Human Factors in Design, Engineering, and Computing, Vol. 238, 2026, 2689–2697
https://doi.org/10.54941/ahfe1008493

A Bloom's Taxonomy-Based Cybersecurity Training Curriculum for Air Traffic Controllers

Hui Wang

Embry Riddle Aeronautical University, Daytona Beach, FL 32114, USA

ABSTRACT

Advancements in computer technology have improved the efficiency of air traffic management (ATM) systems while introducing new cybersecurity vulnerabilities. Cyberattacks targeting ATM infrastructure may disrupt air traffic control (ATC) services and compromise aviation safety. To strengthen the cybersecurity and resilience of ATM systems, air traffic controllers (ATCOs) need appropriate knowledge and skills to identify and respond to cyber threats. This paper presents a cybersecurity training curriculum designed to enhance ATCOs' cybersecurity awareness and cyber threat identification skills. Guided by Bloom's taxonomy, the proposed curriculum consists of three stages: lecture-based training, simulation-based training, and evaluation. The curriculum follows a sequential learning approach, progressing from foundational cybersecurity knowledge to the practical application of threat identification skills in simulated ATC operations. The instructional design specifies learning outcomes, training activities, and assessment methods to support the development of these competencies. Training effectiveness will be evaluated through pre- and post-training assessments and a follow-up questionnaire. The proposed curriculum provides a structured approach to developing ATCOs' cybersecurity competencies and supporting the resilience of ATM operations.

Keywords: Air traffic management, Cybersecurity training, Cyber threat identification, Cybersecurity awareness, Simulation-based training, Bloom's taxonomy

INTRODUCTION

The increasing integration of computer technology into air traffic management (ATM) has improved the efficiency and capability of air traffic control (ATC) services (Pereira et al., 2022). In particular, initiatives under the Next Generation Air Transportation System have supported faster and more effective communication, greater accuracy and precision in aircraft navigation, and improved workload management for air traffic controllers (ATCOs; Elmarady & Rahouma, 2021). However, the increasing reliance on computer technology also introduces cybersecurity vulnerabilities that malicious actors may exploit to steal data, disrupt operations, or damage system infrastructure (Hird, 2021; Tamimi et al., 2020). Such cyber threats may interrupt ATM operations or terminate ATC services, potentially compromising airspace safety (Elmarady & Rahouma, 2021; Hird, 2021).

Received October 20, 2026; Revised November 20, 2026; Accepted November 30, 2026; Available online December 1, 2026

© 2026 The Authors. This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License.
For more information, see https://creativecommons.org/licenses/by-nc-nd/4.0/

As end users of ATM technologies, ATCOs play an important role in detecting and responding to potential cyber threats. Therefore, there is a need to develop a practical cybersecurity training curriculum that equips ATCOs with the knowledge, skills, and abilities (KSAs) necessary to identify and respond to cyber threats during ATC operations. This paper proposes a cybersecurity training curriculum guided by Bloom's taxonomy that integrates lecture-based instruction, simulation-based training, and evaluation.

ATC CYBERSECURITY

Cyber threats involve malicious activities targeting digital networks to gain unauthorized access, disrupt operations, steal information, or damage software and hardware (Cybersecurity and Infrastructure Security Agency, n.d.). The rapid advancement of computer technology has been accompanied by growing cybersecurity risks. Global cybercrime costs were projected to increase by 15% annually, reaching $10.5 trillion by 2025 compared to $3 trillion in 2015 (INTRUSION Inc., 2020). Cyber threats can result in equipment malfunctions, information theft, and data breaches (Elmarady & Rahouma, 2021). Similar threats pose significant risks to ATM systems. For example, a cybersecurity incident in Alaska in 2006 reportedly compromised system integrity and resulted in a complete system shutdown (Center for Strategic and International Studies, 2024). Since then, ATM systems have continued to face cybersecurity threats.

