Journal of Military and Strategic Studies

VOLUME 24, ISSUE 1

Cutting the Tangled Webs of Civil and Military Aviation Toward a Practical Cybersecurity Framework

Kristen Csenkey, Jason Furlong, Lieutenant-Colonel (Retired)

Introduction

In February 2024, it was reported[1] that a threat actor with known links to Iran's Islamic Revolutionary Guard Corps[2] engaged in espionage activities targeting companies in the aviation, aerospace, and defence sectors. Using social engineering and phishing campaigns, the threat actor, also known as UNC1549,[3] targeted employees at American defence and aerospace companies and Israeli shipping and logistics firms.[4] A few months earlier, in September 2023, a distributed denial of service attack was reported to have caused disruptions at several Canadian airports.[5] The pro-Russia (or Russian state-sponsored) hacking group, NoName,[6] claimed

[1] Ofir Rozmann et al., "When Cats Fly: Suspected Iranian Threat Actor UNC1549 Targets Israeli and Middle East Aerospace and Defense Sectors," *Mandiant*, 27 February 2024, https://www.mandiant.com/resources/blog/suspected-iranian-unc1549-targets-israel-middle-east.

[2] Andy Greenberg, "Facebook Catches Iranian Spies Catfishing US Military Targets," *WIRED*, *15*July 2021, https://www.wired.com/story/facebook-iran-espionage-catfishing-us-military/.

[3] Joe Warminsky, "Suspected Iranian Cyber-Espionage Campaign Targets Middle East Aerospace, Defense Industries," *The Record Recorded Future News*, 28 February 2024, https://therecord.media/iran-cyber-espionage-campaign-targeting-middle-east-defense-aerospace.

[4] Daryna Antoniuk, "Suspected Iranian Hackers Target Israeli Shipping and Logistics Companies," *The Record Recorded Future News*, 23 May 2023, https://therecord.media/israel-shipping-logistics-watering-hole-cyberattacks.

[5] Vincent Larin et al., "Agence des services frontaliers: La panne dans les aéroports provenait bien d'une attaque informatique." [Border Services Agency: The outage at the airports was due to a cyber attack]. *La Presse*, 19 September 2023, https://www.lapresse.ca/actualites/national/2023-09-19/agence-des-services-frontaliers/la-panne-dans-les-aeroports-provenait-bien-d-une-attaque-informatique.php.

[6] Canadian Centre for Cyber Security, "Alert: Distributed Denial of Service Campaign Targeting Multiple Canadian Sectors," Government of Canada, 15 September 2023, https://www.cyber.gc.ca/en/alerts-advisories/distributed-denial-service-campaign-targeting-multiple-canadian-sectors#fn1-rf.

ISSN : 1488-559X

responsibility for the attack, which affected check-in kiosks and electronic gates.[7] These two real-world examples provide snapshots into the threats that increasingly impact the interconnected, complex, and digital–physical spaces within the modern aviation ecosystem. This ecosystem is composed of aircraft, people, goods, data, airports, systems, services, and connected technologies that link national and international networks. To illustrate this interconnection and dually highlight the complex problems it may pose, consider the following.

A Hypothetical Scenario

In our example, an aircraft maintenance company is careless in selecting vendors to supply the components needed for its avionics systems. Avionics are safety-critical, aircraft-specific electronic information systems used in all modern military, civilian, and commercial aircraft. Avionic systems can include radar, navigation, communication, and flight control electronics. They are used to inform the aircrew and operate the aircraft during all phases of flight, including takeoff, landing, and in-flight monitoring. Aircraft avionics comprise a mix of hardware and software components designed and produced to meet rigorous safety levels, so they are subject to several layers of review and testing before an aircraft is declared safe to fly. Consequently, a failure in one of these systems or components can lead to a catastrophic incident, such as the crash of Air France flight 447 into the South Atlantic Ocean[8] and two crashes involving Boeing's 737 Max that led to this aircraft model being grounded twice.[9]

In this hypothetical scenario, the aircraft operator's unscrupulous parts vendor poses risks that could include delivering a defective part or supplying an avionics component with embedded (malicious) software. Perhaps there is resident code in the embedded systems or an exploitable flaw in the design. For example, maintenance personnel may source and purchase a

---

[7] Ashish Khaitan, "Cyber Attacks on Canadian Airports Have Disrupted Operations," *The Cyber Express*, 21 September 2023, https://thecyberexpress.com/cyber-attacks-on-canadian-airports-disrupt-ops/.

[8] Bureau d'Enquêtes et d'Analyses [BEA] pour la sécurité de l'aviation civile, *Final Report on the Accident on 1st June 2009 to the Airbus A330-203 Registered F-GZCP Operated by Air France Flight AF 447 Rio de Janeiro – Paris*, translated by BEA from French, 11 July 2012, https://bea.aero/docspa/2009/f-cp090601.en/pdf/f-cp090601.en.pdf. The cause of the crash was reported to be due to an improper airspeed value being measured and displayed to the pilots, causing them to put the aircraft into a stall.

[9] Vance Badawey, "A Study of Aircraft Certification in Canada in Light of Two Incidents Involving Lion Air Flight 610 and Ethiopian Airlines Flight 302, *Report of the Standing Committee on Transport, Infrastructure and Communities, 43rd Parliament, 2nd Session,* Government of Canada, June 2021, https://www.ourcommons.ca/DocumentViewer/en/43-2/TRAN/report-2/page-39. This was the combined result of a faulty angle-of-attack sensor and poorly designed software that put the aircraft into an irrecoverable state.

component that is to be installed in the in-flight entertainment system of a commercial aircraft.[10] In this case, the in-flight entertainment system has maintenance ports that a passenger can easily plug into without the in-flight crew noticing. There are a number of small, easily purchased devices[11] that attackers can use to connect to open ports and leave in place to function as a system on a chip. By connecting a network device to an open port in a vulnerable in-flight entertainment system, an attacker could eventually have access to entire systems, enabling them to infiltrate the avionics networks and leave malicious code that would activate on a subsequent flight.

