RAIS Journal for Social Sciences | Vol. 10, No. 2, 2026
ISSN 2574-0245 (Print) | ISSN 2574-1179 (Online) | DOI:10.5281/zenodo.24454406

Squawk 7500 in the Digital Sky:
The Convergence of Cyberspace, Cyber Diplomacy, Cyberwar, and Cyber Terrorism in Civil Aviation, 2024–2026

Sharon L. Burton

College of Aviation, Embry-Riddle Aeronautical University, Daytona Beach, FL, USA
burtons6@erau.edu

Abstract: Between December 2024 and October 2026, civil aviation became a setting in which cyberspace, cyber diplomacy, cyberwar, and cyber terrorism converged. On December 25, 2024, Azerbaijan Airlines Flight 8243 crashed in Kazakhstan after Russian air-defense missiles detonated nearby, killing 38 people. In 2025, ransomware disabled shared check-in software at European airports, and pro-Ukrainian hackers forced Aeroflot to cancel flights. Intruders also broadcast pro-Hamas messages over airport public address systems. The International Civil Aviation Organization (ICAO) Assembly then condemned the Russian Federation and the Democratic People's Republic of Korea for satellite-navigation interference. By 2026, the International Air Transport Association (IATA) reported more than 71,000 interference cases, and European regulators proposed mandated crew training. This qualitative document analysis examines these events through Reason's Swiss cheese model and Nonaka's knowledge-creation theory. Six findings emerged. Gray-zone electronic and cyber activity reaches civilians far from conflict zones, and diplomatic responses remain slow and lack enforcement. Third-party digital dependencies concentrate risk, and propaganda intrusions target public trust rather than aircraft. Human operators limited harm in the events examined, whereas cross-border knowledge sharing was the weakest layer. This article argues that aviation leaders should treat cyber resilience as a workforce discipline grounded in human factors and knowledge management rather than as a purely technical problem.

Keywords: Aviation Cybersecurity, Cyber Diplomacy, Cyberwar, Cyber Terrorism, GNSS Interference, Human Factors, Training, Knowledge Management

Introduction

Civil aviation has long relied on a silent signal for an aircraft under seizure. In controller usage, to squawk is to set the aircraft transponder to a code that air traffic control requests (Federal Aviation Administration [FAA], 2026, Pilot/Controller Glossary). Code 7500 means "I am being hijacked/forced to a new destination," and controllers will not issue it unless a pilot has first reported unlawful interference (FAA, 2026, Section 6-3-4). The title of this article borrows that signal. Each event examined here involved a comparable seizure of the systems on which aviation depends, as navigation signals, check-in software, and terminal loudspeakers were taken over without anyone boarding an aircraft. Nobles (2017) attributed rising cyber risk in civil aviation to dense system interconnection and missing common security frameworks, and he identified workforce education as one route to stronger defense. Five years later, Nobles et al. (2022) argued that weak international cyber governance impedes enforcement. Events between 2024 and 2026 turned those warnings into documented operational realities.

The significance of this article rests on verifiable national and international events. A passenger jet was lost in war-adjacent airspace (Faulconbridge & Papachristou, 2025), and satellite-navigation interference affected the aircraft carrying the European Commission President (Reuters, 2025b). Ransomware against a single supplier disrupted check-in at major European hubs (Scroxton, 2025), and intruders used airport loudspeakers, including at Harrisburg International Airport in Pennsylvania, to broadcast political propaganda (Catchpole, 2025). The Assembly of the International Civil Aviation Organization (ICAO) then formally condemned two states for interference with civil aviation (ICAO, 2025). Together, the events reveal that the four domains now operate within one aviation ecosystem, and that convergence defines the purpose of this article.

This article examines that convergence. It addresses one research question: How did cyberspace, cyber diplomacy, cyberwar, and cyber terrorism converge in civil aviation between 2024 and 2026, and what lessons do human factors, training, and knowledge management offer aviation leaders? Its analysis draws on human factors scholarship (Burton et al., 2023; Nobles, 2022; Nobles & McAndrew, 2023) and on training and workforce development scholarship (Burrell, 2024; Burton, 2021, 2025; Merritt et al., 2024). Knowledge management scholarship (Dodla & Jones, 2023a, 2023b; Jones, 2020) informs the analysis as well. It also incorporates critical-infrastructure and cyber terrorism research (Bhambri & Khang, 2026; Dawson et al., 2021). Cyber diplomacy and cyberwar scholarship (Libicki, 2026; Radanliev, 2025; Willers & Gjesvik, 2026) and forensic cyberpsychology (Ohu & Jones, 2025a, 2025b) complete that foundation. The Background section documents those events.

Background

Cyberwar Reaches the Passenger Cabin

The crash of Azerbaijan Airlines Flight 8243 demonstrates how armed conflict can reach civilian aircraft beyond a war zone. On December 25, 2024, the Baku-to-Grozny flight crash-landed near Aktau, Kazakhstan, after diverting from southern Russia during reported drone attacks. Thirty-eight people died (Faulconbridge & Papachristou, 2025). The preliminary Kazakh report of February 4, 2025, recorded external metal fragments in the tail stabilizer and hydraulic system without identifying their origin (Reuters, 2025a). Assigning responsibility thus fell to governments.

Diplomatic acknowledgment followed the technical findings. On October 9, 2025, President Putin told President Aliyev that two Russian air-defense missiles had detonated near the aircraft (Faulconbridge & Papachristou, 2025). Six months later, on April 15, 2026, the two foreign ministries announced a compensation settlement. It covered a crash "resulting from the unintended operation of an air defense system in the airspace of the Russian Federation" (Ministry of Foreign Affairs of the Republic of Azerbaijan, 2026, para. 1). The sequence illustrates why Nobles et al. (2022) described commercial aviation as international critical infrastructure. Kinetic conflict, however, is only one channel of war.

Interference With Navigation Signals

Interference with Global Navigation Satellite Systems (GNSS) became persistent gray-zone pressure on civil aviation. On August 31, 2025, the Global Positioning System (GPS) on the aircraft carrying European Commission President Ursula von der Leyen was jammed on approach to Plovdiv, Bulgaria. Controllers switched to ground-based navigation systems, and Bulgarian authorities attributed the jamming to Russian interference (Reuters, 2025b). Days later, Bulgaria's prime minister told parliament that no sustained jamming had occurred, while not ruling out an onboard signal anomaly (Nilsson-Julien & Jones, 2025). The reversal shows that electromagnetic attribution remains contested.

ICAO responded through two of its organs, the Council and the Assembly. On October 3, 2025, the ICAO Assembly endorsed a Council determination about recurring interference from the Democratic People's Republic of Korea (DPRK) and the Russian Federation. The Council had found that this interference infringed the Convention on International Civil Aviation, known as the Chicago Convention (ICAO, 2025). These actions show that cyber diplomacy was active but lacked enforcement. Industry bodies then sought to fill that gap through operational measures.

