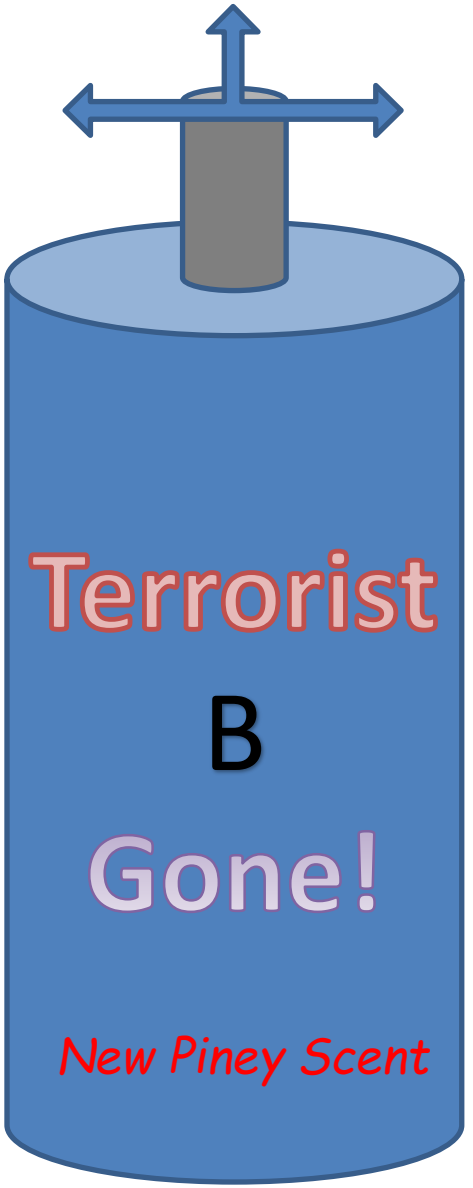
Summary and Next Steps

Carl Crawford, Suriyun Whitehead and Harry Martz

ADSA 21 November 5-6, 2019

98% Gibbon



What did we hear

- How many terrorists have you found?
  - All of them: we have not seen any major terrorist attacks in the aviation sector.
  - Passenger volume increasing, confidence is good?
- Think outside the box and help enable new CONOPS.
  - Airports are capacity controlled
  - Terrorist are adapting so we have to adapt as well
  - Be proactive; new capabilities must be developed before you need it
- Cognitive Load and Human Implications
  - Adopt automation and semi-automation
  - Visual search is a specialized skill
  - Trustworthy operator assist; the future TSO as an analyst
- TSA Administrator Pistole: All your pieces are like swiss cheese, once you layer them, the holes are covered
- What problem to be solved that would drive unlimited funding?
  - A: Its not a technology, its an incident

What did we hear

- Real data is hard to get ahold of
  - Desensitization, proprietary, non-proprietary
  - Validating non-sensitive datasets as analogous
  - Validating simulated datasets
- TSA needs technology innovation
  - Machine learning is promising but fragile
  - Evolution in components, devices, integration, open architecture, 3rd party algorithms
- Deterrence, prevalence and displacement
  - Target rich environment; protect the targets we care about the most
  - We need to thwart attacks to avoid complacency
- Disseminate or censor terrorist propaganda?
  - crowdsourcing, public awareness, both good and bad
  - brings fringe ideologies into the public sphere, fame, recognition, tools and tactics
  - mutually self-reinforcing, accelerant, amplification

What did we not hear?

- PD/PFA of system
- How do you certify 3rd party algorithms, fused systems?
- Who fixes fused hardware, software systems, systems of systems?
- Positive 3rd party-incumbent vendor stories
- Should we stand down and go away?
- Do we have enough security?