The International Air Transport Association (IATA) divides airborne digitized systems into three categories;[12] avionics are subject to an intense level of scrutiny, while a system such as in-flight entertainment is assumed to be isolated and therefore is not required to achieve the same level of certification. In reality, this isolation is not present and connectivity between the domains has been seen on several production aircraft.[13] An attacker's intention could be to infiltrate the avionics systems, take control of the aircraft, navigate it to another destination or even force a terminal descent of the plane. Either one of these scenarios would be classified as a terrorist act and result in the alerting of and a response by the North American Aerospace Defense Command (NORAD). While NORAD certainly has sufficient capacity to manage the hijacking of a single aircraft, it still diverts resources and attention. A multitude of simultaneous threats originating within North American airspace would therefore have the potential to reduce or eliminate NORAD's ability to defend against an external attack.

Our hypothetical scenario serves to highlight why it is vital to recognize the international security implications of the interconnected elements of the aviation ecosystem, which cyber threat

---

[10] Kim Zetter, "Feds Say That Banned Researcher Commandeered a Plane," *WIRED*, 15 May 2015, https://www.wired.com/2015/05/feds-say-banned-researcher-commandeered-plane/. In this specific case, the attacker picked a seat where they knew there was an open port in the crew cabin that would give them access to the in-flight entertainment system network.

[11] Hak5, Shark Jack (product), accessed 31 December 2024, https://shop.hak5.org/products/shark-jack?variant=21284894670961; Hak5, LAN Turtle (product), accessed 31 December 2024, https://shop.hak5.org/products/lan-turtle.

[12] The three categories, in order of IATA priority, are: aircraft control systems, airline and aircraft service-related information, and passenger information and entertainment. International Air Transport Association, *Aviation Cyber Security Guidance Material, Part 1: Organization Culture and Posture*, 1st ed. (February 9, 2021): 5, https://go.updates.iata.org/acys-guidance-material-part1-organization.

[13] Greg Freiherr, "Will Your Airliner Get Hacked?" *Smithsonian Magazine*, Air & Space Magazine, February 2021, https://www.smithsonianmag.com/air-space-magazine/will-your-airliner-get-hacked-180976752/; Kim Zetter, *WIRED*, 2015. Both articles report on how supposedly isolated domains have been connected.

actors are increasingly seeking to penetrate and subvert.[14] The goals of these threat actors and their methods are varied but can include stealing intellectual property, gathering intelligence, terrorizing (through malicious hacking, data breaches, and phishing),[15] or leaving resident code (i.e., code that is stored in memory) that can be used as a potential future threat vector.

Within the aviation industry, North America consistently suffers from the most cyber-related incidents and attacks.[16] The risks posed by the overlapping connections between states, companies, and individuals are further heightened due to the airspace being shared among civilian and military entities in the cyber and air domains. In the context of the North American aviation ecosystem, civilian air traffic controllers and service providers (services delivered primarily through Nav Canada and the Federal Aviation Administration) play a key role in ensuring the safety and security of the air domain. This is especially the case when it comes to detecting an aircraft that is not operating within prescribed limits. Aircraft operating above a specific altitude limit operate in *controlled airspace* and are required to file a flight plan with the requisite authorities. When an aircraft takes off, air traffic control follows the aircraft through a combination of ground-based radar stations and associated network technologies. These technologies include transponders (also known as Automatic Dependent Surveillance-Broadcast technology) that reside on the aircraft. Any deviation from the original flight plan, a failure to communicate, or the cessation of a transponder signal is cause for the air traffic authorities to immediately attempt to reach the aircraft. If the pilot does not respond and communicate a flight plan change, this could signal a potential hijacking or other malicious activity.[17]

In the case of our hypothetical scenario, if an attacker used the in-flight entertainment system as an attack vector to commandeer and reroute the plane, then the air traffic controllers would recognize the change of flight plan and attempt to communicate with the aircraft. If this attempt failed, then the controllers and air traffic services would notify NORAD. At that point, NORAD would contact the appropriate military authorities—in this case, the force generators of

---

14 Elochukwu Ukwandu et al., "Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends," *Information* 13, no. 3 (2022): pp. 146–, https://doi.org/10.3390/info13030146.

15 Elochukwu Ukwandu et al., "Cyber-Security Challenges in Aviation Industry," Figure 2: Cyber-Attacks by Type.

16 Elochukwu Ukwandu et al., "Cyber-Security Challenges in Aviation Industry," Figure 3: Cyber-Attacks by Location.

17 There are established transponder codes that pilots can set from the cockpit to alert air traffic control of a communications failure or a hijacking. These codes are well known by anyone familiar with flying in controlled airspace. If someone familiar with this practice hijacks an aircraft, they could either ensure the transponder is set back to its last code or turned off.

the Royal Canadian Air Force and US Air Force—and call upon them to respond with a joint military action.