As ATM systems increasingly rely on advanced technologies to accommodate growing air traffic demands, the integration of digital technologies into communication, navigation, and surveillance (CNS) systems also introduces cybersecurity vulnerabilities (Hird, 2021). For example, controller–pilot data link communications (CPDLC) may be vulnerable to unauthorized modification or deletion of messages exchanged between ATCOs and pilots. Similarly, automatic dependent surveillance–broadcast (ADS-B) supports accurate and timely aircraft surveillance, but its signals may be vulnerable to spoofing, allowing malicious actors to impersonate aircraft or transmit misleading surveillance information (Elmarady & Rahouma, 2021).

The increasing availability of software-defined radios (SDRs) may further facilitate the exploitation of vulnerabilities in CNS systems that rely on wireless signals. Malicious actors may exploit these vulnerabilities through malware injection, false data transmission, spoofing, or eavesdropping (Elmarady & Rahouma, 2021). Such attacks may lead to air traffic congestion, flight delays, disruptions to aircraft control services, and financial losses, potentially compromising aviation safety (Hird, 2021). Recognizing these risks, government agencies and aviation organizations have emphasized the importance of strengthening cybersecurity measures in ATM systems (Federal Aviation Administration [FAA], 2022; Hird, 2021).

Beyond technical safeguards, such as antivirus software and firewalls, cybersecurity education and training are important approaches to strengthening cybersecurity preparedness (AlDaajeh et al., 2022). Although the importance of cybersecurity training has been recognized, a formal and comprehensive training program specifically addressing ATCO cybersecurity

awareness remains a need. Cybersecurity-focused training can provide ATCOs with the KSAs to recognize potential cyber threats and apply appropriate response strategies during ATC operations (Wang & Schultz, 2025).

Bloom's Taxonomy

The acquisition of KSAs occurs through education and practice (Aguinis & Kraiger, 2009; Salas et al., 2012). Learning objectives are often organized hierarchically, progressing from simple to more complex cognitive processes (Anderson, 2005). Foundational knowledge supports the development of higher-order cognitive skills (Granello, 2001). Bloom's taxonomy is a widely recognized framework for classifying educational objectives according to their cognitive complexity. The revised taxonomy consists of six levels: remembering, understanding, applying, analyzing, evaluating, and creating (Anderson & Krathwohl, 2001; Bloom et al., 1956).

Bloom's taxonomy provides a hierarchical approach to learning, in which cognitive processes range from acquiring foundational knowledge to applying and integrating knowledge in more complex tasks (Anderson & Krathwohl, 2001). At the remembering level, learners recall previously acquired information, such as memorizing the steps required to start a car, without necessarily understanding the underlying processes (Ullah et al., 2020). Understanding involves interpreting information and connecting it with existing knowledge to develop a mental model of how a system operates (Ullah et al., 2020). A well-developed mental model supports comprehension and effective task performance (Dattel, Goodwin, et al., 2022; Durso et al., 2007). At the applying level, learners use acquired knowledge in practical situations, while analyzing involves examining information and identifying relationships among its components (Ullah et al., 2020). At higher cognitive levels, learners evaluate information and actions based on established criteria and integrate knowledge to develop new solutions (Dattel, Babin, et al., 2022).

Bloom's taxonomy has been widely applied in education to guide instructional design, develop learning activities, and assess cognitive achievement and learning effectiveness across various disciplines (Rahman & Manaf, 2017; Ramirez, 2017). Ramirez (2017) examined its application in personality assessment education and highlighted its usefulness in developing instructional materials with appropriate levels of cognitive difficulty. The framework also supports the assessment of learning outcomes across different cognitive levels, allowing instructors to evaluate learners' progress toward more complex learning objectives. Similarly, Saxena et al. (2021) proposed applying Bloom's taxonomy to character education to support instructional design and knowledge acquisition. Furthermore, Bloom's taxonomy has been used to support the development of higher-order thinking skills, including critical thinking and creativity (Rahman & Manaf, 2017).

