Intelligent Human Systems Integration (IHSI), Vol. 200, 2026, 148–158
https://doi.org/10.54941/ahfe1007074

Fake Aircraft, Real Threats: Training Air Traffic Controllers for Cyberattacks

Maria Hagl[1], Supathida Boonsong[2], Tim-Heiko Stelkens-Kobsch[1], Tim Ruediger[1], Andrei Gurtov[3], and Gurjot Singh Gaba[3]

[1]German Aerospace Center DLR, Institute of Flight Guidance, 38108 Braunschweig, Germany
[2]Air Navigation Services of Sweden (LFV), Research and Innovation, 601 79 Norrköping, Sweden
[3]Department of Computer and Information Science (IDA), Linköping University, Linköping 581 83, Sweden

ABSTRACT

As part of the modernisation of air traffic management, a growing number of infrastructures and technologies are being deployed to improve air traffic services. While these developments can improve situation awareness and operational efficiency, they also come along with increasing cybersecurity risks. This study presents a half-day training concept for air traffic controllers to identify cyberattacks exploiting ADS-B vulnerabilities. Eight experienced Swedish Air Traffic Controllers (ATCOs) participated in three simulation runs using the Attack Simulator, a cybersecurity training platform that simulates various cyberattacks. Performance was measured by the correct identification of six probabilistically occurring attacks, with weighted scores reflecting the difficulty of each event. Knowledge transfer through briefing and video-based training aimed to educate ATCOs about cyberattacks that they could realistically face during their duties. Subjective assessments of situation awareness, workload, and stress were generally acceptable. Results suggest that training significantly improves ATCOs' ability to respond to cyberattacks.

Keywords: Cybersecurity, Risk, Human factors, Training, Air traffic management, Digitalisation

INTRODUCTION

As part of the modernisation of Air Traffic Management (ATM), an increasing number of infrastructures and technologies are being deployed to improve the provision of Air Traffic Services (see Sabatini, 2016, El Asri and Tsiakalos, 2024, Pierattelli et al., 2025). For example, the large-scale implementation of Automatic Dependent Surveillance-Broadcast (ADS-B) enables controllers to gain better situation awareness of aircraft in the airspace and to manage traffic more safely and efficiently (Ahmed, 2024, Kožović et al., 2023). Digitalisation in aviation, however, is accompanied by significant cybersecurity risks (Ukwandu et al., 2022, Lykou et al., 2019). A recent case in Europe illustrated this when a cyberattack on several major airports disrupted automated check-in and boarding systems, resulting in days of operational recovery efforts (Tidy and Wilson, 2025). This incident is by no means unique; the aviation industry has experienced numerous cyberattacks that involved

Received August 29, 2025; Revised November 10, 2025; Accepted November 25, 2025; Available online February 1, 2026

various hacker types and targets between 2000 and 2024, including both airports and airlines (Florido-Benítez, 2024). Moreover, the trend clearly indicates a substantial increase in cyberattacks within the aviation sector in the last year (Thales, 2025). The sources of vulnerability are multifaceted. It is clear, however, that increasing interconnectivity and challenges in human factors create exploitable entry points for attackers (Bernsmed et al., 2024).