ADSA22 – May 6-7, 2020

Possible topics

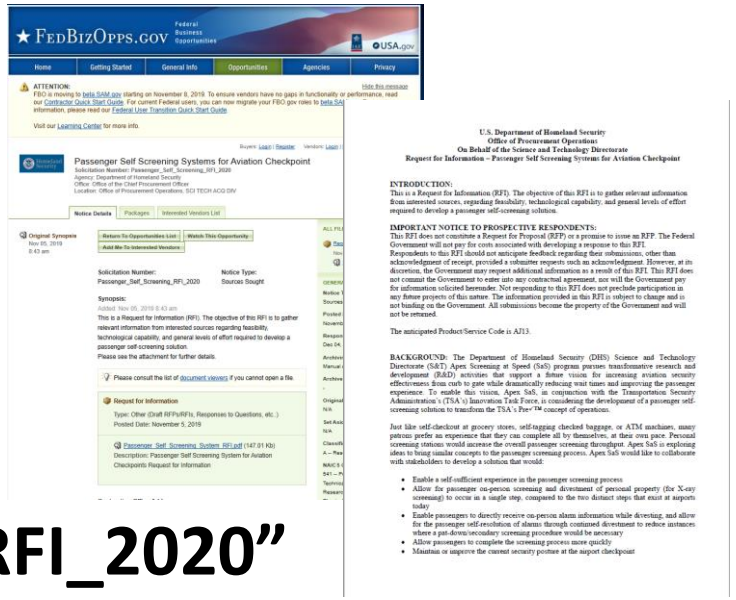
- Reducing cognitive load; “art” vs. technical phrase
- Creation and Validation of simulations/simulated/synthetic/augmented data for Training and Testing
- Physical Simulants
- Displacement
- Insider Threat
- Deeper Dive on Adaptability of ML
- How to improve robustness of the security system
- What TRL should 3rd parties be at…
- Terrorist Be Gone!
  - How do we get rid of terrorist
  - How do we allow passengers to just walk onto the plane?

ADEPT03 - ADSA for Customs and Border Protection (CBP). July 8-9, 2020

- **Theme: Creating Effective Engagements with CBP**

Open DHS RFI

- S&T RFI -- Self Screening Systems for Aviation Checkpoint



FBO.GOV

RFI: Search for
“**Passenger_Self_Screening_RFI_2020”**

“Just like self-checkout at grocery stores, self-tagging checked baggage, or ATM machines, many patrons prefer an experience that they can complete all by themselves, at their own pace.”

Detailed slides follow

What Did We Hear?

- 21 ADSAs so far.
- Talking about [Creating] - System, Integrated, Effective was useful.
- It is a complex multi dimensional space
- Various examples were given
- DHS/TSA Perspectives
  - No shortage of good ideas, but must be acceptable to the public
  - Can not shut the airport down
  - 50% of airports are capacity constrained
    - Push screening out to multimodal entry points, transit station, cruise ship terminal, airport car rental facility
  - Devolution of threat – how to protect against an adversary who will attack anywhere, at anytime?
  - Raise global base of security, international compliance and harmonization
  - If regulatory framework is too difficult, it stymies innovation and deployment
  - How many terrorists have succeeded in attacking aviation?

More DHS/TSA Perspectives

- **Think about the problem you are trying to solve**
  - TSA reorg to capability managers to match this
- **Think like a citizen**
  - Passengers have confidence in the aviation system
- **Environment**
  - Deploy solutions to address devolution of threat
    - Terrorists are planning to attack everywhere
  - Precheck passengers still need to be screened
  - Ecommerce is changing cargo
  - Be effective, efficient to a constrained space
- **Centralized vs. non-centralized screening**
- **Thrusts**
  - Open architecture and integration
  - Cyber security
- **Need**
  - Industry / Government Working Group for validating synthetic data
  - Better colorimetric kits
  - Detect chlorates

What Did We Hear?