An important application of Bloom's taxonomy is the use of action verbs associated with each cognitive level to establish observable and measurable learning objectives (Anderson & Krathwohl, 2001; Bloom et al., 1956). These verbs describe actions that learners can demonstrate to reflect their cognitive achievement. By selecting appropriate action verbs, instructors can

specify what learners are expected to accomplish and develop corresponding assessments to determine whether the learning objectives have been achieved. Blicker (2005) emphasized the importance of assessing learning outcomes throughout the instructional process to support learning effectiveness. Educational institutions have adopted Bloom's taxonomy action verbs to guide lesson planning, instructional design, and assessment development (Iowa State University, 2023; Shabatura, 2022; University of Toronto, 2024). However, instructors should select verbs that accurately reflect the intended learning objectives rather than attempting to incorporate all available verbs into a single instructional activity.

In aviation education, the FAA has established a framework known as the basic levels of learning, which reflects a similar progression in cognitive complexity (FAA, 2020). The framework identifies four levels: rote, understanding, application, and correlation. At the correlation level, learners connect previously acquired knowledge and skills with new situations or tasks (FAA, 2020). For example, an ATCO who has reached the correlation level in learning go-around procedures can relate these procedures to the coordination required when an aircraft discontinues an approach. As learners develop and integrate their KSAs, they may gain a deeper understanding of the subject matter and improve their ability to retain and apply acquired knowledge and skills in future operational tasks (Dattel, Babin, et al., 2022; Noe et al., 2014; Ramirez, 2017).

ATC Training

Training is a widely used approach to developing the KSAs required for job performance (Salas & Cannon-Bowers, 2001). Effective training requires appropriate instructional methods, activities, and assessments to support the development of intended KSAs (Salas et al., 2012). In ATC, training is a mandatory component of ATCO qualification, preparing trainees to manage air traffic safely and efficiently (Hopkin, 1995). In addition to traditional classroom instruction, simulation has become an integral part of ATC training, providing opportunities to develop and practice operational skills (Coyne et al., 2017).

Simulation-based training bridges the gap between classroom instruction and operational practice by allowing trainees to apply knowledge and develop skills, such as problem-solving, critical thinking, and decision-making, in realistic scenarios (Mauro & Barshi, 2007; Simonson et al., 2023). It provides a safe and controlled environment where trainees can practice operational tasks without the risks associated with real-world errors (Foster et al., 2023). Simulation also allows instructors to introduce predefined conditions, such as adverse weather, equipment failures, and traffic conflicts, to facilitate repeated practice and standardized training (Coyne et al., 2017; Foster et al., 2023). These opportunities may support the transfer of acquired KSAs to operational settings (Noe et al., 2014).

In addition, classroom lectures, discussions, and other instructional activities can complement simulation by providing foundational knowledge and promoting engagement with training content (Jentsch & Curtis, 2017).

Combining these instructional approaches allows trainees to acquire knowledge through classroom instruction and reinforce their learning through practical application, supporting knowledge retention and the development of job-related KSAs (Salas et al., 2012).

TRAINING CURRICULUM DEVELOPMENT

To address the need for ATCO cybersecurity training, the proposed curriculum uses Bloom's taxonomy as a framework for organizing learning objectives, instructional activities, and assessments. The framework supports a progression from foundational cybersecurity knowledge to its practical application in simulated ATC operations (Ramirez, 2017). Bloom's taxonomy informs the curriculum design in three ways. First, instructional activities are organized to support the progressive development of KSAs, beginning with foundational cybersecurity knowledge before applying it in simulation exercises. Second, action verbs associated with different cognitive levels help establish specific and measurable learning outcomes and corresponding assessments. For example, trainees may demonstrate their ability to identify cyber threats while managing air traffic in simulated scenarios. Third, instructional methods are selected to support the intended learning outcomes. Accordingly, lecture-based training introduces fundamental cybersecurity concepts, while simulation-based training provides opportunities to apply acquired knowledge to cyber threat identification and response.

The proposed curriculum aims to enhance ATCOs' cybersecurity awareness and develop their ability to identify and respond to cyber threats. Seven learning outcomes are established to guide the development of instructional activities and assessments. Upon completing the training, ATCOs should be able to:

1. Explain the importance of cybersecurity in ATM systems;
2. Recognize the impact of cyber incidents on air traffic safety and efficiency;
3. Explain common cybersecurity vulnerabilities in ATC systems;
4. Identify potential cyber threats and vulnerabilities relevant to ATC systems, such as data breaches, malware attacks, and unauthorized access;
5. Practice responding to cyber threats through simulated exercises in a controlled environment;
6. Demonstrate the ability to detect and respond to cyber threats;
7. Evaluate the effectiveness of actions taken to address cybersecurity issues.