Regulators and industry converted concern into measurement. In June 2025, the European Union Aviation Safety Agency (EASA) and the International Air Transport Association (IATA) published a joint plan calling for standardized interference reporting and tighter controls on jamming devices. Its data also showed a 220% increase in GPS signal-loss events between 2021 and 2024 (IATA, 2025). IATA (2026) later cited more than 71,000 recorded interference cases and 2.1 million GPS signal losses. The call for standardized reporting (IATA, 2025) indicates that reporting practices still varied across operators and regions. These figures indicate systemic exposure extending to airport systems.

Cyberspace Dependencies and Proxy Conflict

Shared software platforms concentrate the consequences of a single compromise. In September 2025, ransomware affecting the Multi-User System Environment (MUSE) check-in software of Collins Aerospace forced Heathrow, Brussels, Berlin Brandenburg, and Dublin airports onto manual check-in. The European Union Agency for Cybersecurity traced the disruption to ransomware at an outside supplier (Scroxton, 2025). Verizon (2025) found that the share of breaches involving a third party doubled from 15% to 30% in its 2025 data set, so the Collins case reflects a wider pattern. Airport resilience thus depends on suppliers beyond airport control. Supply chains, however, are not the only digital route to passengers.

Hacktivism can also serve as a proxy for interstate conflict. In July 2025, the pro-Ukrainian group Silent Crow and Belarusian Cyber Partisans claimed an attack that forced Aeroflot to cancel more than 40 flights (Gozzi & Tidy, 2025). The attackers struck a state-linked carrier rather than military systems, and passengers absorbed the disruption. Intruders repeated that pattern months later when they seized airport loudspeakers.

Propaganda Through Airport Infrastructure

Airport public address systems, the loudspeakers used for terminal announcements, became channels for political propaganda in October 2025. On October 14, intruders took over these systems at three Canadian airports and at Harrisburg International Airport in Pennsylvania, broadcasting messages praising Hamas (Catchpole, 2025). The messages also appeared on terminal display screens at Kelowna International Airport (DiMella & Norman, 2025; Goillandeau, 2025). At Harrisburg, a recording that named a self-described Turkish hacker and voiced pro-Palestinian slogans played for about 10 minutes. Airport officials stated that the political message contained no threats, and the public address system was shut off (DiMella & Norman, 2025; Goillandeau, 2025). These intrusions fit the description by Ohu and Jones (2025a) of cyberwarfare as disinformation and psychological operations conducted digitally.

Research Method and Design

This article used qualitative document analysis, a structured method for examining and interpreting printed and electronic records (Bowen, 2009). Primary records came from ICAO, IATA, EASA, the European Organisation for the Safety of Air Navigation (EUROCONTROL), and national governments (EASA & EUROCONTROL, 2026; IATA, 2026; ICAO, 2025). Established news organizations and peer-reviewed scholarship on aviation cybersecurity, human factors, training, and knowledge management supplied the remaining sources. Events were included if they occurred between December 2024 and October 2026, affected civil aviation, and appeared in at least one primary record or

established news report. Material documented only in blogs or social media was excluded, because Bowen (2009) advises researchers to assess the authenticity and credibility of each document.

Each event was coded against the four domains in the Key Terms and Definitions and against three human dimensions: performance, training, and knowledge flow (Nonaka, 1994; Reason, 2000). The final corpus comprised 53 sources, including eight institutional records from ICAO, IATA, the Latin American and Caribbean Air Transport Association (ALTA), EASA and EUROCONTROL, the FAA, and the Azerbaijani foreign ministry. Ten news reports from Reuters, BBC News, CNN, Euronews, Computer Weekly, and Fox News, one industry breach report (Verizon, 2025), five government standards and statements, and 29 scholarly works completed the corpus. The coding results were recorded in an event-by-domain matrix, presented as Table 1. Figure 1 places the coded events on a timeline, and the assumptions underlying this design follow.

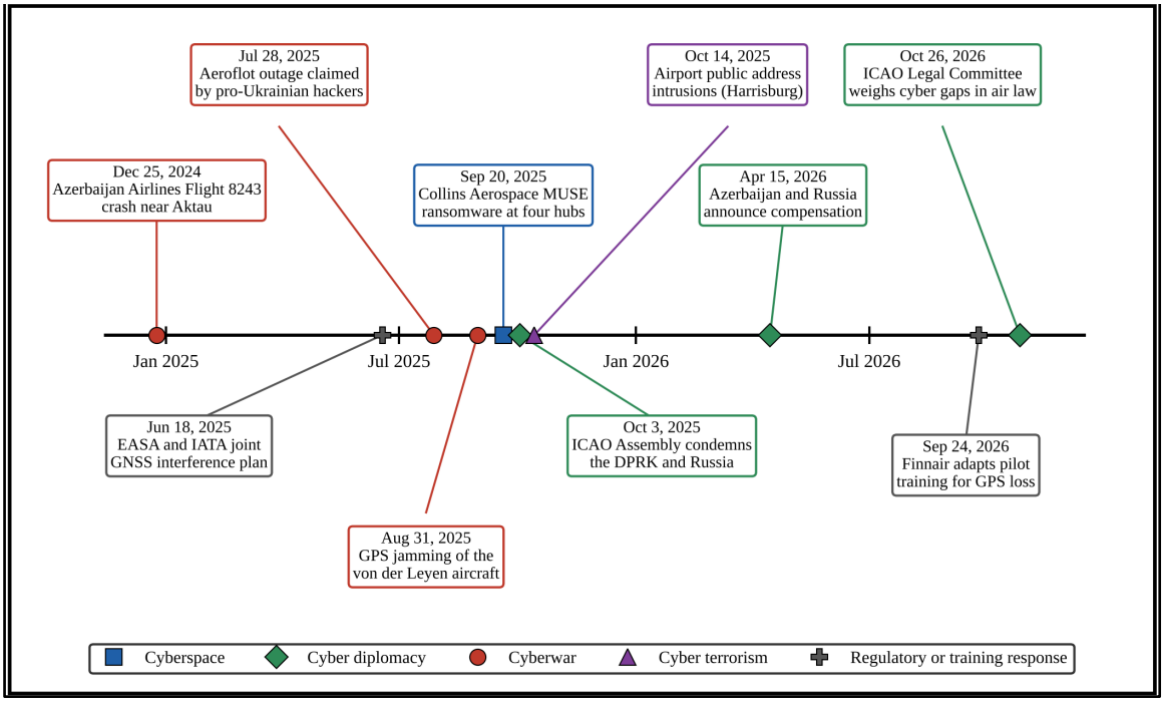

Figure 1. Timeline of Principal Civil Aviation Cyber Events, December 2024–October 2026

Note. Created by the author based on Catchpole (2025); DiMella and Norman (2025); Faulconbridge and Papachristou (2025); Goillandeau (2025); Gozzi and Tidy (2025); IATA (2025); ICAO (2025, 2026); Lo Nostro (2026); Ministry of Foreign Affairs of the Republic of Azerbaijan (2026); Reuters (2025b); and Scroxton (2025). Marker shape and color show the primary domain of each event.