- **Creating**
  - Not enough thinking outside the box, beyond the traditional checkpoint.
    - Expanding CONOPS. Future TSO is an analyst.
    - Machines are what they are, throughput is what it is.
    - Intermodal, pushing the checkpoint out
  - Chicken and Egg – delivery 5-10 years out from date of requirements
  - Machine learning approaches, applications and pitfalls
  - Getting the right data, proprietary data sets, challenges
- **Effective**
  - Low tech, low cost solutions
  - Utility of flipping a coin, deterrence and prevalence
  - Red team testing
  - Synthetic data
- **Integrated**
  - Security of systems
  - Public and restricted datasets
  - Open architecture
  - Intel Feedback / Push and Pull
  - Indoor location awareness for Common Operating Picture
- **Investment**
  - TSA funding accelerates projects / IRAD may do it downstream
  - Datasets

What Did We Hear?

- **Technology**
  - **Components**
    - Phase contrast imaging gratings for X-ray detection for checkpoint screening of explosives
    - Fiber-optic based perimeter intrusion detection
    - Low cost tamper evident physical security tags, IDs, print on demand
  - **Systems**
    - Checkpoint CT system
      - For fixed gantry scanner built around carbon nanotube based X-ray source
      - Tube manufacturer partnered with systems developer
    - Checkpoint XRD system
      - Alarm Resolution tool following targeting; does not have built in prescreener.
      - DICOS enabled
      - Under TSL evaluation
    - MultiView CT scanner for Palleted Air Cargo
      - 35 views, 3x3x3mm voxels – worked with ALERT to bring it down to 20s.
      - Potential to move to 2x2x2mm and single digit seconds.
      - GUI from 3rd party (Telesecurity Systems)
      - Test jig and software for IQ evaluation
      - Deployed to JFK
      - TSA did not work to finalize
        - » Final steering, operational guidance and funding by UK-DFT and Israel/El-Al
      - Israelis are sponsoring 3rd party ML detection algorithms
      - Future simplified design funded by S&T to meet cargo industry budgets.

What Did We Hear?

- **TSA reorganization**
  - Capability managers focus on problem areas, vs technology alone
    - Biometrics and Identity Management – partnership with CBP
      - Identification is the problem, using biometrics as one approach
    - Accessible Property Screening
      - Prohibited Item detection with 3rd parties
    - On Person Screening
      - Don't stop people, detect everything, common GUIs and interconnect everything
      - Insider threat; crew / employee screening
    - Alarm Resolution
      - Includes screening protocol
      - Recap BLS to address opaque containers, chlorates, powders, gas
      - Footprint
    - Checked Baggage
      - Remote screening, including international inbound bags
  - Desired end states
    - Automate, Partially Automate vs. Manual.
  - Phased capability roadmaps for better integration with S&T (slotting in projects, milestones, and outcomes, by aspect).
- **Cyber**
  - Culture changes; security by design; defense in depth
    - Why can't the equipment be abstracted away from security?
    - Forever problem.
    - NIST 800-53 is a guideline. Not every control has to apply.
  - Vendors are responsible for maintaining certification configuration; cyber patching adds uncertainty.
- **Red Teaming**
  - Annual work plan.
    - 8 projects / year; proactive agenda / black swan; not tailored to a specific airport.
    - Connect with users; return reliable quantitative data. Defensible and actionable to leadership; methodology similar to pharmaceutical trial
    - Additional perpetual / index testing
    - Focus is on catastrophic damage to airplane
  - Standard Passenger Lane
    - Operate with the level of knowledge the adversary would have
    - Can create tickets that will be a valid boarding pass for security
    - Social engineering – how many layers will adversary withstand?
    - Simulants and real threats
  - Need
    - Better understanding of upcoming solutions to avoid testing what will be updated
    - Better colorimetric kits, detection of chlorates

What Did We Hear?