The curriculum consists of three phases: lecture-based training, simulation-based training, and evaluation. These phases are conducted over three consecutive days, with one phase completed each day. The first phase consists of two hours of classroom instruction using multimedia materials, including printed materials, PowerPoint presentations, and videos, supplemented by instructional activities. The second phase involves two hours of training using ATC simulation systems appropriate to the trainees' assigned ATC environment. The instructor first demonstrates how to identify cyber threats in

simulated ATC scenarios. Trainees then manage air traffic in three predefined scenarios incorporating cyber threats under the instructor's supervision and guidance. The third phase consists of a one-hour evaluation session involving three ATC simulation scenarios. The instructor assesses trainees' performance and provides oral feedback after each scenario, followed by opportunities for trainees to reflect on their performance.

Aligning instructional methods and assessments with the intended learning outcomes is important for evaluating training effectiveness. Bloom's taxonomy provides a framework for selecting appropriate instructional activities and developing assessments that reflect different cognitive levels. By incorporating measurable action verbs, instructors can evaluate whether trainees have achieved the intended learning outcomes. Table 1 summarizes the relationships among the training phases, cognitive levels, action verbs, corresponding assessments, and learning outcomes (LOs).

Table 1: Connections between elements in the training curriculum.

Training Phase	Bloom's Taxonomy	Action Verb	Assessment	Learning Outcome
Lecture-based	Remember Understand	• Recognize potential cybersecurity vulnerabilities in ATM system • Describe the impacts of cyber threats on the ATM system • Explain the cyber threat detection techniques	• Participation • Written quiz on the basics of cybersecurity and detection techniques	LO1 LO2 LO3
Simulation-based	Apply Analyze	• Identify suspicious activities • Apply cyber threat detection technique • Manage air traffic accordingly	• Record of successfully identified cyber threats • Overall performance and disruption of managing air traffic	LO4 LO5
Evaluation	Evaluate Create	• Assess the knowledge application • Generalize effective resolution	• Performance improvement assessment • Self-reflection	LO6 LO7

Training effectiveness can be evaluated using pretest–posttest assessments and a post-training follow-up questionnaire. The pretest and posttest will each include a knowledge test and an ATC simulation with embedded cyber threats to evaluate changes in cybersecurity knowledge, threat identification, and ATC performance. Different but comparable questions and simulation scenarios should be used to minimize potential learning effects. Additionally, a post-training follow-up questionnaire will assess trainees' reported retention and application of acquired KSAs in operational settings and identify opportunities for curriculum improvement (Centers for Disease Control and Prevention, 2023).

CONCLUSION

This paper proposes a cybersecurity training curriculum for ATCOs guided by Bloom's taxonomy. The framework provides a structured approach to aligning learning objectives, instructional activities, and assessments to support the development of cybersecurity awareness and cyber threat identification skills. By integrating lecture-based instruction with simulation-based exercises, the curriculum allows trainees to acquire foundational cybersecurity knowledge and apply it in simulated ATC operations. The proposed evaluation methods will provide opportunities to assess training effectiveness and identify areas for improvement. As cybersecurity threats continue to evolve, this curriculum offers a structured approach to preparing ATCOs to recognize and respond to potential cyber threats, ultimately supporting the cybersecurity and resilience of ATM operations.

REFERENCES

Aguinis, H., & Kraiger, K. (2009). Benefits of training and development for individuals and teams, organizations, and society. *Annual Review of Psychology, 60*, 451–474. https://doi.org/10.1146/annurev.psych.60.110707.163505

AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Choo, K.-K. R. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers & Security, 119*, Article 102754. https://doi.org/10.1016/j.cose.2022.102754

Anderson, L. W. (2005). Objectives, evaluation, and the improvement of education. *Studies in Educational Evaluation, 31*(2), 102–113. https://doi.org/10.1016/j.stueduc.2005.05.004

Anderson, L. W., & Krathwohl, D. R. (Eds.). (2001). *A taxonomy for learning, teaching, and assessing: A revision of Bloom's taxonomy of educational objectives*. Longman.

