Summary and Next Steps

ALERT ADSA 19, Northeastern University

October 16-17, 2018

Carl Crawford (Csuptwo),
Suriyun Whitehead (Booz Allen Hamilton,
Larry McMichael (LLNL)

This research was funded by the Science & Technology Directorate of the Department of Homeland Security

LLNL-PRES-760759

This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under contract DE-AC52-07NA27344. Lawrence Livermore National Security, LLC

Lawrence Livermore National Laboratory

Nondestructive Characterization Institute

Livermore Explosives Detection Program LEDP

Summary and Next Steps

Carl Crawford, Suriyun Whitehead and Larry McMichael

ADSA 19 October 16-17, 2018

Was ADSA19 Successful?

- It depends on the metrics you choose, examples include
  - Audience learning about where TSA is headed
  - TSA learning about new technologies/capabilities
  - Number of
    - Attendees
    - Forming partnerships
    - Developed products
    - People working together
    - Enabled DHS sponsorship
  - Increase of stakeholders' participation
  - Spin off of other ADSAs
  - Number of side bar conversations

What Did We Hear?

- Overview:
  - ADSA will continue, program may evolve
  - Expectation of outreach, programmatic impact through interactions between the whole community
    - COE success stories depend upon technology transfer to fielded capability (e.g., CMU voice recognition tool barrier to widespread use within Coast Guard)
  - Transition of technology versus product capability
  - Avoid need to shutdown airports when a new threat emerges
  - Is TSA creating the impression for the public and Congress that their equipment is perfect versus effective?
  - Rapid response capability requires preparation and commitment – a new ecosystem required

What Did We Hear?

- DHS/TSA Perspectives
  - Research investments should have a transition plan for deployment at the onset
  - Threats adapt versus go away
  - Better security, faster – does it mean better detection, faster operations, networked equipment, all of it – you can only go fast when grabbing low hanging fruit
    - Can't wait for perfect system to deploy, must adapt in the field
    - Leveraging TSA's existing authorities to respond quicker (e.g., Innovation Taskforce, Automated Screening Lanes, accept donated technology)
    - AIT without divestment – Enhanced technology deployed for Pre Check program
  - Checkpoint CT deployment
    - Limited deployment show encouraging results, throughput remains a challenge
  - Is TSA overly optimistic for Checkpoint CT? Overly focused on CT due to political pressure?

What Did We Hear?

- DHS/TSA Perspectives
  - Adversaries are becoming more strategic, testing boundaries
  - Use of ML for prohibited items to reduce cognitive load on TSOs
    - Potential first application of “algorithm certification”
    - How to avoid “garbage in, gospel out” – how much data is adequate to enable accurate generalization of ML algorithms
  - Do all prohibited items pose the same level of risk? Subset to be incorporated into the PI detection standard.
  - Future Lane Experience (FLEx) based on risk mitigation where least information is available, Passenger Risk Differentiation, adjustable algorithms – initially by lanes, future by dynamic equipment

What did we hear?

- DHS/TSA Perspectives
  - Air cargo is going to 100% screening
    - Integration of air cargo screening with existing technology, pushing capability to offsite, non-federally staffed facilities; 500K ceiling.
    - Exploring application of x-rays, nuclear quadrupole resonance, fused imaging for air cargo
  - Any loss of life is a terrorist attack? How do you quantify the minimum threat that you protect against – individual, small group, a full aircraft?
  - At what point is an image too complicated for a person to decipher versus send directly to secondary inspection – developing OCAS, OCAST

What did we hear?

- DOD Perspective
  - Are we looking at a problem the same way every time and missing what the opportunities are
  - When requirements are set, that is what will be built – do they incorporate your future needs?
  - Collaboration with end user to develop a better product
  - Soft target protection: layered, covert at perimeter, overt at chokepoint
  - Advocation of communication with public – make the wait worth it

- Advanced Technology – Transitioning Technology
  - Need for balance between long-term development versus short-term impact when evaluating transition

What did we hear?

- Advanced Technology – Use of simulation
  - Drive concurrent hardware design to minimize time to market (eliminate nonviable configurations)
  - Application of rapid design and prototyping algorithms to develop hardware and achieve better performance and cost optimization
    - Toolkit available for simulating photon counting detectors, working on pulse pileup effect

- Advanced Technology – Emerging capabilities
  - Video analytics
  - Standoff trace chemical detection as a collaboration between academia and industry
  - Prototype deployment of mass spectrometry system
  - Commodity WiFi hardware
  - Are different metrics needed to evaluate algorithms – volume basis vs overlap (segmentation)
  - Hyperspectral CT as an alternative to dual-energy CT
  - Biometrics coupled with ML (e.g., facial recognition)
  - Distributed sensors for monitoring airport environment (early detection)

What did we hear?

