THE WEAK SIGNALS OF CYBER
DISCERNING AND LEARNING
THAT WHICH IS MEANT TO BE IMPERCEPTIBLE, ILLUSORY, AND TO INVEIGLE

Elena St Amour, Phat Ngo, Tameah Young, James Ness
Federal Aviation Administration
William J. Hughes Technical Center
Atlantic City International Airport, NJ 08405

Cyber threats are often weak signals designed to exploit targeted systems. These signals manipulate cyber, psyber, and risk communication components of the signal to diminish signal-to-noise ratio. Cyber components are the physical aspects of the signal that can range from viral code to the use of aberrant signals from the electromagnetic spectrum to confound operations such as global positioning systems. The psyber component includes the behavioral propensities of the individual operator and level of experience detecting and managing threats. Risk communication is the tension set by the organizational culture priming individual operator propensities. The psyber components affect the ability to perceive contingencies. The risk communication sets the signal detection threshold for distinguishing true threats from false alarms. This paper describes current simulation efforts to afford the application of evidence-based methods to discern weak signals and to accelerate the experience of operators in discriminating weak signals via immersive training simulations.

In compliance with the Aircraft Certification, Safety, and Accountability Act (2020), the National Academy of Sciences, Engineering, and Medicine initiated a 10-year program to identify, categorize, and analyze emerging safety trends in air transportation. In the report, an identified critical need is to discern anomalous patterns in the aviation system visible only as “weak signals” (National Research Council, 2022). Cyber threats are often in the form of weak signals with the signal-to-noise ratio typically manipulated along cyber, psyber, and risk communication parameters. Cyber refers to physical aspects such as hardware, software, and the electromagnetic spectrum used in information technology. Psyber is the influence of cyber on that which is apprehended by the targeted system’s operators. Risk communication is the level of tension set in the organizational culture influencing the degree of operator attention from complacency to overreaction.

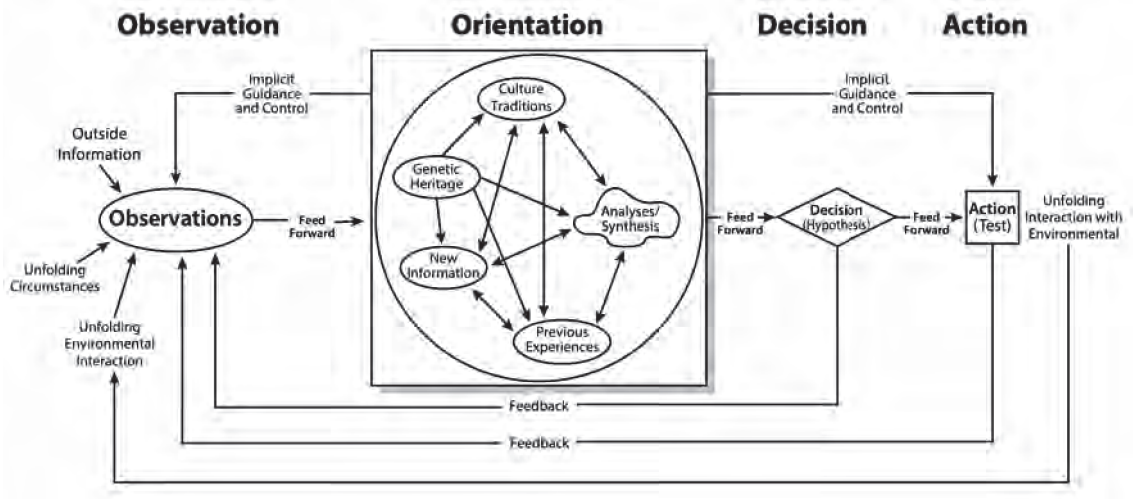

Figure 1. Boyd's OODA Loop

The causal attribution of cyber is perceived in that the operator must detect, either directly or by way of automation, the antecedent/consequent events associated with the signal pursuant to attributing a cause. The causal attribution is the perception of the cyber threat as being either present or absent. In either case the attribution can be correct or mistaken, with the intent of the cyber threat to promote a mistaken perception. The decision process is influenced by the signal's cyber, psyber, and risk communication aspects. Given these aspects, the decision process assigning cause is best described in the OODA loop (MacCuish 2012). Figure 1 shows the OODA loop decision process, which is a feedback loop integrating the steps of Observe, Orient, Decide and Action (Boyd, 2018). Orientation is central in the feedback loop process; previous experience and organizational culture shape Orientation to the signal influencing Decisions and Actions. By nature, cyber signals are novel as the threats evolve. Given potential consequences of the evolving threat, organizations tend toward strict information technology cyber safety protocols. This action, in some ways prudent, does affect the organizational culture in its ability to use information technology to achieve organizational mission, which in turn influences its shared idea of cyber security as legitimate action to an imminent threat or overreaction.