Blicker, L. (2005). Evaluating quality in the online classroom. In C. Howard, P. L. Rogers, & G. A. Berg (Eds.), *Encyclopedia of distance learning* (pp. 2429–2433). IGI Global. https://doi.org/10.4018/978-1-59140-555-9.ch127

Bloom, B. S., Engelhart, M. D., Furst, E. J., Hill, W. H., & Krathwohl, D. R. (1956). *Taxonomy of educational objectives: The classification of educational goals. Handbook I: Cognitive domain*. David McKay.

Center for Strategic and International Studies. (2024). *Significant cyber incidents*. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Centers for Disease Control and Prevention. (2023). *Training effectiveness*. https://www.cdc.gov/training/development/evaluate/training-effectiveness.html

Coyne, W., Rice, S. C., Winter, S., Tamilselvan, G., & Drechsel, P. V. (2017). Simulation challenges: Student perception of air traffic control simulation. *International Journal of Aviation, Aeronautics, and Aerospace, 4*(3). https://doi.org/10.15394/ijaaa.2017.1088

Cybersecurity and Infrastructure Security Agency. (n.d.). *Cyber threat source descriptions*. https://www.cisa.gov/uscert/ics/content/cyber-threat-source-descriptions

Dattel, A. R., Babin, A. K., & Wang, H. (2022). Human factors of flight training and simulation. In J. R. Keebler, E. H. Lazzara, K. A. Wilson, & E. L. Blickensderfer (Eds.), *Human factors in aviation* (3rd ed.). Elsevier.

Dattel, A. R., Goodwin, T., Brodeen, H., Friedenzohn, D., Ochoa, O., Wang, H., Gao, P., Haris, S., & Parkar, I. (2022). Using virtual reality for training to identify cyber threats in the bridge of a ship. *Proceedings of the Human Factors and Ergonomics Society 66th Annual Meeting*.

Durso, F. T., Rawson, K. A., & Girotto, S. (2007). Comprehension and situation awareness. In F. T. Durso, R. S. Nickerson, S. T. Dumais, S. Lewandowsky, & T. J. Perfect (Eds.), *Handbook of applied cognition* (2nd ed., pp. 163–193). Wiley. https://doi.org/10.1002/9780470713181.ch7

Elmarady, A. A., & Rahouma, K. (2021). Studying cybersecurity in civil aviation, including developing and applying aviation cybersecurity risk assessment. *IEEE Access, 9*, 143997–144016. https://doi.org/10.1109/ACCESS.2021.3121230

Federal Aviation Administration. (2020). *Aviation instructor's handbook* (FAA-H-8083-9B). U.S. Department of Transportation. https://www.faa.gov/regulations_policies/handbooks_manuals/aviation/aviation_instructors_handbook

Federal Aviation Administration. (2022, October). *DOT 2022 cybersecurity symposium – keynote*. U.S. Department of Transportation. https://www.faa.gov/speeches/dot-2022-cybersecurity-symposium-keynote

Foster, T. C., Moroney, W. F., Phillips, H. L., IV, & Lilienthal, M. G. (2023). Human factors in simulation and training: An overview. In D. A. Vincenzi, M. Moloua, P. A. Hancock, J. A. Pharmer, & J. C. Ferraro (Eds.), *Human factors in simulation and training*. Taylor & Francis.

Granello, D. H. (2001). Promoting cognitive complexity in graduate written work: Using Bloom's taxonomy as a pedagogical tool to improve literature reviews. *Counselor Education and Supervision, 40*, 292–307. https://doi.org/10.1002/j.1556-6978.2001.tb01261.x

Hird, J. (2021). *Air traffic management: A cybersecurity challenge*. EUROCONTROL. https://www.eurocontrol.int/sites/default/files/2021-12/eurocontrol-atm-cybersecurity-report.pdf

Hopkin, V. D. (1995). *Human factors in air traffic control*. Taylor & Francis.