Implementing cooperation at all levels to address aviation-specific threats is particularly complicated. Quoting a line from Sir Walter Scott's poem, *Marmion* about the tangled webs we weave,[18] the US Federal Aviation Administration's Chief Counsel, Marc Nichols appropriately expressed that, "We live in the tangled international aviation webs we have interwoven, and our shared burden is to build an ever-adapting cyber defense system."[19] This tangled web—of overlapping sectors, domains, and national and international actors and systems within the aviation ecosystem—requires protection and defence against attacks, like the above-mentioned real-world examples and our hypothetical scenario. We can view these examples as challenges to enhancing defence in the air and space domains, but we can also see them as opportunities to enhance cooperation between trusted allies within complex and overlapping national networks.

As the aviation ecosystem becomes increasingly digitized and interconnected, it is essential that strategic and high-level policy decisions be supported with the necessary conceptual tools to keep our collective skies safe. We propose that one way to deepen cooperation between trusted allies to protect and defend North America is through the integration of a human-centric cybersecurity framework. The aim of this framework is to provide shared and evolving solutions to emerging cybersecurity problems with the goal of deepening the Canada–US partnership on aviation cybersecurity. The integration of this framework has potential implications for NORAD in terms of cooperation, modernization initiatives, and the continued protection of the interlinked civil and defence aviation ecosystems.

Overview

The remainder of this paper is structured as follows.

First, we outline the main elements of the aviation ecosystem to show that humans, technologies, and ideas form part of this sector's digital-physical infrastructures. We also detail the high-level strategy and policy landscape that offers guidance and recommendations to the state and non-state actors that operate cooperatively within the ecosystem. Next, we demonstrate the urgency of developing and integrating proactive aviation cybersecurity frameworks that can

[18] Walter Scott, *Marmion*, ed. Thomas Bayne (Oxford: Clarendon Press), 1889.

[19] Marc Nicols, "What a Tangled Web: Aviation Prosperity, Cybersecurity Risk" (address, International Air Law Conference on Aviation Cybersecurity, Leiden, Netherlands, 11 May 2023), https://www.faa.gov/speeches/what-tangled-web-aviation-prosperity-cybersecurity-risk.

be implemented through existing bilateral and multilateral partnerships. We then provide background information on the main binational partnership—NORAD—the organization that is tasked with ensuring the security of North American airspace. We detail NORAD's mission and recent modernization strategies to reveal the increasing need to approach the cyber and aviation nexus in a way that acknowledges it as a dynamic security ecosystem.

Second, we look at existing frameworks and engage with the current theoretical and practical approaches that aim to address challenges within this ecosystem. We also demonstrate why we need new frameworks that incorporate humans as part of the solution.

Third, we introduce our novel approach to aviation cybersecurity: the Inter-Organization Learning Culture (IOLC) framework. We explore how our approach could be applied in practice, and we rely again on our hypothetical scenario. In our application of the IOLC framework, we emphasize its incorporation into a North American context through NORAD.

Lastly, we conclude our paper by reiterating that aviation cybersecurity must incorporate a human- and cyber-centric design and application, and stress that accomplishing this requires a shared cybersecurity culture of improvement instead of silos of specialization.

A Look into the Cyber and Aviation Security Nexus

The modern aviation ecosystem is a complex social and technical space of connected technologies, aircraft, people, data, services, systems, and more. This ecosystem has both physical and digital aspects that span national, regional, and international networks and is made up of both civilian and military domains. These domains—and the humans, ideas, and technologies within them—intersect with each other and across the entire aviation landscape in a shared airspace.

In its simplest form, the aviation ecosystem comprises four types of stakeholders: aircraft manufacturers and parts vendors, aircraft operators and airline companies, the entities that supply supporting infrastructure, and government bodies and providers of air navigation services. Each stakeholder has an implicit responsibility to contribute to cybersecurity resilience since a failure in any of their operating domains can cascade into a cybersecurity incident of indeterminate magnitude. The aviation industry is immense and extends its tendrils into many parts of society; thus, for the purposes of our paper, we limit our analysis to first-order effects.

Cybersecurity can be roughly divided into three sub-domains. The first is *platform technologies*. In the context of aviation, this is further divided into vehicles and mobile devices that have intermittent connectivity to a network or the internet, and embedded devices, such as the avionics and entertainment systems in aircraft, the latter of which is characterized by smaller footprints and lower processing power compared with their static, terrestrial equivalents. The second domain is *operational technologies*. These include buildings and static infrastructure such as heating, ventilation, and air conditioning; power distribution; and utilities and utility service providers. Operational technologies can be connected to the Internet but, for safety and security reasons, there are often many layers between operational networks and the Internet. Aviation examples include hangar controls and fuel distribution systems. *Information technology* (IT) is the last domain, and it includes general-purpose computing devices that have a persistent connection to the internet, such as desktop computers, laptops, smartphones, and servers. Within aviation, it includes ticketing, accounting, and scheduling systems.

Due to all the aforementioned factors and actors driving the aviation ecosystem—and, most importantly, the widespread adoption of networked systems of systems—cybersecurity is a critical component of the aviation safety chain. We can envision this safety chain as part of the digital-physical infrastructure and socio-technical connections that link people, technologies, services, and devices across domains and sectors. Unfortunately, these connections are not always visible at a strategic or high level or are limited to a single sector or domain.