Since all permutations of experiences in the future of air and space transportation cannot be known *a priori*, proscribed intentional controls, memorization of facts, or scripted sequences are likely to be of limited value. A more human centric approach to meeting the future is to note that the quintessential human means for diffusing lessons and experiences is through a tradition of passing on stories (Campbell, 1973). Representations of experiences, as in cave paintings and storytelling are the oldest traditions of recounting events, imparting lessons, and projecting affect (Lord, 1971). These formats structure information in part-whole relations affording the experiencer schematic frameworks to interpret past, present, or future analogous events (Mandler & Johnson, 1977). The diffusion of lessons through stories, using technology-mediated means diffuses lessons in a rapid and salient manner affording exploration of the art of the possible (Aldrich, 2005).

Within big data there exists the foundations of stories in that within big data is an extensive time series of information that cuts across contexts. This information can be compressed and presented in models and simulations to accelerate the experiences of the principals. This process is leveraged in the development of air traffic control simulations which are based on data from the Performance Data Analysis and Reporting System (PDARS). PDARS is the repository for key flight events such as flight transitions, facility handoffs, air space crossing, etc. Leveraging the PDARS, models and simulations can be developed to accelerate experience in the art of the possible in cyber threats, the mitigation of those threats, and in refining the organization's risk communication of cyber threats.

In shaping risk communication, the leadership must recognize that certain terms and actions have a psychological saliency that focuses collective attention on a concept (e.g., cyber) in a manner that can overshadow alternatives and exceptions to the collective idea (Ness, 2006). The replicated idea shared across individuals in the organization becomes the organizational culture's meme. A meme is a concept first introduced by Dawkins (1976) arguing that all life evolves by the differential survival of replicating entities. Extending the idea of the biological replicating entities, genes, the meme is a unit of cultural transmission. As a replicating entity a meme exhibits the properties of longevity, fecundity, and copying-fidelity, which make an established meme hard to undo. Thus, in conveying its meme of cyber, the organization should apply due diligence in forming and communicating its unit of cultural transmission through its actions and words, balancing along the continuum of complacency to overreaction.

This paper presents an ongoing effort to develop models and simulations to meet the challenge of detecting and acting appropriately on weak signals often associated with cyber threats. The purpose of these models and simulations is to optimize operator decision making as described in the OODA loop. Within this broader purpose, the methods presented are a framework for models, simulations, and digital

twins of future potential strains on the National Airspace System such as challenges of remote piloted aircraft and commercial space transportation.

Method

In collaboration with other Federal Agencies, The Federal Aviation Administration's William J. Hughes Technical Center contributes to and leads efforts to defend the Nation's infrastructure from cyber threats. One such effort is the Cyber Rodeo Lab Intrusion Detection Event. For the 2022 event, a remotely accessible Standard Terminal Automation Replacement System (STARS) simulation (Stasiowski, Kaelin, & Prata 2021) was employed. Figure 2 depicts the system image of the remote simulation. The remote simulation differs from the test facility set up in that the remote simulation renders the trackball and keypad hardware as interactive virtual input devices.