INTRUSION Inc. (2020, November 18). *Cybercrime to cost the world $10.5 trillion annually by 2025*. https://www.globenewswire.com/news-release/2020/11/18/2129432/0/en/Cybercrime-To-Cost-The-World-10-5-Trillion-Annually-By-2025.html

Iowa State University. (2023). *Revised Bloom's taxonomy*. Center for Excellence in Learning and Teaching. https://www.celt.iastate.edu/instructional-strategies/effective-teaching-practices/revised-blooms-taxonomy/

Jentsch, F., & Curtis, M. (2017). *Simulation in aviation training*. Routledge.

Mauro, R., & Barshi, I. (2007). Effective computer-based training in aviation: An evaluation of the NASA in-flight icing program. In *Proceedings of the 2007 International Symposium on Aviation Psychology* (pp. 426–431). https://corescholar.libraries.wright.edu/isap_2007/63

Noe, R. A., Clarke, A. D. M., & Klein, H. J. (2014). Learning in the twenty-first-century workplace. *Annual Review of Organizational Psychology and Organizational Behavior, 1*(1), 245–275. https://doi.org/10.1146/annurev-orgpsych-031413-091321

Pereira, B. A., Lohmann, G., & Houghton, L. (2022). Technology trajectory in aviation: Innovations leading to value creation (2000–2019). *International Journal of Innovation Studies, 6*(3), 128–141. https://doi.org/10.1016/j.ijis.2022.05.001

Rahman, S. A., & Manaf, N. F. A. (2017). A critical analysis of Bloom's taxonomy in teaching creative and critical thinking skills in Malaysia through English literature. *English Language Teaching, 10*(9), 245–256. https://doi.org/10.5539/elt.v10n9p245

Ramirez, T. V. (2017). On pedagogy of personality assessment: Application of Bloom's taxonomy of educational objectives. *Journal of Personality Assessment, 99*(2), 146–152. https://doi.org/10.1080/00223891.2016.1167059

Salas, E., & Cannon-Bowers, J. A. (2001). The science of training: A decade of progress. *Annual Review of Psychology, 52*(1), 471–499. https://doi.org/10.1146/annurev.psych.52.1.471

Salas, E., Tannenbaum, S. I., Kraiger, K., & Smith-Jentsch, K. A. (2012). The science of training and development in organizations: What matters in practice. *Psychological Science in the Public Interest, 13*(2), 74–101. https://doi.org/10.1177/1529100612436661

Saxena, R., Agarwal, C., & Ganguly, S. (2021). Application of the Blooms taxonomy model of teaching and learning in character education for designing effective program. *Academy of Marketing Studies Journal, 25*(6), 1–12.

Shabatura, J. (2022, July). *Using Bloom's taxonomy to write effective learning outcomes*. University of Arkansas. https://tips.uark.edu/using-blooms-taxonomy/

Simonson, R. J., Williams, K. N., Keebler, J. R., & Lazzara, E. H. (2023). Simulation-based training for decision-making. In D. A. Vincenzi, M. Moloua, P. A. Hancock, J. A. Pharmer, & J. C. Ferraro (Eds.), *Human factors in simulation and training*. Taylor & Francis.

Tamimi, A., Hahn, A., & Roy, S. (2020). Cyber threat impact analysis to air traffic flows through dynamic queue networks. *ACM Transactions on Cyber-Physical Systems, 4*(3), 1–22. https://doi.org/10.1145/3377425

Ullah, Z., Lajis, A., Jamjoom, M., Altalhi, A., & Saleem, F. (2020). Bloom's taxonomy: A beneficial tool for learning and assessing students' competency levels in computer programming using empirical analysis. *Computer Applications in Engineering Education, 28*(6), 1628–1640. https://doi.org/10.1002/cae.22339

University of Toronto. (2024). *Active verbs for Bloom's revised taxonomy*. Centre for Teaching Support & Innovation. https://teaching.utoronto.ca/resources/active-verbs-for-blooms-revised-taxonomy/

Wang, H., & Schultz, N. R. (2025). Investigating human factors engineering integration in ATC cybersecurity resilience. *Human Factors in Cybersecurity, 168*, 100–110. https://doi.org/10.54941/ahfe1006147