For the purposes of this study, cyberattacks do not refer to common IT incidents such as phishing emails or malware, but to ADS-B-related vulnerabilities and cyberthreats (Ali and Leblanc, 2024, Mohsen and Naima, 2017). Within this framework, our primary focus is on operationally critical threats to Air Traffic Controllers (ATCOs), such as the injection of false data into surveillance data streams, where an *"attacker modifies, blocks, or emits fake ADS-B messages to dupe controllers and surveillance systems"* (Cretin et al., 2020, p. 143). The potential consequences could range from economic losses (e.g., inefficient staffing caused by the appearance of non-existent aircraft on a controller's surveillance display) to safety-critical situations, such as controller overload resulting from false information, which in turn may increase the likelihood of human error. Preventive measures are therefore required. One option is to develop technologies capable of automatically detecting cyberattacks in surveillance systems (see Nagothu et al., 2019), such as in ADS-B (see Khoei et al., 2024, Kacem et al., 2021, Ying et al., 2019, Vajrobol et al., 2025). However, even with such support, the human operator remains central and ultimately responsible for decision-making. In aviation, the risk of incorrectly categorising a real aircraft as a false object is too high to rely solely on algorithmic indications or filters. ATCOs must be able to evaluate all information critically, integrating system outputs with their professional judgment to distinguish actual traffic from maliciously generated false information. This underlines the need for targeted training to prepare ATCOs for potential cyberattacks occurring in their operational environment. Such training should enable them to recognise and respond appropriately to cyberattacks through both theoretical knowledge transfer and practical exercises. With this in mind, this study introduces and evaluates an initial training concept using the Attack Simulator, described in the method section below.

METHOD

Participants and Study Framework

Participants of the study were eight experienced Swedish ATCOs (five male and three female), recruited via a purposive sampling method provided by the Swedish ANSP Luftfartsverket (LFV). Participants' ages ranged from 30 to 59 years ($M = 45.1$), with work experience from 1 to 35 years ($M = 18.1$). None of the participants had received prior training specific to cyberattacks in ATM, nor had they encountered the Attack Simulator used in this study. The experiment was conducted at the Air Traffic Control Centre (ATCC) Malmö, Sweden, in a quiet conference room. Participants were briefed on the study's goals, completed an informed consent form, and a demographic questionnaire. The overall study setting is shown in **Figure 1**.

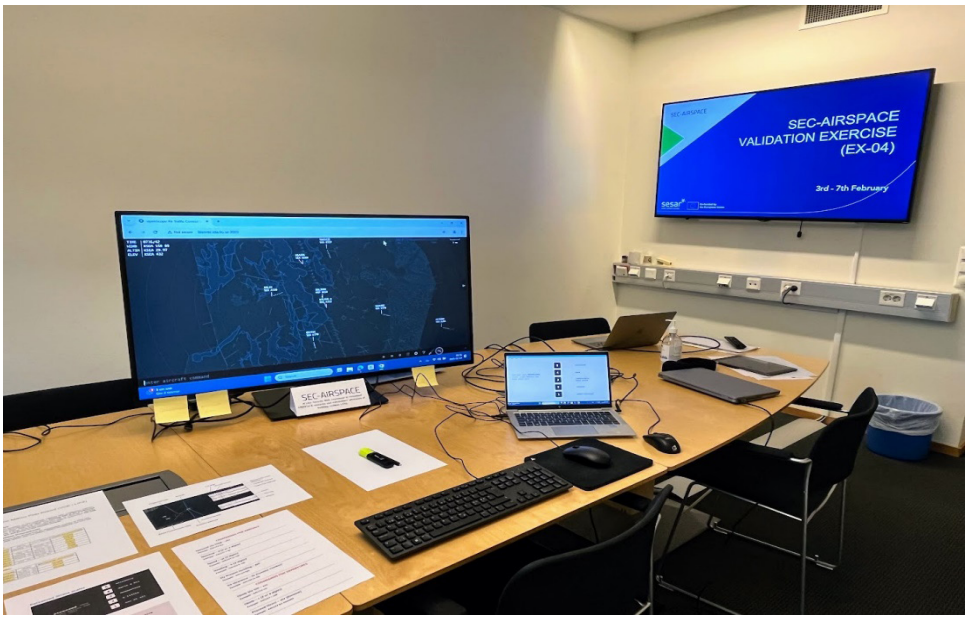

Figure 1: Study setting at air traffic control center Malmö.