High-Level Global Strategies and Aviation Cybersecurity Cooperation

According to the American Institute of Aeronautics and Astronautics 2020 report on aerospace cybersecurity, although enhanced cyber protection is an important priority for professionals in the field, comprehensive cybersecurity practices, training, and frameworks are generally lacking at the organizational,[20] national and, most importantly, international level. High-level frameworks for aviation cybersecurity would allow diverse aviation stakeholders to unify responses, streamline public and private partnerships, and share information, where appropriate. Such frameworks should aim to support proactive approaches to address threats that span the air-cyber domain nexus in the defence sector and the civilian and commercial space. Since both the air-cyber domain and aviation spaces exceed national borders, link economies

[20] American Institute of Aeronautics and Astronautics, "Aerospace Cybersecurity: Enduring Challenges Enduring Solutions," 2, accessed 31 December 2024, https://www.aiaa.org/docs/default-source/uploadedfiles/issues-and-advocacy/policy-papers/whitepaper-cybersecurity-based-on-research-study-2021-srl.pdf/1000.

within the global market, and connect people, goods, and services, international high-level strategies on aviation cybersecurity are especially pertinent to ensure the safety and security of the ecosystem.

Although many aviation and aerospace associations recognize the importance of international sector-specific frameworks, very few exist. For example, the IATA [21] offers a compilation of industry stakeholder–focused guidance material through its *Aviation Cybersecurity Strategy*.[22] The International Civil Aviation Organization's (ICAO) *Aviation Cybersecurity Strategy* is the primary source of unified high-level guidance.[23] This strategy recognizes cyber as dynamic and multidisciplinary and calls for coordinated aviation cybersecurity among the 193 ICAO member states.[24] Citing the borderless nature of both cybersecurity and aviation, the ICAO notes that this coordination must take place at multiple levels, emphasizing the need for harmonization at "global, regional and national levels in order to promote global coherence and to ensure full interoperability of protection measures and risk management systems."[25] In line with the ICAO's vision and mission,[26] the *Aviation Cybersecurity Strategy* focuses on the safety and security of the global civil aviation community and encourages states and industry stakeholders to implement the strategy.[27] Canada and the US are both ICAO member states and closely cooperating allies, yet they do not have specific civil aviation cybersecurity strategies, neither individually at national levels nor national or regionally in either country.

Within a defence context, binational cooperation is essential to the protection and defence of Canada–US airspace and associated infrastructures. Nuanced cooperation frameworks are

---

21 International Air Transportation Association, "Aviation Cyber Security" (web page), accessed 31 December 2024, https://www.iata.org/en/programs/security/cyber-security/.

22 International Air Transportation Association, *Aviation Cybersecurity Fact Sheet*, November 2023, https://www.iata.org/en/iata-repository/pressroom/fact-sheets/fact-sheet--cyber-security/.

23 International Civil Aviation Organization, *Security and Facilitation Strategic Objective: Aviation Cybersecurity Strategy*, October 2019, https://www.icao.int/aviationcybersecurity/Documents/AVIATION%20CYBERSECURITY%20STRATEGY.EN.pdf.

24 International Civil Aviation Organization, "Member States" (web page), accessed 31 December 2024, https://www.icao.int/about-icao/Pages/member-states.aspx.

25 International Civil Aviation Organization, "Security and Facilitation Strategic Objective," p. 2; International Civil Aviation Organization, *Resolution A41-19: Addressing Cybersecurity in Civil Aviation*, accessed December, 2024, 1, https://www.icao.int/aviationcybersecurity/Documents/A41-19.pdf.

26 International Civil Aviation Organization, "Vision and Mission to 2025" (web page), accessed December 31, 2024, https://www.icao.int/about-icao/Council/Pages/vision-and-mission.aspx.

27 International Civil Aviation Organization, *Resolution A40-10: Addressing Cybersecurity in Civil Aviation*, 2, accessed 31 December 2024, https://www.icao.int/aviationcybersecurity/Documents/A40-10.pdf.

required, as civil, military, air, and cyber domains interact at multiple levels in aviation security. The ICAO's *Cybersecurity Action Plan*[28] and *Policy Guidance*,[29] which accompany the strategy, call for coordination and information sharing between civil and military authorities to ensure cyber resiliency.

Recognizing the human element of cybersecurity is an important part of cyber resiliency, a fact the ICAO notes in its *Aviation Cybersecurity Strategy*.[30] In the strategy, the ICAO suggests that one way to emphasize the human factor is by creating and implementing a cybersecurity culture in civil aviation.[31]

At a national level, the *Royal Canadian Air Force Strategy* recognizes the importance of adapting and improving cyber resiliency through "threat awareness, training and systems development."[32] In this document, the Royal Canadian Air Force states that one of its strategic objectives is to be mission-ready and combat-capable through achieving and sustaining cyber resilience by "incorporating cyber mission-assurance constructs to safeguard operational capabilities."[33] The US Air Force recently released organizational changes affecting both the Air Force and Space Force to optimize the different service branches and maintain air superiority in the face of great power competition.[34] While Barno and Bensahel[35] call for the US Air Force to reconsider the changing meaning of air superiority in this reorganization, generally, the integration of cyber at the nexus of domains is enacted through the creation and expansion of technical skill tracks, the creation of a standalone service component command, and the creation

---

[28] International Civil Aviation Organization, *Cybersecurity Action Plan*, 2nd ed., January 2022, p. 11, https://www.icao.int/aviationcybersecurity/Documents/CYBERSECURITY%20ACTION%20PLAN%20-%20Second%20edition.EN.pdf.

[29] International Civil Aviation Organization, *Cybersecurity Policy Guidance*, January 2022, p. 2, https://www.icao.int/aviationcybersecurity/Documents/Cybersecurity%20Policy%20Guidance.EN.pdf.

[30] International Civil Aviation Organization, "Security and Facilitation Strategic Objective," p. 4.