Assumptions, Limitations, and Delimitations

Assumptions

This article rests on seven assumptions, the first three of which concern sources and categories. First, it assumes that the institutional documents examined accurately represent the positions of ICAO, IATA, EASA, and EUROCONTROL at the time of publication (EASA & EUROCONTROL, 2026; IATA, 2026; ICAO, 2025). Second, it assumes that established news organizations reported facts in good faith and corrected errors when identified. These organizations include Reuters, the BBC, CNN, and Fox News (DiMella & Norman, 2025; Goillandeau, 2025; Gozzi & Tidy, 2025; Reuters, 2025b). Third, it assumes that the four domains can be distinguished analytically even when they overlap in practice. Satellite-navigation interference near a conflict zone, for example, is simultaneously an act within cyberspace, an instrument of conflict, and a subject of diplomacy (ICAO, 2025). These assumptions establish the evidentiary base on which the human-centered assumptions rest.

The remaining four assumptions concern people and organizations. Fourth, this article assumes that human operators, including pilots, air traffic controllers, airport staff, and security personnel, remain the final layer of defense. Burrell (2024) supports this assumption, concluding that human mistakes remain the leading source of cybersecurity incidents. Fifth, it assumes that training can change operational outcomes. Finnair reported that it now prepares its pilots for airspace with routine GPS interference (Lo Nostro, 2026), and EASA and EUROCONTROL (2026) proposed mandatory crew and controller training. Sixth, it assumes that performance, training, and knowledge flow are interdependent rather than separate concerns, a relationship reflected in the view of Burton (2021) that knowledge drives human capital development. Seventh, it assumes that the reported events represent broader patterns rather than isolated anomalies, which the multiyear IATA (2025, 2026) data support for navigation interference. If any assumption proves incorrect, the interpretations in this article would require revision. The limitations below describe that risk.

Limitations

Nine limitations bound the findings, beginning with the nature of the evidence. First, this article relies on publicly available documents. Classified intelligence and confidential safety files were inaccessible, so the analysis cannot confirm technical causes beyond official disclosures (Reuters, 2025a). Second, Bowen (2009) warns that documents may lack detail or reflect biased selection, and public aviation reporting shares those weaknesses. Third, attribution in cyberspace is contested. The later Bulgarian statement on the Plovdiv incident (Nilsson-Julien & Jones, 2025) and the unverified self-identification in the Harrisburg recording (DiMella & Norman, 2025) illustrate how early claims can shift. These evidentiary constraints shape how firmly any conclusion can be stated.

Additional limitations arise from timing and measurement. Fourth, some matters remained unresolved at the time of writing, including the final technical report on Flight 8243, because the published Kazakh findings were preliminary (Reuters, 2025a). Fifth, aggregate figures such as the IATA (2026) count of more than 71,000 interference cases depend on voluntary reporting. The 2025 EASA and IATA plan sought to standardize that reporting (IATA, 2025), so actual totals may differ. Sixth, coverage depth varies. The Collins Aerospace incident is documented through a statement from a European Union agency (Scroxton, 2025), whereas the Harrisburg details rest on news reports of airport statements (DiMella & Norman, 2025; Goillandeau, 2025). Findings thus carry unequal weight across cases.

The final limitations concern design and perspective. Seventh, this article is qualitative and interpretive, treating documents as data for interpretation rather than as measures of causal effect (Bowen, 2009), and its findings are not statistically generalizable. Eighth, this article did not include interviews with pilots, controllers, or airport security staff, so their lived experience is inferred from documents rather than captured directly. Gontar et al. (2018) addressed that gap experimentally for pilots facing cyberattacks. Ninth, the author' professional backgrounds may shape interpretation, a risk mitigated by citing each claim. These boundaries differ from the deliberate scope choices described under Delimitations.

Delimitations

The author narrowed the scope of this article through seven deliberate choices, the first two of which concern sector and time. First, this article is limited to civil aviation, comprising airlines, airports, air navigation service providers, and their suppliers. Military aviation and space launch are excluded, although Dawson and Khan (2025) list navigation among space-system functions exposed to cyberattack. Second, the time frame extends from December 2024 through October 2026, a window spanning the Flight 8243 crash, the ICAO condemnation, and the 2026 regulatory responses (EASA & EUROCONTROL, 2026; ICAO, 2025). This window balances recency against documented outcomes.

The next three choices concern concepts and theory. Third, this article examines four domains and three human dimensions, following the workforce emphasis of Nobles (2017); economic loss, insurance, and legal liability fall outside its scope. Fourth, this article applies two theoretical frameworks: the Swiss cheese model of Reason (2000) and the knowledge-creation theory of Nonaka (1994). Nonaka's theory is organized around socialization, externalization, combination, and internalization (SECI), and systems-theoretic alternatives (Leveson, 2011) appear only in the critique. Fifth, this article treats cyberwar and cyber terrorism as analytic categories rather than legal findings, consistent with the argument by Libicki (2026) that designating cyber operations as war is a political judgment. Events are called terror-adjacent when digital means carried ideological messages (Catchpole, 2025). These conceptual choices keep the analysis focused on human and organizational questions.

The final two choices concern sources. Sixth, only English-language sources were analyzed, so regional reporting may be underrepresented, although official English-language Azerbaijani government statements were included (Ministry of Foreign Affairs of the Republic of Azerbaijan, 2026). Seventh, scholarly sources were drawn from human factors, training, knowledge management, critical infrastructure, and forensic cyberpsychology (Dodla & Jones, 2023a; Nobles, 2022; Ohu & Jones, 2025a). Engineering remedies such as receiver hardening are acknowledged but not evaluated. This scope is narrow enough for actionable guidance yet broad enough to show an international pattern.

Theoretical Framework

Framework One: Reason's Swiss Cheese Model of Accident Causation

The Swiss cheese model describes how organizational defenses fail. Reason (2000) proposed that complex organizations protect against hazards through successive layers, including technology, procedures, training, and supervision, each of which contains weaknesses, or holes. Holes arise from active failures by front-line operators and from latent conditions created by design, management, and regulatory decisions, and an accident occurs when holes in successive layers momentarily align (Reason, 2000). The model therefore directs attention to the conditions behind an error rather than to the individual alone, an orientation suited to aviation cybersecurity.

The model was selected because it aligns with the argument by Nobles that cybersecurity must account for human performance rather than rely on technology alone (Nobles, 2022; Nobles & McAndrew, 2023). In the events examined, GNSS interference created holes in the equipment layer, while inconsistent reporting (IATA, 2025) and unharmonized training (EASA & EUROCONTROL, 2026) functioned as latent organizational conditions. Stress, burnout, and security fatigue widen holes in the human layer (Nobles, 2022), and a simulated cyberattack altered pilot workload, trust, and behavior (Gontar et al., 2018). The model thus explains why an external event becomes dangerous only when internal layers are also weak.

The 2025 events show the model operating in practice. When the Collins Aerospace software failed, staff and manual check-in formed the next layer, keeping passengers moving (Scroxton, 2025). After the von der Leyen aircraft lost GPS, the switch to ground-based navigation systems closed the gap (Reuters, 2025b). Resilience, in this view, is measured by the strength of the layers behind the one that failed. Figure 2 maps these layers to three of the events examined, and the second framework extends the same principle to organizational learning (Nonaka, 1994).