Information about the Attack Simulator

The Attack Simulator is a specialised cybersecurity training platform that simulates various cyberattacks on ATM systems. Built upon the OpenScope air traffic simulator (Openscope, 2025), it integrates multiple cyberattack vectors that exploit known vulnerabilities in ADS-B protocols (see Costin and Francillon, 2012, Smailes et al., 2021) that ATCOs could realistically face during their duties. The simulator featured six types of cyberattacks. They included:

- 'Non-Responsive Aircraft', which ignored Air Traffic Control (ATC) instructions
- 'False Information', where an aircraft intermittently transmitted incorrect altitude (5,000–40,000 ft) and speed (280–600 knots);
- 'Standing Still', where an aircraft paused for 3–15 seconds
- 'False Squawk Code', where an aircraft used invalid or emergency codes (e.g., 7500, 7600)
- 'False Heading', where an aircraft made uncommanded directional changes
- 'Duplicate Aircraft', where a cloned aircraft replicated a legitimate one with identical identifiers.

By embedding these attack types into an interactive environment mirroring actual ATC workflows, the simulator provides a realistic setting to evaluate a controller's performance under adversarial conditions (Blåberg et al., 2020).

The graphical interface (see screen at the working position in **Figure 1**) replicated standard ATC workflows, displaying aircraft callsigns, altitude,

type, and trajectory. Controllers interacted with the system using a text-based command box and standard ATC syntax (e.g., *"AAL123 d 40"* for descent, *"AAL123 h 130"* for heading, *"AAL123 ils 04r"* for ILS clearance). Detected cyberattacks were reported using structured inputs to flag anomalies, such as 'non-responsiveness'. These commands enabled real-time logging of participants' cyber incident assessments.

Regarding the simulated airport, Malmö Airport (ESMS) was initially preferred, as participants were familiar with its operational environment. However, since the airport had not yet been integrated into the simulation platform, Venice Airport (LIPZ) was selected as a suitable alternative. Its classification as a light-traffic airport, combined with its airspace structure and simple traffic patterns, offers an accessible and pedagogically effective simulation environment. Detection performance was evaluated using a time-weighted score that prioritised speed and accuracy. Each scenario had a probabilistic threat model to mimic real-world unpredictability. Correct identifications within a minute earned 100 points, decreasing by 10 points per minute to 50 after five minutes. An incorrect or no response within eight minutes lead to a 100-point penalty. Participants could retract guesses.

Study Design and Measured Variables

The study followed a repeated-measures design, with each participant completing three 25-minute simulation runs. The first run was a training session that allowed participants to familiarise themselves with the Attack Simulator; no data from this phase were included in the analysis. In the second and third runs of the experiment, we conducted actual measured simulations with cyberattacks. Before the second run, participants received a short briefing on the types of cyberattacks that could occur during the simulation. Prior to the third run, participants were presented with a video-animated knowledge transfer session designed to improve their understanding of how cyberattacks manifest within the simulation environment. In both Run 2 and Run 3, all six types of attacks could occur, with a 30% probability for pre-spawned aircraft and a 40% probability for newly spawned aircraft. This experimental design was intentionally selected to mimic real-world cyberattacks and minimise the likelihood that participants would anticipate all potential stimuli and adjust their responses accordingly.

During the two experimental simulation runs, we recorded performance scores, which were later weighted based on the detection rate of specific attacks and the total number of events per scenario. For any omission or incorrect guess regarding an event type, the points deducted for that event type were multiplied by the detection rate of the event type. The points awarded for a correct identification were multiplied by (1 minus the event's detection rate). Thus, events that were more difficult to correctly identify were penalised less than those that were easier to correctly identify. The final score for a scenario was divided by the total number of attacks during the simulation run.