[31] International Civil Aviation Organization, *Cybersecurity Culture in Civil Aviation*, January 2022, https://www.icao.int/aviationcybersecurity/Documents/Cybersecurity%20Culture%20in%20Civil%20Aviation.EN.pdf.

[32] Department of National Defence, *RCAF [Royal Canadian Air Force] Strategy: Agile,·Integrated,·Inclusive*, February 2023, 6, Government of Canada, https://www.canada.ca/content/dam/rcaf-arc/documents/reports-publications/royal-canadian-air-force-strategy-portrait.pdf.

[33] Department of National Defence, "RCAF Strategy," p. 16.

[34] Juan Femath, "Reoptimization for Great Power Competition," US Air Force, March 2024, https://www.af.mil/reoptimization-for-great-power-competition/.

[35] David Barno et al., "Drones, the Air Littoral, and the Looming Irrelevance of the US Air Force." *War on the Rocks*, March 7, 2024, https://warontherocks.com/2024/03/drones-the-air-littoral-and-the-looming-irrelevance-of-the-u-s-air-force/.

of a new information dominance systems centre as part of the Air Force Materiel Command.[36] Yet, neither Canada nor the US—as cooperating allies that share information and airspace and engage in trusted collaborations involving cyber operations—have specified the role that the human element plays in ensuring cyber resiliency and securing North American cyber and air space. A clear approach is needed to coordinate cybersecurity efforts in the fields at national, regional, and international levels.

In 2021, the World Economic Forum released *Pathways Towards a Cyber Resilient Aviation Industry*, an insight report focused on mitigating cyber-related threats by fostering collaborations at international, national, and organizational levels.[37] The report attempts to contextualize gaps and the barriers to achieving a harmonized approach to global cybersecurity in the aviation sector, as specified in the ICAO *Aviation Cybersecurity Strategy.* Among these barriers are fragmented governance and policy approaches and under-investment in cyber-resilience capabilities.[38] Recognizing that people are an important part of cybersecurity in terms of building cyber resilience, the World Economic Forum report puts forth a vision for human involvement that complements the one outlined in the ICAO *Aviation Cybersecurity Strategy* and associated guidance.[39] Drawing on the National Institute of Standards and Technology's (NIST) systems security engineering definition,[40] the World Economic Forum defines cyber resiliency as: "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources."[41] The World Economic Forum, ICAO, and the IATA envision fostering a cybersecurity culture as a way to build cyber resilience across levels. According to the ICAO, cybersecurity culture is:

> … a set of assumptions, attitudes, beliefs, behaviours, norms, perceptions, and values that are inherent in the daily operation of an organization and are reflected by the actions and behaviours of all entities and personnel in their interaction with digital assets.[42]

---

36 Juan Femath, "Reoptimization for Great Power Competition."

37 World Economic Forum. *Pathways Towards a Cyber Resilient Aviation Industry: Insight Report*, April 2021, https://www3.weforum.org/docs/WEF_Pathways_Cyber_Resilient_Aviation_2021.pdf.

38 World Economic Forum, "Pathways Towards a Cyber Resilient Aviation Industry."

39 International Civil Aviation Organization, "Cybersecurity Culture in Civil Aviation."

40 Ron Ross et al., *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*," NIST Special Publication 800-160 Vol. 2, National Institute of Standards and Technology, US Department of Commerce, December 2021, https://doi.org/10.6028/NIST.SP.800-160v2r1.

41 World Economic Forum, "Pathways Towards a Cyber Resilient Aviation Industry,"p. 7.

42 International Civil Aviation Organization, "Cybersecurity Culture in Civil Aviation," p. 1.

Unfortunately, as a 2019 Atlantic Council report suggests, incorporating this culture into aviation is a difficult task, however important that objective may be.[43]

A culture of cybersecurity—learned, practised, and led by humans as part of the complex and interconnected digital–physical infrastructure of the aviation ecosystem—is difficult to implement and requires coordination and cooperation at all levels. As the sophistication and frequency of cyber attacks in Canada and the US continue to increase, individually and collectively,[44] what existing organizations can we call on to enhance Canada–US continental defence? And relatedly, do they integrate a human-centric approach to building a cybersecurity culture at the nexus of the cyber and air domains?

The Role of NORAD in the Nexus

NORAD plays an important role in the aviation ecosystem in North America; however, at the organizational level, it lacks a human-centric approach to cybersecurity and building cyber resilience. The basic mission of NORAD is to monitor and defend North America. Canada and the US, as part of the binational command of NORAD, issue aerospace and maritime warnings and conduct aerospace control.[45] Faced with a complex, global, and integrated system of people, technologies, and ideas about security, this partnership requires Canada and the US to cooperate across domains and geographies. In carrying out their joint mission, the two countries must also consider state, command, and civil-authority borders. Both countries have sought to modernize NORAD to protect against new and emerging threats to North America and address the challenges of an increasingly digitized and interconnected threat landscape.[46]

n this case, modernization refers to improving the ability to deter, detect, and defend in domains beyond and including air and sea. According to the 2021 *Joint Statement on NORAD*

---

43 Pete Cooper et al., *Aviation Cybersecurity: Scoping the Challenge*. Atlantic Council, 2019, 8, p. 10.

44 See for example, US Department of Justice, "Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research" (press release), July 19, 2021, https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion.

45 US Northern Command, *North American Aerospace Defense Command and United States Northern Command Strategy: Executive Summary*, March 2021, https://www.northcom.mil/Portals/28/(U)%20NORAD-USNORTHCOM%20Strategy%20EXSUM%20-%20Signed.pdf.