- Advanced Technology – Application of ML/DL
  - How will it perform outside of visual identification tasks?
    - E.g., promise with metal artifact reduction in reconstructed images
  - Use of synthesized data to address imbalanced data sets for low probability events and impact on data availability, generalization on ML algorithms
  - Synthesized data set generation complicated by nonlinearities in x-ray physics
  - Use synthetic data to evaluate how well ML/DL generalize by introducing feature variations
- Advanced Technology – Use of open architectures
  - Driven by government requirements
  - Proprietary formats lead to a fragmented solution space which impedes sharing information between systems/equipment
  - DICOS v2A: multi-energy, multi-view, hope for beta version in early 2019, maintenance contract for toolkit in place
  - Integrated airport information system via OTAP
  - Means of deploying innovations from crowd-sourcing

What did we hear?

- Perspectives: Airports and Humans (cont)
  - How to recognize and deter terrorists (other violent actors) – what to look for
    - Terrorists more likely to surveille targets than mass shooters
    - How can we monitor and detect risk factors? Legal limitations? Return of Behavioral Detection Officers?
    - No predictive models, only indicators for people that are susceptible to recruitment
    - Radicalization is a process
  - Need to redefine what the checkpoint looks like, from a customer, airport, and security perspective – invisible processes that extend screening beyond a set checkpoint
  - Human factors affect engagement versus complacency; need to balance the cognitive load on TSOs as we introduce new technologies and automation (aptitude alignment)
  - TSOs should provide feedback to passengers on why their baggage triggers a false alarm and how to avoid it, so long as it doesn't reveal system capability – what guidance do TSOs get or need to provide appropriate feedback?

What did we hear?

- Threat Characterization
  - Learning from the past to identify patterns for terrorist activity – similar methodologies across centuries, means evolved
  - Tendency to use materials that are readily available
  - Why aren't suicide bombers (more) active domestically? – mass shootings are easier, other means allow the terrorist to see the effects, control
  - LENGTHY process for addressing an emerging threat
  - What are the practical differences between simulants and material of interest for a particular modality? Is it good enough for a simulant to match the x-ray physics and to what extent is that necessary?
- Adaptive technology: Incorporation of meta data to adjust system parameters for local conditions that could affect performance

What did we hear?

- Kaggle Competition
  - Complementary approach to traditional R&D investments to create outreach to non-traditional performers (attract new sources of talent to the problem domain)
  - Augmented images will often lead to training on the mutation – simple overlay doesn't work, have to account for the inherent nonlinearities (physics matter)
  - Winner exploited data groupings (artifacts) intentionally, but others who avoided grouping data did well too
  - Implications on data collection to generalize algorithms to production environment

What we did not hear?

- Are we adapting fast enough? Lots of discussion on what current processes are, but little on how we can adapt those processes to make them faster
- How do we avoid reliance on luck for having new equipment or protocols on hand?
- Is displacement TSA's problem?
  - Should that be someone else's problem?
  - Have airline passengers bought into the risk?
- What happens to risk based screening when someone goes through the Pre Check lane and brings down an aircraft?
- Additional outreach is great, but what happens when all the low hanging fruit from other fields has been plucked?
- The level of discussion has waned compared to early workshops – how do we recover it as the workshop grows?
- What are the airlines role in security? Have they been too removed from the process? (push from LaGuardia, Atlanta to be more integrated… speed vs security)
- How do you certify equipment & algorithms for different levels of differentiation? Sliding ROC curves? Multiplicative factor for hardware and software changes.
- How does testing adapt when a host of third party algorithms are submitted?
- What is the incentive framework for third parties to participate?

ADSA20 – May 7-8, 2019

- The design, development, testing, deployment, and operation of *effective* systems
  - Defining *effective*
  - Human in the loop – use of simulants
  - Statistical significance of tests and influence of limited training data
  - Positive predictive value improvement
  - Detection vs deterrence vs displacement
  - Reducing time to market
  - Role of interconnectivity with open architectures
  - Is 30/1 (PD/PFA) better than (80/30)?
  - How to specify effective systems
  - Application of metadata
  - Rapid response to an adapting adversary
  - How do we drop a threat to the list
  - Dealing with imperfect equipment
  - Transition – particularly from academia
  - Effectiveness for other stakeholders: airlines and passengers, but also subway, rail, and cargo
  - True vs auto-detect – current supposition that we need imaging to detect
  - Data augmentation
  - Role of third parties