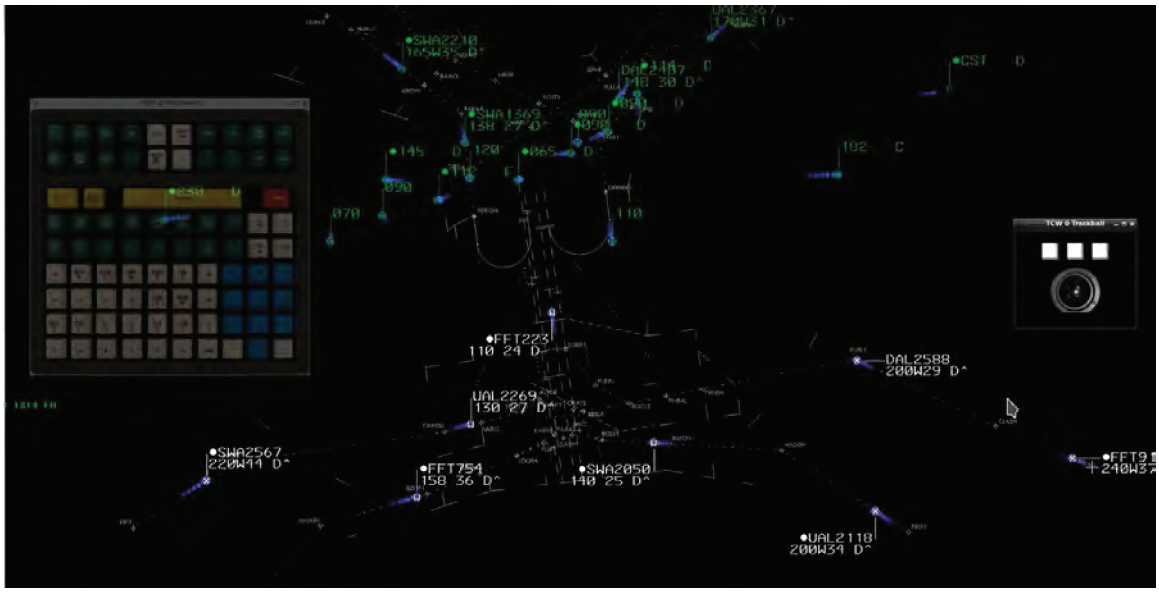

Figure 2. STARS interface showing west sector arrivals in white. Note that the trackball and keypad are virtual.

The Standard Terminal Automation Replacement System (STARS) is the fielded system used by Air Traffic Controllers to ensure the safe separation of military and civilian aircraft within the terminal airspace of the United States. STARS is a real-time digital processing and display system that replaced legacy air traffic control automation equipment at over 200 FAA and Department of Defense (DoD) Terminal Radar Approach Control (TRACON) facilities, over 600 FAA and DoD Air Traffic Control Tower facilities, and more than 100 systems installed and maintained at STARS support sites including Operational Support Facilities (OSFs) and the FAA Academy airspace (*FAA,* 2022).

Procedure

Air traffic scenarios were derived from Denver traffic flow archived in the PDARS. Figure 2 shows the virtual user interface with which the volunteer air traffic controller interacted. The controller was assigned the west sector for incoming traffic, which are the white airline track identifications. For a trial, the controller was briefed on their sector, within which they controlled the traffic for several minutes to establish baseline performance. Subsequent the baseline period anomalous targets were introduced into the traffic flow. Figure 3 shows a Google Earth Pro rendition of the Denver scenario depicting the anomalous target labeled "Spoof2" in conflict with UAL282. The insertion of anomalous targets was to

test the effect on controller actions upon presentation of the anomalous target. The anomalous target simulated a drone signaling its position using an Automatic Dependent Surveillance-Broadcast (ADS-B). Thus, the anomalous target's flight characteristics were not typical of commercial aircraft, but its broadcasted information mimicked that of commercial aircraft. To verify that the target was anomalous the controller had to switch from a fused sensor mode to a single sensor radar mode turning off sensors registering the ADS-B information.

Single Sensor Mode is a mode that displays data from only one sensor/radar on the STARS Terminal Controller Workstation (TCW) display. Fused Mode is a mode that combines all data from all sensors/radars normally used by the site along with ASD-B data and displays the combined data on the TCW display. ADS-B is an advanced surveillance technology that combines an aircraft's positioning source, aircraft avionics, and a ground infrastructure to create an accurate surveillance interface between aircraft and air traffic control. ADS-B is a performance-based surveillance technology that is more precise than radar and consists of two different services: ADS-B Out and ADS-B In. ADS-B Out works by broadcasting information about an aircraft's GPS location, altitude, ground speed, and other data to ground stations and other aircraft, once per second. ADS-B In provides operators of properly equipped aircraft with weather and traffic position information delivered directly to the cockpit (*FAA, n.d.*).

Figure 3. Google Earth rendition of flight path showing the Spoof2 and UAL282 conflict.

Results and Discussion

The results of the simulation proved a successful test of the remote access STARS simulations. There was mention in the post-trial debriefing that using the virtual trackball presented some difficulties and that the hardware version of the trackball interface would improve immersion and realism. A hardware version for remote access simulations is being worked. Notwithstanding, the success of a remotely accessible system means greater access to principals involved in air traffic control toward greater representation of elements of the National Airspace System (NAS) informing models and simulations designed to discern the weak signal of the cyber threat.

During the post-trial debriefings, the controllers mentioned that "spoof" was not currently in the lexicon of Air Traffic Controllers. A discussion of communicating the risk of anomalous targets resulted in maintaining the current risk communication to the term "anomalous target" vice the promulgation of the term "spoof" or other terms that would bias the controller's orientation in the OODA loop process.

