelling public. To accomplish its mission, TSA must coordinate with a multitude of federal, state, and local agencies, in addition to foreign nations and regulatory bodies, on a daily basis.

There are over 280 foreign airports that provide direct service to the United States from around the world. TSA does not provide screening in those locations, but they still must ensure that each access point upholds the standards that permit them to provide direct service to the United States. Recognizing that the primary threat from AQAP would most likely emanate from outside the United States, the TSA has worked continually with foreign nations to upgrade their security capabilities.

In the summer of 2009, the TSA held a series of tabletop exercises discussing a number of threat streams and scenarios to ensure that the essential requirements of a validated crisis response could be put into place quickly. They conducted these exercises with other agencies, most notably the Federal Aviation Administration (FAA), and many included terrorism scenarios with three goals: first, determining when it would be necessary for the TSA and FAA to conduct a “ground stop” of all aircraft; second, what the process would be to reinitiate service based on threat conditions; and third, increasing recognition for communications capability and how to handle a worldwide threat, simultaneously.

On Christmas Day 2009, a would-be suicide bomber named Umar Farouk Abdulmutallab boarded an aircraft in Amsterdam bound for Detroit. He used a completely non-metallic explosive device which he had placed within his underwear (AQAP had conducted enough research, simulations training, and their own brand of due diligence to understand that a walk-through metal detector would not detect the device, as well as understanding the cultural constraints which would preclude truly invasive screening and profiling). He attempted to detonate the explosive once the aircraft commenced the final approach into the Detroit airport, but the trigger mechanism failed, and he was subdued by passengers on the flight. Initial reports by the media reported there were fireworks used on the flight by an unruly passenger, but after a preliminary assessment by law enforcement, TSA understood they were facing a different type of threat and therefore must react quickly to mitigate any other attempts which might be underway, both domestically as well as at any of the other approximately 280 embarkation routes.

Based on lessons learned from previous training exercises and simulations, TSA set up a crisis incident management group. This group acted immediately to ground all remaining flights from Europe, Africa, and the Middle East until further screening could be accomplished, as well as setting in motion a mitigation plan and accompanying communication plan focusing on audiences throughout the rest of the world.

The mitigation plan called for immediate full-body screens of all passengers boarding U.S.-bound flights lasting for a 72-hour period. Detailed information was also provided to airlines on certain procedures that would have to be taken for aircraft already airborne. TSA further recognized that due to the holiday period, this mitigation would have a significant impact on flight delays and operations. Knowing that these measures could only be sustained for a short duration, they developed a different mitigation strategy for this type of threat after the initial 72-hour period had expired. Finally, TSA ensured that other countries were all following these new procedures and adhering to the standards set forth.

As a result of this incident, TSA significantly changed their approach to identify "clean skin" threats, while also developing the "body scanner" X-ray technology now in use at all major U.S. airports. There were many lessons learned from this event, particularly in how to mitigate the threat; however, perhaps the most important was TSA's understanding that the successful response and recovery once the event occurred was directly proportional to the amount of time and effort given to rigorous planning and rehearsal exercises beforehand, all designed to help develop awareness and capabilities to prosecute the crisis incident effectively.

Relation to war gaming

As mentioned, TSA held a series of tabletop exercises and war games months before the events of Christmas Day 2009. As a result of these exercises, TSA recognized it had to coordinate better with other government agencies, particularly the FAA. TSA also learned that to react quickly in a crisis, they needed to develop a "ready-to-issue" series of regulations to mitigate a specific threat. TSA developed a template for these type of events that could be put into place within hours. The exercises and war gaming also identified the need to have a very thorough communications plan in place around the world. Key contacts and stakeholders needed to be identified, messaging needed to be standardized, and TSA personnel needed to be able to respond quickly to all 280+ airports that flew directly to the U.S.

> "Nothing is more effective for a leader and their organization than experiencing the reality of making difficult decisions and building cohesion and team unity. War gaming provides this opportunity, but does so in a cost effective way and in the relatively safe environment of a simulation"
>
> John Halinski
> Former Deputy Administrator,
> Transportation Security Administration

While the events of Christmas Day 2009 identified shortfalls in the aviation security system identifying a new threat, the reaction and quick mitigation of this threat can be attributed directly to prior planning and exercises which identified capability gaps and holes in the system. These vulnerabilities were corrected shortly after the series of simulations, and as a direct result, no aircraft was grounded for more than two hours. While initial mitigation measures were intense and not passenger friendly, they ***were*** put into place quickly, effectively neutralizing any additional threats. Information and intelligence was sent worldwide within a six-hour period, and no other threats were identified during this timeframe. If TSA had not been dedicated to the intellectual rigor of prior war gaming and tabletop exercises, the response time to this event could have been much longer and significantly more costly.

War gaming, as a specific tool and discipline, can greatly enhance the value of existing analysis. By creating immersive scenarios with dynamic and free-thinking adversaries with capabilities greater than prevailing biases and assumptions allow, organizations are forced to confront undesirable and unintended consequences, yielding insights that enable better preparation and anticipation of future crises and risks. As such, conducting war games as an integral part of the planning cycle can bring value to any decision maker planning to allocate large resources to a fixed and strategically vital piece of infrastructure, be they government buildings, corporate headquarters, energy pipelines or grids, or other similar high-cost, high-vulnerability projects.