This approach ensured that participants' reactions were evaluated in the context of the actual events they experienced. It is essential to note that ATC task points have been excluded, as evaluating operator performance related to ATC tasks was outside the scope of this study. After each experimental run, participants completed post-simulation questionnaires that assessed situation awareness via SASHA (Dehn, 2008), perceived workload via Raw TLX, an unweighted version of the NASA-TLX (Hart, 1986, Hart, 2006), stress via SSSQ (Helton and Näswall, 2015), and tailored questions regarding their confidence in correctly identifying and labelling the cyberattacks. Additional questions related to the perception of the Attack Simulator for cybersecurity training, followed by a debriefing, were included after the final simulation run. To get a better insight into data patterns during the individual simulation runs, we collected participants' subjective assessments of perceived workload via the ISA-workload scale (Jordan and Brennen, 1992, Kirwan et al., 1997) and stress via a single-indicator item (Jones et al., 2017) at two-minute intervals. Additionally, we measured their heart rate to calculate heart rate variability with Kubios (Tarvainen et al., 2014). The study received approval from an institutional ethics committee that was independent of the project.

RESULTS

Cyberattack Detection Performance

An analysis of the descriptive statistics for ATCO performance during simulation runs 2 and 3 (see **Table 1**) shows that there were no positive performance scores in either run. The lowest performance score was observed in Run 2 at −697.64 points, while the highest score was recorded in Run 3 at −7.69 points.

Table 1: Descriptive statistics of performance scores in Run 2 and Run 3.

Run	M	SD	P50	Min	Max
2	–390.90	200.37	–314.90	–697.64	–191.67
3	–198.53	135.41	–233.98	–346.60	–7.69

A comparison of individual participant performance between the two simulation runs (see **Figure 2**) reveals that all participants, except one (KD5Y), consistently improved from Run 2 to Run 3.

A Wilcoxon signed-rank test indicates that the difference is significant $z = -2.38$, $N = 8$, $p < .05$. On average, participants improved by 192 points, which represents a mean relative performance increase of 48.52%. As shown in **Figure 2**, the performance gaps for KD5Y (−33 points) and for two other participants (KP9V, +40 points; RT2N, +61 points) were not particularly large. It is noteworthy that participants who performed particularly poorly in Run 2 achieved some of the highest improvements, with increases exceeding +300 points (see DF4W, JN6Z, and ML3T).

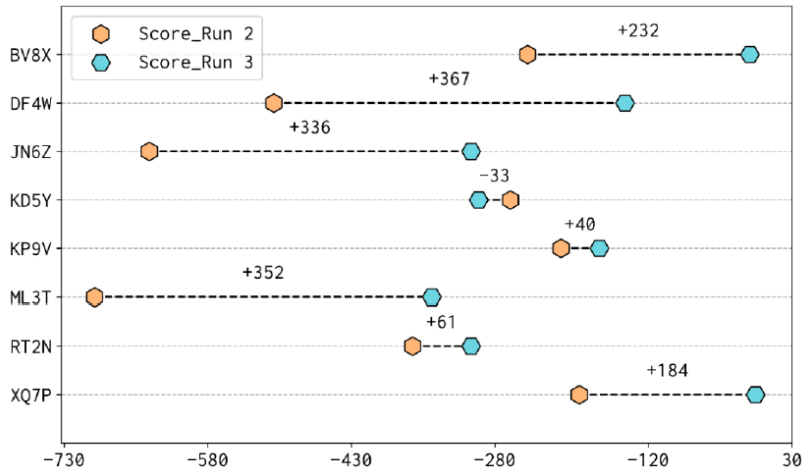

Figure 2: Performance scores per simulation run and participant, sorted alphabetically by pseudonym.

Perceived Situation Awareness After Simulation

Participants evaluated their situation awareness after each simulation run on a scale from 0 to 6 (SASHA). The average score in both simulation runs exceeds 4, indicating that situation awareness was generally fairly good in Run 2 and Run 3. While their subjective situation awareness slightly improved from the second ($M = 4.15$; $SD = .91$) to the third simulation run ($M = 4.23$; $SD = .98$), a Wilcoxon signed-rank test indicates that the difference is not significant $z = -.56$, $N = 8$, $p = .62$.