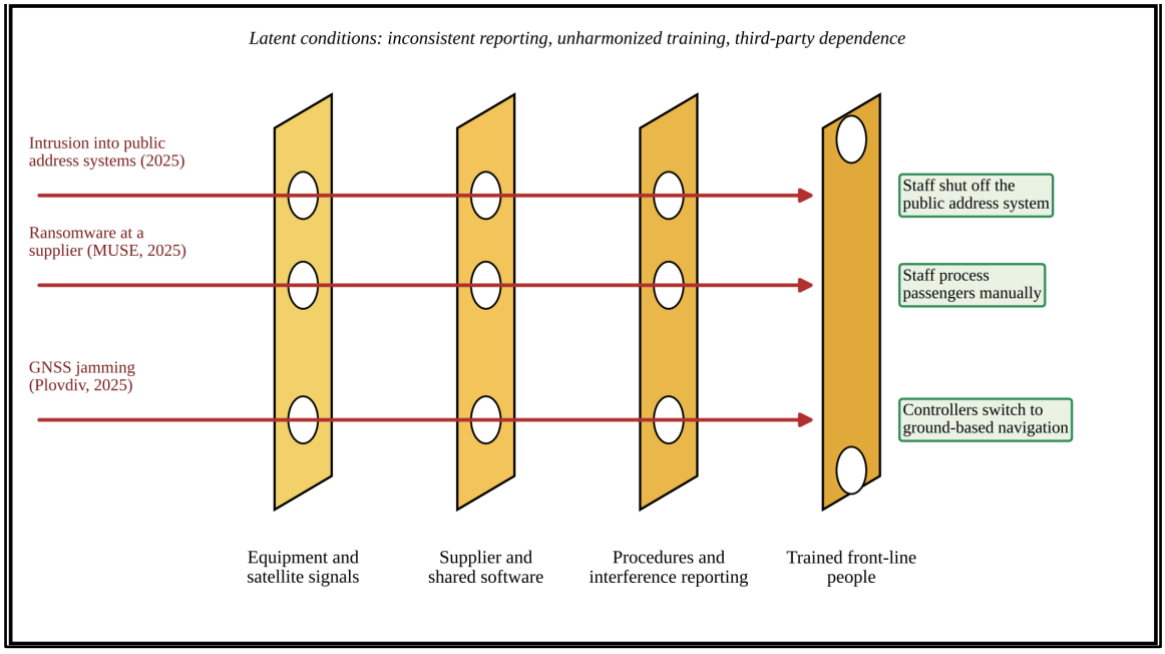

Figure 2. Swiss Cheese Model Applied to Three 2025 Civil Aviation Events

Note. Created by the author, adapting the Swiss cheese model of Reason (2000) to events reported by DiMella and Norman (2025), Goillandeau (2025), Reuters (2025b), and Scroxton (2025).

Framework Two: Nonaka's Knowledge-Creation (SECI) Theory

Knowledge-creation theory explains how organizations convert experience into shared capability. Nonaka (1994) and Nonaka and Takeuchi (1995) describe knowledge creation as a spiral between tacit and explicit knowledge. This spiral moves through socialization, or sharing experience; externalization, or articulating experience as concepts; combination, or integrating explicit knowledge; and internalization, or learning by doing. The spiral implies that lessons from one crew or airport must be articulated and redistributed before they protect others (Nonaka, 1994). This logic addresses the training and knowledge management dimensions of this article.

The theory was selected because aviation cyber resilience depends on converting front-line experience into procedures and training. Burton (2021) argued that cybersecurity leaders require continuous, interdisciplinary learning, and Burrell (2024) observed that added cyber training has not stopped attackers from exploiting weaknesses. Dodla and Jones (2023a) examined strategies for knowledge management systems, and Dodla and Jones (2023b) classified knowledge risks as human, technological, and organizational. Burton (2022) further connected cybersecurity leadership to knowledge and organizational development, treating knowledge flow as a security control.

The SECI spiral is visible in the 2026 responses. At Finnair, pilots share daily interference experience, procedures capture it, industry reporting integrates it, and simulator training returns it to crews, mirroring the four SECI stages (EASA & EUROCONTROL, 2026; Lo Nostro, 2026). Figure 3 illustrates this cycle and marks cross-border combination as its weakest stage. Burton (2025) similarly recommends scenario-based training and simulation exercises so that aviation employees can recognize and report suspicious behavior. The Swiss cheese model thus identifies where defenses fail, while SECI explains how organizations learn to close those gaps (Dodla & Jones, 2023a; Nobles, 2022).

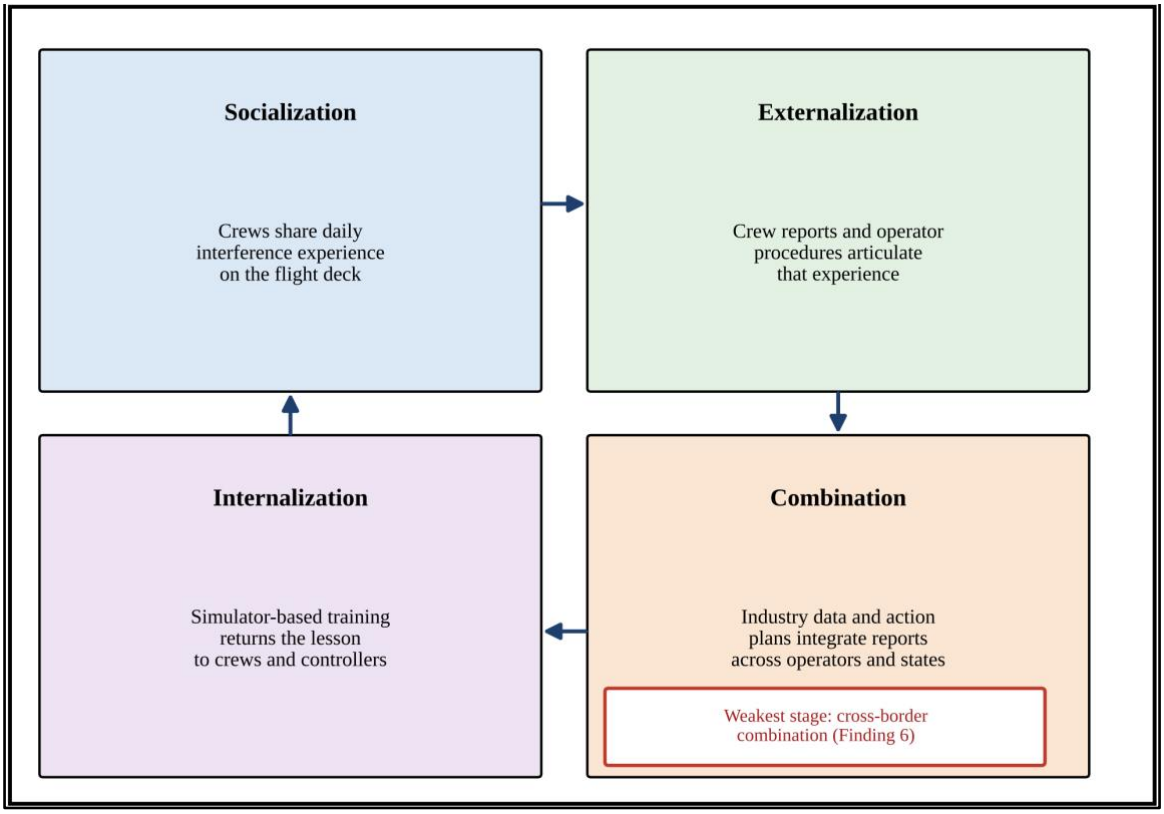

Figure 3. Knowledge-Creation (SECI) Cycle for GNSS Interference Knowledge

Note. Created by the author, adapting the SECI model of Nonaka (1994) to responses reported by EASA and EUROCONTROL (2026), IATA (2025), and Lo Nostro (2026).