46 Department of National Defence, "Fact Sheet: NORAD Modernization Project Timelines," last modified May 9, 2024, https://www.canada.ca/en/department-national-defence/services/operations/allies-partners/norad/norad-modernization-project-timelines.html.

Modernization, [47] investments include research and development, the procurement of new technologies or upgrading of existing technologies and systems to improve situational awareness, surveillance and weapons systems, and upgrading infrastructure.[48] In 2022 and again in 2024 with the release of the defence policy update, *Our North, Strong and Free*,[49] Canada announced plans to invest billions of dollars to accomplish these modernization goals to pre-emptively enhance its ability to respond to future threats in the context of binational security cooperation.[50] Part of this investment is slated to go toward future-proofing capabilities, especially the use of technological solutions in the areas of quantum technologies; cyber; artificial intelligence (AI); cloud-enabled command, control, communications and computers; and intelligence, surveillance, and reconnaissance.[51] Investment in cyber is an important part of the cooperation, but must be coupled with the enhancement of resiliency and capabilities to reach operational capability. Furthermore, NORAD modernization activities will take important steps toward all-domain awareness that will include a cyber component.[52]

Previous calls for the integration of digital technologies into a cyber-physical layered system of networked command and control as part of NORAD modernization were made by the former Commander of US Northern Command and NORAD, General Terrence O'Shaughnessy, and the Former Deputy Director of Operations for NORAD, Brigadier General Peter Fesler in

47 Department of Defense (US) and Department of National Defence (Canada), "Joint Statement on NORAD Modernization" (press release), 17 August 2021, https://www.defense.gov/News/Releases/Release/Article/2735041/joint-statement-on-norad-modernization/.

48 Department of National Defence, "NORAD Modernization Project Timelines."

49 Department of National Defence, *Our North, Strong and Free: A Renewed Vision for Canada's Defence*, Government of Canada, 2024, https://www.canada.ca/en/department-national-defence/corporate/reports-publications/north-strong-free-2024.html.

50 Department of National Defence, "Fact Sheet: Funding for Continental Defence and NORAD Modernization" (web page), last modified July 21, 2022, https://www.canada.ca/en/department-national-defence/services/operations/allies-partners/norad/facesheet-funding-norad-modernization.html.

51 Department of National Defence, "Annex C: Canada's NORAD Modernization Plan," last modified 17 April 2024, https://www.canada.ca/en/department-national-defence/corporate/reports-publications/north-strong-free-2024/annex-c-canada-norad-modernization-plan.html.

52 Andrea Charron et al., *NORAD: In Perpetuity and Beyond* (Montreal: McGill-Queen's University Press, 2022), 165. For a discussion about the formal integration of a cyber component into NORAD, see Kristen Csenkey, D. P. Genest, and Canadian Intelligence Corps, "An Opportunity for NORAD Modernization in a Joint CA-US Cyber Component," *Strategic Perspectives,* North American and Arctic Defence and Security Network, 2021, https://www.naadsn.ca/wp-content/uploads/2021/01/Strategic-Perspectives-An-Opportunity-for-NORAD-Modernization-in-a-Joint-CA-US-Cyber-Component-21jan.pdf.

their paper on how to strengthen "North America's shield" (NORAD).[53] Their proposed approach and the related Pathfinder[54] initiative largely focus on the use of data collection and analysis to increase defence domain awareness, improve decision-making, and support civil aviation authorities. However, as Andrea Charron aptly notes in her critique of the approach recommended by O'Shaughnessy and Fesler, while there are benefits to this type of integration, including enhancement of capabilities through the incorporation of technologies such as AI, it may pose several challenges, including costs and the coordination of procurement. It also raises questions about the ownership of data.[55] Indeed, the integration of technologies such as AI and cloud-based systems as part of NORAD modernization efforts also extends to the modernization of the Canadian Armed Forces (CAF) through its digital transformation initiatives.[56] Yet, as Major Jason Chor argues, the CAF's digital transformation framework is fragmented because it lacks cohesive objectives; thus, its focus needs to be on achieving unity.[57] Integrating digital technologies into the layered cyber and aviation network is a challenge that both NORAD member states must contend with separately and cooperatively.

Cybersecurity is important to NORAD defence because, to operate effectively, the air domain relies on networks of interconnected devices that incorporate humans, organizations, and ideas. These networks include intricate "systems of systems" with emergent properties that are

[53] General Terrence J. O'Shaughnessy et al., *Hardening the Shield: A Credible Deterrent & Capable Defense for North America* (Washington, DC: The Wilson Center, September 2020), https://www.wilsoncenter.org/sites/default/files/media/uploads/documents/Hardening%20the%20Shield_A%20Credible%20Deterrent%20%26%20Capable%20Defense%20for%20North%20America_EN.pdf.

[54] Rachel S. Cohen, "Pentagon's Silicon Valley Hub Is Helping NORAD Monitor US Airspace," *Air & Space Forces Magazine*, 23 October 2020, https://www.airandspaceforces.com/pentagons-silicon-valley-hub-is-helping-norad-monitor-us-airspace/.

[55] Andrea Charron, "Responding to 'Hardening the SHIELD: A Credible Deterrent and Capable Defense for North America,'" in *Shielding North America: Canada's Role in NORAD Modernization*, ed. Nancy Teeple and Ryan Dean (Peterborough, ON: North American and Arctic Defence and Security Network, 2021), pp. 84–89, https://www.naadsn.ca/wp-content/uploads/2021/03/NAADSN-engage4-NORAD-NT-RD-upload.pdf.