Perceived Workload and Stress During and After Simulation

Participants rated their workload after each simulation run on the Raw TLX. The average RTLX score (maximum possible score = 100) in both runs is below 50, indicating that the workload was generally within an acceptable range. While their subjective workload slightly decreased from the second ($M = 43.65$; $SD = 14.52$) to the third simulation run ($M = 35.31$; $SD = 17.02$), a paired t-test indicates that the difference is not significant $t(7) = 1.24$, $p = .13$.

Stress was evaluated after each simulation run on a scale of 1 to 5 across three dimensions (i.e., engagement, distress, and worry). For 'engagement', the average score in both runs was above 4, indicating a relatively engaging stress level. While their engagement slightly increased from the second simulation run ($M = 4.05$; $SD = .37$) to the third run ($M = 4.22$; $SD = .30$), a Wilcoxon signed-rank test indicates that the difference is not significant $z = -1.62$, $N = 8$, $p = .13$. Concerning 'distress', the average score in both runs were below 2, indicating a relatively low level of distress. While their distress slightly decreased from the second simulation Run ($M = 1.64$; $SD = .87$) to the third simulation run ($M = 1.33$; $SD = .29$), a Wilcoxon signed-rank test indicates that the difference is not significant $z = .91$, $N = 8$, $p = .5$. Regarding 'worry', participants reported moderate worry after the

second simulation run and relatively low worry after the third simulation run. Worry decreased from the second simulation run ($M = 2.83$; $SD = .81$) to the third simulation run ($M = 1.83$; $SD = .61$). A Wilcoxon signed-rank test indicates that the difference is significant $z = 2.39$, $N = 8$, $p < .05$.

The relatively nuanced picture in individual response patterns for past-simulation workload and stress perception is not particularly surprising. After all, the likelihood of cyberattacks was programmed probabilistically, so no two simulation runs were identical. However, examining the continuously measured subjective assessments of workload and stress alongside the raw simulator data in individual runs reveals apparent patterns: when air traffic controllers were exposed to higher traffic loads or faced multiple attacks, they reported higher levels of workload and stress, and their heart rate variability seemed to decrease concurrently. These patterns are based solely on a visual inspection of the raw data and should therefore be interpreted with caution.

Confidence in Identification and Labelling of Malicious Aircraft

Participants evaluated their confidence in identifying and labelling malicious aircraft on a scale from 0 (not at all confident) to 4 (completely confident).

On average, participants were slightly confident that they had correctly identified malicious aircraft in the second simulation run ($M = 1.0$; $SD = .93$) and somewhat confident in the subsequent run ($M = 1.88$; $SD = .83$). A Wilcoxon signed-rank test indicates that the difference is not significant $z = -1.97$, $N = 8$, $p = .13$. When they were confident that they had correctly identified a malicious aircraft as a cyberattack, they were only somewhat confident that they had labeled it correctly as the specific type of cyberattack in Run 2 ($M = 1.88$; $SD = 1.55$) and somewhat to fairly confident in Run 3 ($M = 2.38$; $SD = .92$). A Wilcoxon signed-rank test indicates that the difference is not significant $z = -.74$, $N = 8$, $p = .5$.

Perception of the Attack Simulator for Training Purposes

When asked whether training with the Attack Simulator had increased their *"awareness of potential cybersecurity threats"* and whether training with the Attack Simulator had improved their *"ability to respond to cybersecurity threats in real-time"*, the perceptions among participants vary. The distribution of responses regarding the effectiveness of the Attack Simulator in improving cybersecurity awareness and responsiveness among ATCOs is shown in **Figure 3**.