Critique of the Theoretical Framework

Drawbacks of the Swiss Cheese Model

The Swiss cheese model carries structural drawbacks for this research. First, Leveson (2011) argued that chain-of-events models inadequately explain accidents in complex sociotechnical systems, where losses can emerge from unsafe interactions among components that each function as designed. Second, Reason (2000) framed the model around error and accidents; therefore, it does not fully represent an intelligent adversary who deliberately creates or aligns holes, as ransomware operators and state-linked jammers do. Because the 2025 campaigns were intentional, an accident model can describe their effects but not the reasoning of their perpetrators. Third, Libicki (2026) argues that whether a cyber operation counts as war is a political judgment, and the model contains no layer for such judgments even though they shape how states respond. These weaknesses limit the precision of the model in adversarial settings.

Further drawbacks concern scope and timing. Fourth, the model treats layers as largely internal to an organization, whereas the 2025 holes originated in a third-party supplier, in foreign electronic activity, and in contested diplomatic attribution (Nilsson-Julien & Jones, 2025; Scroxton, 2025). Fifth, the model offers limited guidance on cascading, cross-border effects, such as one supplier outage that disrupted airports in four countries at once (Scroxton, 2025), or on geopolitical remedies such as ICAO condemnation (ICAO, 2025). Sixth, the model invites hindsight reasoning, because analysts can usually locate aligned holes after an incident but cannot easily rank weaknesses before an adversary acts (Leveson, 2011). Accordingly, this article uses the model to describe how defenses failed, not to predict failure.

Drawbacks of the SECI Model

The SECI model presents empirical and contextual drawbacks for this research. First, Gourlay (2006) criticized the theory for weak empirical support and for a conceptually problematic

treatment of tacit knowledge conversion. Second, the model assumes trust and a willingness to share. Jones (2020) and Dodla and Jones (2023b), however, identify reputational risk as a material organizational threat, and fear of reputational harm can suppress the disclosure that SECI requires. Third, knowledge spirals operate on organizational timelines, while interference patterns can shift within months, as the sharp rise in Latin American and Caribbean airspace after September 2025 showed (IATA & ALTA, 2026). A lesson reaching crews months after an interference pattern changes may already be obsolete. These constraints raise doubt about whether the spiral can keep pace with adversaries.

Additional drawbacks concern scale and knowledge quality. Fourth, Nonaka and Takeuchi (1995) developed the model from studies of Japanese companies, and it does not directly address cross-border knowledge flows among regulators, airlines, and states. A working paper presented to the ICAO Legal Committee reflected the same gap. That paper noted that responsibility for cross-border aviation cyber incidents may be divided among national criminal law, aviation regulation, data-protection law, and international law (ICAO, 2026). Fifth, the model presumes a shared vocabulary, yet aviation still lacked standard phraseology and coding for interference reports when EASA and IATA called for them in 2025 (IATA, 2025). Sixth, SECI does not address the manipulation of knowledge itself, including the disinformation that Ohu and Jones (2025a) associate with cyberwarfare and early attributions later disputed (Nilsson-Julien & Jones, 2025). For that reason, this article uses SECI to explain how knowledge moves, not to guarantee that knowledge will be shared or accurate.

Results and Data Findings

Table 1 maps the principal events to the four domains and the human dimensions examined, and Figure 1 shows their sequence. Four of the seven events spanned two or more domains, which is the central result. Domains defined separately in the Key Terms and Definitions converged within single events, a pattern consistent with the call by Nobles et al. (2022) for a coordinated global aviation cyber defense. Six findings emerged.

Table 1. Convergence of Four Cyber Domains in Civil Aviation, December 2024–October 2026

Event (date)	Primary domain(s)	Human factors, training, or knowledge management signal
Azerbaijan Airlines Flight 8243 crash (Dec. 2024); settlement (Apr. 2026)	Cyberwar battlespace; cyber diplomacy	Crew operated in contested airspace; settlement after nearly 16 months
Aeroflot outage claimed by pro-Ukrainian hackers (Jul. 2025)	Cyberwar by proxy; cyberspace	More than 40 flights canceled; operational dependence on information technology
GPS jamming of the von der Leyen aircraft (Aug. 2025)	Cyberwar (electronic); cyber diplomacy	Controllers switched to ground-based navigation; attribution later disputed
Collins Aerospace MUSE ransomware (Sep. 2025)	Cyberspace (criminal supply-chain compromise)	Manual check-in at four major hubs; third-party dependence
ICAO Assembly condemnation of the DPRK and Russia (Oct. 2025)	Cyber diplomacy	Condemnation issued; no enforcement described
Airport public address intrusions, including Harrisburg, Pennsylvania (Oct. 2025)	Cyber terrorism–adjacent propaganda	Public trust targeted; airport shut off the system
IATA interference data, EASA and EUROCONTROL action plan, and Finnair training (2026)	Cyberspace; cyberwar spillover	Inconsistent reporting; movement toward mandated, simulator-based training

Note. Compiled by the author based on Catchpole (2025); DiMella and Norman (2025); EASA and EUROCONTROL (2026); Faulconbridge and Papachristou (2025); Goillandeau (2025); Gozzi and Tidy (2025); IATA (2026); ICAO (2025); Lo Nostro (2026); Ministry of Foreign Affairs of the Republic of Azerbaijan (2026); Nilsson-Julien and Jones (2025); Reuters (2025b); and Scroxton (2025).

Finding 1: Cyberwar and electronic warfare reach civilians outside conflict zones. IATA and ALTA (2026) reported a sharp rise in GNSS interference in Latin American and Caribbean airspace after September 2025 and linked it to military operations and government countermeasures. The Flight 8243 crash and the von der Leyen incident show civil aircraft sharing spectrum and airspace with military defenses (Faulconbridge & Papachristou, 2025; Reuters, 2025b). In its Foundational PNT Profile, the National Institute of Standards and Technology (NIST) likewise addresses the risk of interrupted or falsified positioning, navigation, and timing (PNT) services (Bartock et al., 2023). A 220% rise in GPS signal-loss events from 2021 to 2024 (IATA, 2025) raises the stakes for diplomacy.