[56] Department of National Defence, "Canadian Armed Forces Digital Campaign Plan" (web page), last modified 28 February 2023, https://www.canada.ca/en/department-national-defence/corporate/reports-publications/canadian-armed-forces-digital-campaign-plan.html.

[57] Major Jason Chor, "The CAF Digital Campaign Plan: Digital Transformation in Jeopardy," JCSP 49 Service Paper (Canadian Forces College, 2022–2023), https://www.cfc.forces.gc.ca/259/290/49/192/Chor.pdf.

both undocumented and unknown. For a variety of reasons, potential adversaries could choose to exploit those emergent properties to crack open our security shield. Canada and the US need to defend this aviation system of systems because, as previously characterized, it forms a vital ecosystem that requires a cybersecurity framework to increase cybersecurity resiliency.

Recalling the aforementioned sub-sectors and domains of aviation and cyber and placing them in the context of NORAD reveals some of the interwoven webs in the cyber defence system. NORAD's formal and informal defence responsibilities require the presence of systems in each of the cybersecurity sub-domains. This multi-system reality complicates the issue of cybersecurity due to differences in and between the specific techniques, technologies, and operations. For instance, platform technologies do not have a persistent connection to the internet or to any network. This means that many types of embedded devices are slow to receive security updates, often because physical access to the device is required.

The Need for an Aviation Cybersecurity Framework

Connected networks link—and entangle—people, states, services, technologies, and devices within the webs of cyber- and air-domain networks. Within aviation, these tangled webs pose problems for cooperation and coordination at an organizational, national, regional, and international level, especially as new cybersecurity frameworks are needed to ensure these domains remain safe and secure. The lack of a nuanced aviation cybersecurity framework, one that recognizes the value of the human factor in building and maintaining cyber resiliency, makes such cooperation and coordination difficult. There are many high-level industrial, regional, and international guidelines and strategies, such as those produced by the IATA, ICAO, and World Economic Forum, as previously discussed in this section. If we accept that a strategic approach to cyber must necessarily include the human factor in building and maintaining a culture of cybersecurity, then part of this approach must include building cyber resilience along with cyber defence.[58] Long-standing and trusted partnerships between allies, such as NORAD, could provide an opportunity to approach security at the nexus of cyber and air domains differently. In the following section, we explore the theoretical and practical underpinnings of existing cybersecurity frameworks as they relate to these domains. This exploration allows us to identify the conceptual and practice-based challenges facing existing cybersecurity-specific frameworks. Further, it allows us to introduce the IOLC framework, our recommended approach for taking

[58] Calvin Nobles et al., "The Need for a Global Aviation Cybersecurity Defense Policy," *Land Forces Academy Review* 27, no. 1 (March 2022): pp. 19–26, https://doi.org/10.2478/raft-2022-0003.

the best practices from existing frameworks and bringing them together to create a human approach to cyber resilience.

Existing Frameworks

Theoretical Approaches: Human-as-Problem Versus Human-as-Solution

Previous approaches to cybersecurity generally position humans as the problem, the weakest security component and the one most in need of correction. Zimmermann and Renaud[59] frame this approach as *human-as-problem* and argue that it is based on a mindset that embeds uncritical assumptions about cybersecurity-associated problems. In their analysis of cybersecurity-related government and industry public announcements and publications, the authors found that humans are often positioned as the issue within the socio-technical system of cybersecurity. For example, they found that blaming humans in this context is often justified as a lack of awareness, knowledge, and skills, among other reasons, at individual and societal levels. Zimmermann and Renaud argue that these assumptions frame current approaches to cybersecurity and this is problematic because it puts the focus on excluding and constraining human behaviour.[60] When organizations focus on protecting themselves from undesirable human behaviour, they enter a self-reinforcing loop that does not necessarily solve the problem.[61] Instead, the authors argue that the thinking on cybersecurity needs to move toward a "human-as-solution" approach. Drawing on Roberts[62] and Dekker,[63] Zimmermann and Renaud[64] argue that when people are seen as playing an active role in finding a solution—or seen as the solution themselves—organizations generally begin to reflect a culture of reliability. This is why a new paradigm is needed, one in which human actors are positioned as contributors to cybersecurity

---

59 Verena Zimmermann et al., "Moving from a 'Human-as-Problem' to a 'Human-as-Solution' Cybersecurity Mindset," *International Journal of Human-Computer Studies*, 131 (November 2019): pp. 169–187. https://doi.org/10.1016/j.ijhcs.2019.05.005.

60 Zimmermann et al., "Moving from a 'Human-as-Problem' to a 'Human-as-Solution' Cybersecurity Mindset," 173.

61 Zimmermann et al., "Moving from a 'Human-as-Problem' to a 'Human-as-Solution' Cybersecurity Mindset," 174, 175.

62 Karlene H. Roberts, "New Challenges in Organizational Research: High Reliability Organizations," *Industrial Crisis Quarterly* 3, no. 2 (1989): pp. 111–125, https://doi.org/10.1177/108602668900300202.

63 Sidney Dekker, *Safety Differently* (London: CRC Press, 2014).

64 Zimmermann et al., "Moving from a 'Human-as-Problem' to a 'Human-as-Solution' Cybersecurity Mindset," 131.

with the goal of maintaining and enhancing security—and therefore resilience—within socio-technical systems.