- **Open architecture**
  - Defer recapitalization: it is expensive to install and remove.
  - Infrastructure / Interoperability to plug in 3rd party algorithms
  - Common workstation, GUI, common platform
  - Communication with TSA Enterprise Architecture
  - Unified File Format, DICOS
  - Own the architecture, own the brains of TSA systems.
- **How do you train your officers to interact with technology?**
  - Support operations with Automation and reduce cognitive load.
  - Analyst is the future TSO
  - Remote screening allows reduced and redeployment of FTE
  - Image review effectiveness and efficiency
    - Hire screeners that excel in visual search task, correlated to on-the-job performance
    - Search patterns, fixations, durations, fatigue

- **Simulated images for DT&E**
  - Have to recollect data if the beam path changes or if the threats change
  - Validating synthetic data, extend the testing timeline.
  - How to smartly test machine learning connecting with the OEM and not connected with the OEM?
  - How do I validate that synthetic data? What do I show to an auditor or vendor who failed that my simulated data was valid?
  - What about simulating real world systems performance
    - Evaluated permissible range of image corruption applied to clean baseline images against winning Kaggle scan images to simulate component failure
    - How is every scanner deployed doing in the field? Is it performing as well as it did when it was initially deployed?
  - Potential for Industry / Government Working Group to standardize features needed by algorithms.
    - Identifying the different use cases for the data, define primary and secondary characteristics.

What Did We Hear?

- **Machine Learning**
  - **Overall**
    - May provide relief vs. costs for traditional algorithm development.
    - Trustworthy AI; even non-critical systems still have serious ramification for decisions.
    - "Magic" - understand failure modes; understanding how decisions are made
    - Transferability of attacks and of training
    - Need to be a human-machine team.
  - **Deep Learning Prohibited Item detection; internal flyoff between several methods**
    - TRL7 – need more data, for more perturbations, more variety to address diverse background, concealment
      - Trained on 13K target images, 450K stream of commerce images.
      - E.g. 3D printed weapons. Perhaps look for ammunition.
    - Algorithm has to work in a way that will provide confidence to an operator.
      - Trust needs to be earned; previous experience has lower confidence.
      - Ceramic knives performed well, plastics, not so well.
    - Physics based knowledge encoded into the color image, based on calibration of known objects.
  - **CLASP: Passenger/baggage correlation though video**
    - Analyze every frame vs. optical flow optimization.
    - First step of 3-step process, temporal consistency.
    - Mask R-CNN
  - **3D reconstruction with limited data**
  - **Machine Learning Issues**
    - Garbage in, gospel out; Trustworthy AI
    - Adaptability to new threats and how to efficiently bootstrap vs. millions of images
    - Overfitting and uncertainty aware models
      - Evaluating the accuracy of the estimated uncertainties. How to combine task-specific variances into useful model information.
    - Non imaging problems
    - Geometric models can overly constrain the problem
    - Fooling neural networks; resiliency against adversarial attacks

What Did We Hear?

- **Deterrence, prevalence and displacement**
  - We need to actively thwart attacks to avoid complacency
  - Not a zero sum game. Multiple and conflicting objectives.
  - Overlapping, not additive
    - May change attack mode, impact, likelihood, displacement
  - Exploit adversary biases for deterrence and countermeasures
  - Perceived randomness enhances countermeasure deterrence value, greater perceived uncertainty
  - Layered or early defenses adds more deterrence than concentrated defense
  - Target rich environment; protect the targets we care about the most
- **Disseminate or censor of terrorist propaganda?**
  - crowdsourcing, public awareness, both good and bad
  - brings fringe ideologies into the public sphere, fame, recognition, tools and tactics
  - mutually self-reinforcing, accelerant, amplification
- **What makes an effective TSO for visual search?**
  - the group of prospective TSOs reflect a range of inherent potential performance
  - training can alleviate the learning curve, but can not turn a poor performer into a excellent performer
  - game performance is correlated to on-the-job-performance

What did we hear/What can we do?

- Understand perspectives of other stakeholders and improve cooperation
- Road to sharing data
  - Data desensitization vs. getting to the finish line
  - Validity of analogous data vs. managing sensitive data

What Did We Hear?

- Panel on alternate stakeholder Perspectives

What do we need to hear more of?

- Show me the money
  - Passenger volume is up. “We will find the money [for screening]”.
  - Enable a vibrant 3rd party and vendor market with funding falling
- How do you get solutions piloted with TSA? Deployed nationwide?
- How to get TSA data?
- How do you validate that detecting analogous problems is equivalent to real detection?
- Does TSA do outreach beyond ADSA?