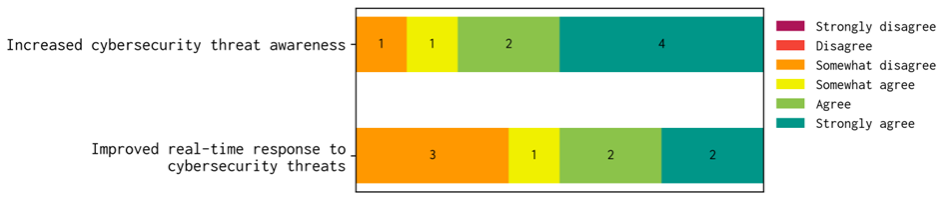

Figure 3: Distribution of responses regarding the effectiveness of the attack simulator in enhancing cybersecurity awareness and responsiveness among ATCOs.

All three participants who somewhat disagreed with one or both statements were asked to clarify why they felt they made little or no progress in their knowledge or training with the Attack Simulator. One participant explained that maintaining vigilance regarding these issues at work is difficult because these situations occur rarely, almost never. Two other responses pointed to limitations in the simulator's equipment. One participant emphasised that the simulation should be carried out in a more realistic work environment. In their case, this involves using radio communication rather than written instructions for pilots. Another participant remarked on the limited range of available tools, noting that the equipment in their actual work setting allows them to determine *"whether there is a pilot error or an actual threat from someone attacking the system"*. Nonetheless, this same participant acknowledged that the simulation improved their understanding of certain cyberattacks and improved their capacity to detect them.

When asked whether using data from the Attack Simulator could be *"beneficial to refine ongoing training programs in air traffic control"*, one participant somewhat agreed, five agreed and two strongly agreed (cumulative positive responses $n = 8$; 100%). Similarly, in response to whether using data from the Attack Simulator could help *"to improve operational protocols for enhancing cybersecurity resilience in air traffic control"*, one participant somewhat agreed, six agreed and one strongly agreed (cumulative positive responses $n = 8$; 100%).

DISCUSSION AND CONCLUSION

This study evaluated an initial training concept using the Attack Simulator, designed to train ATCOs for operationally critical cyberthreats in ADS-B systems, such as the injection of false surveillance data (see Ali and Leblanc, 2024, Cretin et al., 2020, Costin and Francillon, 2012).

Results indicate significant improvements in performance scores between simulation Runs 2 and 3, even though not all participants perceived the improvement, possibly because they found the user interface unfamiliar or inconsistent with their standard operational tools. The observed gains are likely attributable to learning effects from repeated practice, video-based knowledge transfer, or both, with the highest improvements among participants who initially performed poorly. Subjective assessments of situation awareness, workload, and stress were generally acceptable, suggesting that participants were not overloaded with traffic and that the experimental conditions were appropriate for training. Individual variability in these measures likely reflects the probabilistic generation of events in the simulator, with higher traffic or multiple attacks associated with increased workload and stress. However, future studies should implement identical or comparable scenarios to allow more precise evaluation of ATCOs' understanding of how cyberattacks manifest and how workload and stress respond to varying attack patterns.

Preliminary in-simulation workload and stress indicators (psychometric and physiological measurements) were only visually inspected to complement the results presented in this article. A detailed analysis of these data was

beyond the scope of the present paper, but is planned for future research. Such an analysis could provide insights into how psycho-physiological responses evolve during training. This could help nuance the distinction between normal adaptive stress reactions and potential cognitive overload. Thus, individually adapted training could target the moments when operators are most likely to enter these states.

For this study, Venice Airport (LIPZ) was used, as Malmö (ESMS) was not yet available in the simulator. In future studies, it would be preferable to simulate the sectors in which ATCOs actually operate to improve training realism.

In conclusion, the tested training concept using the Attack Simulator was positively received and represents a valuable tool for training ATCOs to detect and respond to ADS-B cyberattacks. Larger sample sizes are needed to confirm these findings and further explore the potential of the training concept.