Finding 2: Cyber diplomacy is active but slow and lacks enforcement. ICAO condemned the DPRK and the Russian Federation, yet the documents examined describe no enforcement (ICAO, 2025). Settling the Flight 8243 crash took nearly 16 months (Ministry of Foreign Affairs of the Republic of Azerbaijan, 2026). Willers and Gjesvik (2026) showed that early framings of cyber diplomacy around major-power rivalry and international security shaped later practice, as this state-to-state response reflects. Leloudas (2026) examines how international air law applies to cyber-interference. A working paper presented to the ICAO Legal Committee in October 2026 reported that existing instruments do not always classify cyberattacks as acts of unlawful interference (ICAO, 2026). Without that classification, a condemnation carries no defined legal consequence, which helps explain why the 2025 response ended with words rather than penalties. These outcomes support the call by Nobles et al. (2022) for stronger global governance, including governance of private supply chains, which the next finding examines.

Finding 3: Cyberspace dependencies concentrate risk in third parties. One ransomware incident at a supplier disrupted hubs in four countries (Scroxton, 2025). The NIST Cybersecurity Framework 2.0 addresses that risk by directing organizations to manage cybersecurity risk from their suppliers (NIST, 2024). Dawson et al. (2021) stress that weak controls in critical infrastructure expose nations to harm, and Verizon (2025) found that the human element contributed to about 60% of 12,195 confirmed breaches. Ohu and Jones (2025b) propose detecting insider threats through cognitive and psychological indicators, which implies a need for behavioral as well as technical controls. Behavioral controls carry particular weight where suppliers and staff hold trusted access. The propaganda intrusions in Finding 4, however, show that attackers may also bypass insiders and target the public directly.

Finding 4: Terror-adjacent cyber propaganda targets public trust rather than aircraft. The October 2025 public address intrusions caused no physical harm, yet used aviation infrastructure to broadcast ideological messages to travelers (Catchpole, 2025). This pattern matches the account by Bhambri and Khang (2026) of attackers using digital means to spread fear and social disruption and the description by Ohu and Jones (2025a) of cyberwarfare as psychological manipulation. Whether these acts legally constitute terrorism remains undetermined, but their effect on public confidence makes them a human security concern. Finding 5 examines how people responded to these and other events.

Finding 5: Human factors and training now form the operative defense. Finnair adapted pilot training for daily interference (Lo Nostro, 2026), and EASA and EUROCONTROL (2026) proposed mandated training for crews and controllers. In three 2025 events, the layer that limited harm was human. Controllers switched to ground-based navigation, staff processed passengers manually, and employees shut off a public address system (DiMella & Norman, 2025; Goillandeau, 2025; Reuters, 2025b; Scroxton, 2025). This pattern supports the call by Nobles (2017) for workforce education, which depends on knowledge flow.

Finding 6: Knowledge management is the weakest layer. Inconsistent terminology and reporting formats impede combination, the SECI stage that integrates knowledge across

organizations (IATA, 2025; Nonaka, 1994). Dodla and Jones (2023a) examined how knowledge management strategies support knowledge systems, yet the documents examined describe no shared, cross-border repository for aviation interference knowledge (EASA & EUROCONTROL, 2026; IATA, 2025). Until that gap closes, lessons from one operator will spread slowly. The discussion that follows interprets these six findings.

Discussion

The six findings answer the research question by showing that convergence occurred within single events rather than across separate policy domains. One GPS jamming episode, for example, was at once an electronic act within cyberspace, a spillover of armed conflict, and a diplomatic dispute (Nilsson-Julien & Jones, 2025; Reuters, 2025b). This pattern extends the warning by Nobles (2017) that dense interconnection exposes civil aviation to cyber risk, because the interconnection now includes geopolitical as well as technical links. Nobles et al. (2022) called for a global aviation cybersecurity defense policy, and the absence of enforcement after the 2025 ICAO condemnation shows that the gap they identified persists (ICAO, 2025). The two theoretical frameworks explain this convergence in different ways.

The Swiss cheese model explained where defenses failed, yet the events also exposed its limits in adversarial settings. Attackers reached suppliers, spectrum, and public address systems that sat outside airline control (Catchpole, 2025; Scroxton, 2025). That pattern supports the critique by Leveson (2011) that losses can emerge from interactions among components rather than from a single chain of failures. SECI, by contrast, explained how crews and regulators converted experience into training (EASA & EUROCONTROL, 2026; Lo Nostro, 2026). Read together, the two frameworks suggest that aviation resilience depends on the speed at which knowledge moves from one failed layer to the people who staff the next one.

The human-performance findings align with earlier experimental and leadership research. Gontar et al. (2018) found that a simulated cyberattack altered pilot workload, trust, and behavior, and the 2025 events show the same human layer deciding outcomes in actual operations (Reuters, 2025b; Scroxton, 2025). Burton et al. (2023) linked cybersecurity leadership to human factors, emotional intelligence, and innovative work behavior, which suggests that leaders shape whether front-line staff act decisively when systems fail. Nobles (2022) adds that stress, burnout, and security fatigue weaken that human layer, so workforce resilience requires attention to well-being as well as skill. These implications inform the recommendations in the conclusion.

Conclusion

Civil aviation now experiences cyberspace, cyber diplomacy, cyberwar, and cyber terrorism as one connected risk environment rather than four separate subjects. Five events occurred between December 2024 and October 2025. They were a fatal crash, jamming of an official's aircraft, ransomware against shared airport software, terminal propaganda, and a formal ICAO condemnation (Catchpole, 2025; Faulconbridge & Papachristou, 2025; ICAO, 2025; Reuters, 2025b; Scroxton, 2025). A diplomatic settlement and a proposal to mandate interference training followed in 2026 (EASA & EUROCONTROL, 2026; Ministry of Foreign Affairs of the Republic of Azerbaijan, 2026). In each case, human performance and shared knowledge, rather than technology alone, determined how well aviation absorbed the shock. That conclusion has practical consequences for leaders.

Four recommendations follow from the findings. First, leaders should treat GNSS interference and cyber disruption as human-performance hazards. They should also fund simulator-based, scenario-driven training for pilots, controllers, and airport staff within a life cycle learning program (Burton, 2021; EASA & EUROCONTROL, 2026; Merritt et al., 2024). Second, regulators and industry should adopt common reporting terminology and a

cross-border knowledge repository, moving aviation through the SECI combination stage (Dodla & Jones, 2023a; IATA, 2026). Third, airports and airlines should rehearse manual fallback for third-party outages and build stress, fatigue, and workload into cyber exercises (Nobles, 2022). Fourth, states should support ICAO processes and standard interference phraseology. They should also pursue the global governance proposed by Nobles et al. (2022), including the explicit classification of cyberattacks as acts of unlawful interference under air law (ICAO, 2026). These recommendations also suggest an agenda for research.

Future research should include dissertation-level qualitative studies of pilot and controller experience with spoofing and jamming, extending Gontar et al. (2018). Quantitative evaluation of simulator-based interference training would test the internalization stage that EASA and EUROCONTROL (2026) seek to strengthen. Studies of cross-border incident sharing would extend Dodla and Jones (2023b) into aviation. Aviation has historically learned from accidents; the present task is to learn from near-misses, propaganda, and gray-zone interference before the holes align again (Reason, 2000).

