

ADSA25: What Did We Hear and Not Hear?

Harry Martz, Lawrence Livermore National Laboratory

Carl Crawford, Csuptwo

May 4, 2022

What Did We Hear?

- Surface transportation is everything, including pipelines, besides aviation
- SENTRY should help with data fusion and analysis of data acquired by RCA
- RCA has identified several capability gaps, several documents available to the public
- ‘Security is always a balance...’
- DHS S&T, Innovation task force and TSA are developing applicable technologies
- Protective service providers
- Evolving nature of the threat, e.g., drones, melees
- It is not realistic to completely solve the problem, but it is realistic to mitigate and minimize the problem (death and injuries)
- Mass shootings (4 or more deaths) doubled from 2002 to 2021 3 to 6/year
- Mass shooting more for personal reasons vs. terrorism

What Did We Hear?

- The words of Public officials are more powerful than one thinks
- Safe and secure school is required to be able to educate
- Learned a lot by identifying predictive behavior, deal with it immediately/early, adult human bodies are essential, improve school pride, used a metal detector for one day, does may not work at a school
- Balancing welcoming attitudes with security realities; lots of training, community force multipliers; balance security, cost & openness
- Part of protecting soft targets is not stopping the perpetrator but making people feel safer
- Soft targets should not become hard targets
- What is the net security benefit?
- Unintended and intended consequences

What Did We Hear?

- Scenarios need realistic war gaming (table-top exercises)
- Humans are the weakest link in security but could be the greatest asset!
- Technology should complement, not replace security manpower
- Fear and liability is a big issue
- Insider threat is a big issue for DoD
- People are more of a deterrence than technology to a criminal
- There is a lot of data out there on what causes a criminal to select their target and why
- False negatives errors increases as targets are rare: low prevalence
- Profiling increases risk; anti-profiling would be better
- We rarely regulate or test system-level performance
- Cumulative screening (all three levels are used for screening regardless of the outcome at each) >2 or more alarm is better than layered system-level performance (If cleared on level one pass level 2 & 3)
- Is big D detection, deterrent or displacement?



What Did We Not Hear?

- How do we bound the space?
- How do we define the threat?
- What is the threat? Has it been quantified?
- How do we generalize good solutions?
- How do we separate the act from the individual?
- How do you handle alarms?
- What do you do if you detect a threat?
- How to identify predictive behavior?
- How best to utilize Protective Service Providers?
- For systems-level cascading what is the cost (\$, throughput, etc.) of each measurements?
- What are models of adaptive adversary decision making and how validated?
- How to use of distributed, empirical, systematic and scalable red teaming (DESSRT) methodology?
- How to connect equipment and people?
- How to know more about surface transportation passengers?
- How to trade off (balance) security and visitor experience?
- How the virtual sentry is applied?