ACKNOWLEDGMENT

This publication is based on the work performed in the SEC-AIRSPACE project, which has received funding from the SESAR 3 Joint Undertaking under grant agreement No 101114635 under European Union's Horizon Europe research and innovation programme. Views and opinions expressed are, however, those of the authors only and do not necessarily reflect those of the European Union or SESAR 3 Joint Undertaking. Neither the European Union nor SESAR 3 Joint Undertaking can be held responsible for them.

REFERENCES

Ahmed, W. 2024. ADS-B communication in modern air traffic management: threats, risks and security solutions. *Science,* 1, 1–9.

Ali, H. & Leblanc, S. P. 2024. Vulnerabilities of Automatic Dependent Surveillance-Broadcast on Aircraft: Survey. *2024 International Conference on Computing, Internet of Things and Microwave Systems (ICCIMS)*.

Bernsmed, K., Meland, P. H., Stelkens-Kobsch, T. H., Tedeschi, A., Dambra, C., Buselli, I., Frumento, E., Martintoni, D., Senni, V. & Gurtov, A. SEC-AIRSPACE: addressing cyber security challenges in future air traffic management. Eighteenth International Conference on Emerging Security Information, Systems and Technologies., 2024. International Academy, Research and Industry Association (IARIA), 165–171.

Blåberg, A., Lindahl, G., Gurtov, A. & Josefsson, B. Simulating ADS-B Attacks in Air Traffic Management. 2020 AIAA/IEEE 39th Digital Avionics Systems Conference (DASC), 11–15 Oct. 2020 2020. 1–10.

Costin, A. & Francillon, A. 2012. Ghost in the Air (Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices. *Black Hat USA*.

Cretin, A., Vernotte, A., Chevrot, A., Peureux, F. & Legeard, B. 2020. Test Data Generation for False Data Injection Attack Testing in Air Traffic Surveillance. *2020 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW)*.

Dehn, D. M. 2008. Assessing the Impact of Automation on the Air Traffic Controller: The SHAPE Questionnaires. *Air Traffic Control Quarterly.*

El Asri, H. & Tsiakalos, S. Digital Solutions for Enhanced Operational Efficiency: NextGen Air Traffic Management Systems. ICDTA: International Conference on Digital Technologies and Applications, 2024 Cham. Springer Nature Switzerland, 212–221.

Florido-Benítez, L. 2024. The types of hackers and cyberattacks in the aviation industry. *Journal of Transportation Security,* 17, 13.

Hart, S. G. 1986. NASA Task Load Index (TLX): Paper and Pencil Package-Volume 1.0. NASA Armes Research Center Moffett Field, CA United States.

Hart, S. G. 2006. Nasa-Task Load Index (NASA-TLX); 20 Years Later. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting,* 50, 904–908.

Helton, W. S. & Näswall, K. 2015. Short Stress State Questionnaire: Factor Structure and State Change Assessment. 31, 20–30.

Jones, M., Taylor, A., Liao, Y., Intille, S. S. & Dunton, G. F. 2017. Real-time subjective assessment of psychological stress: Associations with objectively-measured physical activity levels. *Psychology of Sport and Exercise,* 31, 79–87.

Jordan, C. & Brennen, S. 1992. Instantaneous self-assessment of workload technique (ISA). *Defence Research Agency, Portsmouth*.

Kacem, T., Kaya, A., Keceli, A. S., Catal, C., Wijsekera, D. & COSTA, P. ADS-B Attack Classification using Machine Learning Techniques. 2021 IEEE Intelligent Vehicles Symposium Workshops (IV Workshops), 11-17 July 2021 2021. 7–12.

Khoei, T. T., Ould Slimane, H., Shamaileh, K. A., Kumar Devabhaktuni, V. & Kaabouch, N. Detecting Injection Attacks in ADS-B Devices Using RNN-Based Models. 2024 Integrated Communications, Navigation and Surveillance Conference (ICNS), 2024. 1–8.