Key Terms and Definitions

Cyberspace: "The interdependent network of information technology infrastructures that includes the Internet, telecommunications networks, computers, information systems, industrial control systems, networks, and embedded processors and controllers" (Committee on National Security Systems, 2022, "Cyberspace"). In civil aviation, this network links aircraft, airports, air navigation service providers, and their suppliers.

Cyber Diplomacy: The application of diplomatic techniques and negotiation to international issues that arise in cyberspace, including efforts to prevent conflict there (Radanliev, 2025, pp. 28–29).

Cyberwar: "Actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption" (Clarke & Knake, 2010, p. 6). Whether a given operation counts as war remains a political judgment (Libicki, 2026).

Cyber Terrorism: "Unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives" (Denning, 2000, para. 1). Such attacks seek to spread fear and social disruption (Bhambri & Khang, 2026).

GNSS Radio Frequency Interference: Jamming, which overpowers satellite-navigation signals, or spoofing, which transmits false signals, either of which degrades or misleads aircraft positioning and timing (EASA & EUROCONTROL, 2026).

References

Bartock, M., Brule, J., Li-Baboud, Y.-S., Lightman, S., McCarthy, J., Meldorf, K., Reczek, K., Northrip, D., Scholz, A., & Suloway, T. (2023). *Foundational PNT profile: Applying the Cybersecurity Framework for the responsible use of positioning, navigation, and timing (PNT) services* (NIST Interagency or Internal Report 8323r1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8323r1

Bhambri, P., & Khang, A. (2026). Cyber security threats, cyber terrorism, cyber warfare. In E. de Silva & S. U. W. Jayaratne (Eds.), *The role of intelligence in countering violent extremism* (pp. 163–184). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-3522-2.ch008

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal, 9*(2), 27–40. https://doi.org/10.3316/QRJ0902027

Burrell, D. N. (2024). Understanding healthcare cybersecurity risk management complexity. *Land Forces Academy Review, 29*(1), 38–49. https://doi.org/10.2478/raft-2024-0004

Burton, S. L. (2021). Cybersecurity leaders: Knowledge driving human capital development. *Scientific Bulletin, 26*(2), 109–120. https://doi.org/10.2478/bsaft-2021-0013

Burton, S. L. (2022). *Cybersecurity leadership from a telemedicine/telehealth knowledge and organizational development examination* (Publication No. 29066056) [Doctoral dissertation, Capitol Technology University]. ProQuest Dissertations and Theses Global. https://www.proquest.com/dissertations-theses/cybersecurity-leadership-telemedicine-telehealth/docview/2662752457/se-2

Burton, S. L. (2025). Digital saboteurs: Unmasking insider cybersecurity threats in aviation and aerospace. *Law, Economics and Society, 1*(2), 1–20. https://doi.org/10.30560/les.v1n2p1

Burton, S. L., Burrell, D. N., Nobles, C., & Jones, L. A. (2023). Exploring the nexus of cybersecurity leadership, human factors, emotional intelligence, innovative work behavior, and critical leadership traits. *Scientific Bulletin, 28*(2), 162–175. https://doi.org/10.2478/bsaft-2023-0016

Catchpole, D. (2025, October 16). Hackers use some Canada and US airport PA systems to praise Hamas, criticize Trump. *Reuters*. https://www.reuters.com/business/media-telecom/hackers-use-some-canada-us-airport-pa-systems-praise-hamas-criticize-trump-2025-10-16/

Clarke, R. A., & Knake, R. K. (2010). *Cyber war: The next threat to national security and what to do about it*. Ecco.

Committee on National Security Systems. (2022). *Committee on National Security Systems (CNSS) glossary* (CNSSI No. 4009). https://csrc.nist.gov/glossary/term/cyberspace

Dawson, M., Bacius, R., Gouveia, L. B., & Vassilakos, A. (2021). Understanding the challenge of cybersecurity in critical infrastructure sectors. *Land Forces Academy Review, 26*(1), 69–75. https://doi.org/10.2478/raft-2021-0011

Dawson, M., & Khan, A. H. (2025). Cyber defense of space systems: Taxonomy of vulnerabilities and framework for resilient infrastructure. *Land Forces Academy Review, 30*(3), 454–465. https://doi.org/10.2478/raft-2025-0044

Denning, D. E. (2000, May 23). *Cyberterrorism* [Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives]. https://irp.fas.org/congress/2000_hr/00-05-23denning.htm

DiMella, A., & Norman, G. (2025, October 16). Pro-Hamas screed blasted through airport speakers in US, Canada after hack. *Fox News*. https://www.foxnews.com/travel/hacker-hijacks-airport-speakers-blasts-anti-trump-other-political-messages

Dodla, T. R., & Jones, L. A. (2023a). Identifying knowledge management strategies for knowledge management systems. *ACCESS: Access to Science, Business, Innovation in Digital Economy, 4*(2), 261–277. https://doi.org/10.46656/access.2023.4.2(8)

Dodla, T. R., & Jones, L. A. (2023b). Mitigating knowledge management internal and external risk factors: A literature review of best practices. *Scientific Bulletin, 28*(1), 44–54. https://doi.org/10.2478/bsaft-2023-0005

European Union Aviation Safety Agency & EUROCONTROL. (2026). *European aviation action plan for ensuring safe operations during GNSS interferences* (Edition 1.0). https://www.easa.europa.eu/en/downloads/143429/en

Faulconbridge, G., & Papachristou, L. (2025, October 9). Putin tells Azerbaijan's Aliyev how Russian air defences downed a passenger plane. *Reuters*. https://www.reuters.com/business/aerospace-defense/putin-tells-azerbaijans-aliyev-how-russian-air-defences-downed-passenger-plane-2025-10-09/

Federal Aviation Administration. (2026). *Aeronautical information manual: Official guide to basic flight information and ATC procedures* (Basic with Changes 1, 2, and 3). U.S. Department of Transportation. https://www.faa.gov/air_traffic/publications/atpubs/aim_html/

Goillandeau, M. (2025, October 16). Harrisburg airport, 3 Canadian airports hacked with pro-Palestinian messages [CNN Wire]. *6abc Action News*. https://6abc.com/post/harrisburg-among-airport-pa-systems-apparently-hacked-play-unauthorized-recordings-north-america/18017932/

Gontar, P., Homans, H., Rostalski, M., Behrend, J., Dehais, F., & Bengler, K. (2018). Are pilots prepared for a cyber-attack? A human factors approach to the experimental evaluation of pilots' behavior. *Journal of Air Transport Management, 69*, 26–37. https://doi.org/10.1016/j.jairtraman.2018.01.004

Gourlay, S. (2006). Conceptualizing knowledge creation: A critique of Nonaka's theory. *Journal of Management Studies, 43*(7), 1415–1436. https://doi.org/10.1111/j.1467-6486.2006.00637.x

Gozzi, L., & Tidy, J. (2025, July 28). Pro-Ukraine hacker group claims Aeroflot cyber-attack. *BBC News*. https://www.bbc.com/news/articles/c87e0ydy3d4o