Figure 4 shows the Air Traffic Controller's action resolving the "Spoof2" and UAL282 conflict. The ADS-B signal displayed on the TCW from "Spoof2", which had no other associated identification, was efficiently identified as anomalous and tagged in yellow as "WATCH". This indicated that the air traffic controller was Observing and Orienting on information to discern the nature of the seeming conflict. Air traffic control was affected only in that some attention was resourced to the "WATCH" anomaly. Upon further OODA loop processing, the controller Decided that the anomaly did not pose a threat and renamed it "whodat", which was followed by the Action of moving the icon from the approach sector.

Figure 2. Anomalous target colored yellow and labeled "WATCH".

In conclusion, the simulation confirmed the centrality of Orientation in the OODA loop process. Moreover, the simulation informs future presentation of simulation generated system images. System images are the operator's conceptual models made manifest by the signals presented in the simulation (Norman, 2013). For example, signal qualities of "Spoof2" Oriented the controller to its track. Inferences concerning effects of controller experience and threshold differences between behaviors of commercial aircraft and anomalous target are plausible explanations of operator behavior but remain empirical questions. Future work will begin with storyboarding scenarios for simulations designed to titrate signal detection thresholds for art of the possible cyber threats. Simulations which best inform signal detection thresholds (Stanislaw & Todorov, 1999), will be candidates for development as immersive training simulations and for the development of digital twins to accelerate modeling of "what ifs". These simulations will provide evidence-based methods to discern "weak signals" and to accelerate the experience of operators in discriminating "weak signals" pursuant to mitigating safety threats, particularly those which evince from accumulated faults along the complex decision stream.

Acknowledgements

Stephanie Bell & Joe Pagano for their leadership ensuring a meaningful product.
Snezana Gatto for her brilliant orchestration of the simulations.
Joseph Stasiowski for his system engineering that afforded us a remotely accessible simulation.
Steve Jacobs & Wes Stoops for their ATC wisdom that guided scenario development.

References

Aircraft Certification, Safety, and Accountability Act (2020). Retrieved from https://www.congress.gov/bill/116th-congress/house-bill/8408

Aldrich, C. (2005). *Learning by Doing: A Comprehensive Guide to Simulations, Computer Games, and the Pedagogy in e-Learning and Other Educational Experiences*. Pfeiffer, New York.

Campbell, J. (1973). *Myths to Live By*. Bantam Books, New York.

Dawkins, R. (1976). *The Selfish Gene*. Oxford University Press, New York.

Boyd, J.R. (2018). *A Discourse on Winning and Losing*. Air University Press, Maxwell AFB, AL.

FAA. (2022, February 25). *Standard Terminal Automation Replacement System (STARS)*. Federal Aviation Administration. Retrieved from https://www.faa.gov/air_traffic/technology/tamr/arts/

FAA. (n.d.). *Automatic Dependent Surveillance - Broadcast (ADS-B)*. Federal Aviation Administration. Retrieved from https://www.faa.gov/about/office_org/headquarters_offices/avs/offices/afx/afs/afs400/afs410/ads-b

Lord, A. B. (1971). *The Singer of Tales*. Atheneum, New York.

MacCuish, D. (2012). Orientation: Key to the OODA Loop – Cultural Factor. *Journal of Defense Resource Management, 3*(2), 67-74. Retrieved from http://www.jodrm.eu/issues/volume3_issue2/05_maccuish_vol3_issue2.pdf

Mandler, J. M. & Johnson, N. S. (1977). Remembrance of things parsed: Story structure and recall. *Cognitive Psychology, 9*, 111-151.

National Research Council (2022). Emerging Hazards in Commercial Aviation Report 1: Initial Assessment of Safety Data and Analysis Process. The National Academies Press, Washington, D.C. Retrieved from http://doi.org/10.17226/26673

Ness, J. (2006). Communicating the Risk of Weapons of Mass Casualty. *U.S. Military Academy Combating Terrorism Center Biodefense Report, 1*(1), 10-12. Retrieved from https://www.files.ethz.ch/isn/26330/ctc_biodefense_rep_june_06.pdf

Norman, D. (2013). *The Design of Everyday Things*. Basic Books, New York.

Stanislaw, H. & Todorov, N. (1999). Calculation of signal detection theory measures. *Behavioral Research Methods, Instruments, & Computers, 31*(1), 137-149.

Stasiowski, J., Kaelin, C. & Prata, W. (2021, May 13). Making T&E Pandemic-Proof: Transforming T&E. *Paper presented at 24th ITEA Test and Training Instrumentation Workshop: Innovating for Tomorrow's Challenges*.