Kirwan, B., Evans, A., Donohoe, L., Kilner, A., Lamoureux, T., Atkinson, T. & Mackendrick, H. 1997. Human factors in the ATM system design life cycle. *FAA/ Eurocontrol ATM R&D Seminar.*

Kožović, D. V., Đurđević, D. Ž., Dinulović, M. R., Milić, S. & Rašuo, B. P. 2023. Air Traffic Modernization and Control: ADS-B System Implementation Update 2022—A Review. *Fme Transactions,* 51.

Lykou, G., Iakovakis, G. & Gritzalis, D. 2019. Aviation Cybersecurity and Cyber-Resilience: Assessing Risk in Air Traffic Management. *In:* Gritzalis, D., Theocharidou, M. & Stergiopoulos, G. (eds.) *Critical Infrastructure Security and Resilience: Theories, Methods, Tools and Technologies*. Cham: Springer International Publishing.

Mohsen & Naima, K. 2017. Analysis of vulnerabilities, attacks, countermeasures and overall risk of the Automatic Dependent Surveillance-Broadcast (ADS-B) system. *International Journal of Critical Infrastructure Protection,* 19, 16–31.

Nagothu, D., Chen, Y., Blasch, E., Aved, A. & Zhu, S. 2019. Detecting Malicious False Frame Injection Attacks on Surveillance Systems at the Edge Using Electrical Network Frequency Signals. *Sensors,* 19, 2424.

OpenScope 2025. OpenScope Air Traffic Control Simulator. GitHub.

Pierattelli, S., Lamberti, F. & Foti, A. Getting Closer to the ATM Digitalization Through the Future Digital Communication Infrastructure. 2025 Integrated Communications, Navigation and Surveillance Conference (ICNS), 8–10 April 2025 2025. 1–5.

Sabatini, R. Next-generation ATM systems: Increasing safety, efficiency and sustainability of the aviation sector. Second International Symposium on Sustainable Aviation (ISSA 2016). Istanbul, Turkey, 2016.

Smailes, J., Moser, D., Smith, M., Strohmeier, M., Lenders, V. & Martinovic, I. 2021. You talkin' to me? Exploring Practical Attacks on Controller Pilot Data Link Communications. *Proceedings of the 7th ACM on Cyber-Physical System Security Workshop*. Virtual Event, Hong Kong: Association for Computing Machinery.

Tarvainen, M. P., Niskanen, J.-P., Lipponen, J. A., Ranta-Aho, P. O. & Karjalainen, P. A. 2014. Kubios HRV–heart rate variability analysis software. *Computer methods and programs in biomedicine,* 113**,** 210–220.

Thales. 2025. *Aviation sector sees 600% year-on-year increase in cyberattacks*. [Online]. Available: https://www.thalesgroup.com/en/news-centre/press-releases/aviation-sector-sees-600-year-year-increase-cyberattacks [Accessed 24 October 2025].

Tidy, J. & Wilson, T. 2025. *EU cyber agency says airport software held to ransom by criminals* [Online]. BBC. Available: https://www.bbc.com/news/articles/cqjeej85452o [Accessed 24 October 2025].

Ukwandu, E., Ben-Farah, M. A., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C., Andonovic, I. & Bellekens, X. 2022. Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends. *Information,* 13, 146.

Vajrobol, V., Saxena, G. J., Singh, S., Pundir, A., Gupta, B. B., Gaurav, A. & Chui, K. T. 2025. Enhancing aviation control security through ADS-B injection detection using ensemble meta-learning models with Explainable AI. *Alexandria Engineering Journal,* 112**,** 63–73.

Ying, X., Mazer, J., Bernieri, G., Conti, M., Bushnell, L. & Poovendran, R. Detecting ADS-B Spoofing Attacks Using Deep Neural Networks. 2019 IEEE Conference on Communications and Network Security (CNS), 10–12 June 2019 2019. 187–195.