International Air Transport Association. (2025, June 18). *EASA and IATA publish comprehensive plan to mitigate the risks of GNSS interference* [Press release]. https://www.iata.org/en/pressroom/2025-releases/2025-06-18-01/

International Air Transport Association. (2026). *Media briefing: Safety & operations – AGM 2026* [Presentation]. https://www.iata.org/en/iata-repository/pressroom/presentations/media-briefing-safety-operations-agm-2026/

International Air Transport Association & Latin American and Caribbean Air Transport Association. (2026). *GNSS signal interference LATAM-CAR region* (NACC/DCA/14-WP/03) [Working paper]. International Civil Aviation Organization, North American, Central American and Caribbean Office. https://www.icao.int/sites/default/files/NACC/MeetingDocs/2026/NACCDCA14/05%20Working%20Papers%20-%20Notas%20de%20Estudio/NACCDCA14WP03.pdf

International Civil Aviation Organization. (2025, October 3). *ICAO Assembly condemns GNSS radio frequency interference originating from the DPRK and the Russian Federation* [Press release]. https://www.icao.int/news/icao-assembly-condemns-gnss-radio-frequency-interference-originating-dprk-and-russian

International Civil Aviation Organization. (2026). *Cyber security vulnerabilities outside the scope of current air law* (LC/40-WP/2-7; presented by South Africa) [Working paper]. Legal Committee, 40th Session, Montréal, Canada. https://www.icao.int/sites/default/files/WP-2-7-South-Africa-cyber_for-gdoc.pdf

Jones, L. A. (2020). *Reputation risk and potential profitability: Best practices to predict and mitigate risk through amalgamated factors* (Publication No. 28152966) [Doctoral dissertation, Capitol Technology University]. ProQuest Dissertations and Theses Global. https://www.proquest.com/dissertations-theses/reputation-risk-potential-profitability-best/docview/2466047018/se-2

Leloudas, G. (2026). International air law in the age of cyber-interference. In B. Soyer (Ed.), *Transport law and digitalisation* (pp. 133–156). Informa Law from Routledge. https://doi.org/10.4324/9781003728283-11

Leveson, N. G. (2011). *Engineering a safer world: Systems thinking applied to safety*. MIT Press. https://doi.org/10.7551/mitpress/8179.001.0001

Libicki, M. (2026). Is cyberwar war – and why might it matter? *The Cyber Defense Review, 11*(2), 81–88. https://doi.org/10.55682/cdr/ahs0-k0pg

Lo Nostro, G. (2026, September 24). Finnair adapts pilot training for daily GPS interference in Baltic. *Reuters*. https://www.reuters.com/business/aerospace-defense/finnair-adapts-pilot-training-daily-gps-interference-baltic-2026-09-24/

Merritt, M., Hansche, S., Ellis, B., Sanchez-Cherry, K., Snyder, J. N., & Walden, D. (2024). *Building a cybersecurity and privacy learning program* (NIST Special Publication 800-50r1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-50r1

Ministry of Foreign Affairs of the Republic of Azerbaijan. (2026, April 15). *Joint statement of the Ministry of Foreign Affairs of the Republic of Azerbaijan and the Ministry of Foreign Affairs of the Russian Federation* (No. 156/26). https://www.mfa.gov.az/en/news/no15626

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST Cybersecurity White Paper 29). https://doi.org/10.6028/NIST.CSWP.29

Nilsson-Julien, E., & Jones, M. G. (2025, September 4). Bulgaria U-turns on claim Moscow jammed GPS of von der Leyen's plane. *Euronews*. https://www.euronews.com/2025/09/04/no-russian-gps-jamming-bulgaria-u-turns-on-claim-that-von-der-leyens-plane-was-targeted-by

Nobles, C. (2017). Cyber threats in civil aviation. In M. Dawson, M. Eltayeb, & M. Omar (Eds.), *Security solutions for hyperconnectivity and the Internet of Things* (pp. 272–301). IGI Global. https://doi.org/10.4018/978-1-5225-0741-3.ch011

Nobles, C. (2022). Stress, burnout, and security fatigue in cybersecurity: A human factors problem. *HOLISTICA – Journal of Business and Public Administration, 13*(1), 49–72. https://doi.org/10.2478/hjbpa-2022-0003

Nobles, C., Burrell, D. N., & Waller, T. (2022). The need for a global aviation cybersecurity defense policy. *Land Forces Academy Review, 27*(1), 19–26. https://doi.org/10.2478/raft-2022-0003

Nobles, C., & McAndrew, I. (2023). The intersectionality of offensive cybersecurity and human factors: A position paper. *Scientific Bulletin, 28*(2), 215–233. https://doi.org/10.2478/bsaft-2023-0022

Nonaka, I. (1994). A dynamic theory of organizational knowledge creation. *Organization Science, 5*(1), 14–37. https://doi.org/10.1287/orsc.5.1.14

Nonaka, I., & Takeuchi, H. (1995). *The knowledge-creating company: How Japanese companies create the dynamics of innovation*. Oxford University Press. https://doi.org/10.1093/oso/9780195092691.001.0001

Ohu, F. C., & Jones, L. A. (2025a). The intersection of cyberwarfare, social media, and adolescent self-esteem: A forensic cyberpsychology analysis. *Proceedings of the 20th International Conference on Cyber Warfare and Security, 20*(1), 332–344. https://doi.org/10.34190/iccws.20.1.3375

Ohu, F. C., & Jones, L. A. (2025b). Predictive behavioral risk intelligence: An AI framework for insider threat detection based on cognitive and psychological indicators. *RAIS Journal for Social Sciences, 9*(2), 108–132. https://doi.org/10.5281/zenodo.17468887

Radanliev, P. (2025). Cyber diplomacy: Defining the opportunities for cybersecurity and risks from artificial intelligence, IoT, blockchains, and quantum computing. *Journal of Cyber Security Technology, 9*(1), 28–78. https://doi.org/10.1080/23742917.2024.2312671

Reason, J. (2000). Human error: Models and management. *BMJ, 320*(7237), 768–770. https://doi.org/10.1136/bmj.320.7237.768

Reuters. (2025a, February 4). *Crashed Azerbaijani plane was riddled with holes after incident over Russia, report says.* https://www.reuters.com/world/asia-pacific/kazakh-report-says-plane-dec-25-crash-probably-damaged-by-external-objects-2025-02-04/

Reuters. (2025b, September 1). *EU says von der Leyen's plane GPS system was jammed, Russian interference suspected.* https://www.reuters.com/world/europe/eu-says-von-der-leyens-plane-gps-system-was-jammed-russian-interference-2025-09-01/

Scroxton, A. (2025, September 22). Cyber attack that downed airport systems confirmed as ransomware. *Computer Weekly*. https://www.computerweekly.com/news/366631592/Cyber-attack-that-downed-airport-systems-confirmed-as-ransomware

Verizon Business. (2025). *2025 data breach investigations report*. https://www.verizon.com/business/resources/reports/dbir/

Willers, J. O., & Gjesvik, L. (2026). Diplomacy in the age of expertise: The case of cyber diplomacy. *International Affairs, 102*(2), 513–534. https://doi.org/10.1093/ia/iiaf271