Humans make mistakes. Within cybersecurity, however, through learning, collaboration, and communication,[65] humans can be a part of the solution and promote a cybersecurity culture of resiliency. To be sure, this approach could benefit malicious actors, and there are a variety of reasons why people may be reluctant to share information.[66] Still, a culture built on control and constraint does not necessarily facilitate trust in leadership, mission-oriented action,[67] and goal alignment.[68]

A human-centric approach is an increasingly popular lens through which to view and model cybersecurity governance in theory and in policy.[69] Often, these models emphasize human behaviours in the context of a cybersecurity culture.[70] The homological human-centric approach to cybersecurity places humans at the centre, thereby making them objects of security.[71] This

---

65 Zimmermann et al., "Moving from a 'Human-as-Problem' to a 'Human-as-Solution' Cybersecurity Mindset," 179.

66 Alain Mermoud et al., "To Share or Not to Share: A Behavioral Perspective on Human Participation in Security Information Sharing," *Journal of Cybersecurity*, 5, no. 1 (2019), pp. 1–13, https://doi.org/10.1093/cybsec/tyz006

67 Rob McClary, *Building Mutual Trust Between Soldiers and Leaders* (white paper), US Army Combined Arms Center, accessed 31 December 2024, https://cdm16040.contentdm.oclc.org/digital/collection/p16040coll2/id/16; Robert B. Scaife et al., "A Paradigm of Dialogue and Trust: Army Mission Command Training," *Military Review* (January-February 2015), https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20150228_art010.pdf.

68 Alain Mermoud et al., "To Share or Not to Share," pp. 1–13.

69 For example, see Alessandro Pollini et al., "Leveraging Human Factors in Cybersecurity: An Integrated Methodological Approach," *Cognition, Technology & Work*, 24, no. 2 (May 2022): pp. 371–390, https://doi.org/10.1007/s10111-021-00683-y; Julie Haney et al., "NIST Unveils Newly Named Human-Centered Cybersecurity Program" *Cybersecurity Insights* (blog), National Institute of Standards and Technology, 28 September 2023, https://www.nist.gov/blogs/cybersecurity-insights/nist-unveils-newly-named-human-centered-cybersecurity-program; Sheetal Kumar, "The Missing Piece in Human-Centric Approaches to Cybernorms Implementation: The Role of Civil Society," *Journal of Cyber Policy* 6, no. 3 (2021): pp. 375–393, https://doi.org/10.1080/23738871.2021.1909090.

70 For example, see Dennik Baltuttis et al., "A Typology of Cybersecurity Behavior Among Knowledge Workers," *Computers & Security*, 140 (May 2024): 103741, https://doi.org/10.1016/j.cose.2024.103741; Ling Li et al., "Investigating the Impact of Cybersecurity Policy Awareness on Employees' Cybersecurity Behavior," *International Journal of Information Management,* 45 (April 2019): pp. 13–24, https://doi.org/10.1016/j.ijinfomgt.2018.10.017; Alessandro Pollini et al., "Leveraging Human Factors in Cybersecurity," pp. 371–390.

71 Myriam Dunn Cavelty, "Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities," *Science and Engineering Ethics,* 20 (2014): pp. 701–715,

"human as security object" approach can affect how threats are classified and how humans and their roles are positioned within networks.[72] As previously argued above, a cybersecurity culture of resiliency should emphasize human participation, communication, and collaboration in the process and avoid seeing human behaviour as inherently in need of constraint and control. This culture should be holistic in approach and emphasize human participation in social and technical processes and systems.[73] A human-centric approach to cybersecurity that envisions people as part of the solution and is incorporated into cyber resiliency can lead to the creation of new models that are not based on linear assumptions about threats, actors, and problems.[74] There is room for new resilience-based models that enhance the capacities of people, technologies, and organizations, allowing them to adapt, pivot, and overcome cyber incidents. This leads us to ask: What are the existing models, guidance, and standards that direct the practical approaches to cybersecurity? How do these current frameworks envision cyber resiliency, especially as it is applied to the modern aviation ecosystem in all of its tangled webs of complexities, networks, and social-technical connections?

Practical Approaches to Resilience

Existing practical approaches to aviation cybersecurity, while influenced by the concepts and overriding concerns of aviation safety and security, are largely extensions of existing cybersecurity best practices borrowed from the IT industry. These best practices are visible within cybersecurity-specific standards, guidance, and models but are not necessarily visible at the intersection points in sector-specific domains. Although these practical approaches serve the security needs of the IT community reasonably well, they do not achieve the same level of transparency and resiliency that the aviation ecosystem requires. To be sure, the misalignment of approaches between aviation-specific needs and cybersecurity-specific best practices could be the

https://doi.org/10.1007/s11948-014-9551-y; Sheetal Kumar, "The Missing Piece in Human-Centric Approaches to Cybernorms."

[72] Myriam Dunn Cavelty, "The Militarisation of Cyberspace: Why Less May Be Better," in *Proceedings of the 4th International Conference on Cyber Conflict,* Tallinn, Estonia, 5-8 June 2012, CCD COE Publications, pp. 141–154, https://ccdcoe.org/uploads/2019/03/CyCon_book_2012.pdf.

[73] Adapted from Marthie Grobler et al., "User, Usage and Usability: Redefining Human Centric Cyber Security," *Frontiers in Big Data,* 4 (2021): 583723–583723, https://doi.org/10.3389/fdata.2021.583723; Malyun Hilowle et al., "Users' Adoption of National Digital Identity Systems: Human-Centric Cybersecurity Review," *Journal of Computer Information Systems*, 63, no. 5 (2023), pp. 1264–1279, https://doi.org/10.1080/08874417.2022.2140089.

[74] Nico Ebert et al., "Learning from Safety Science: A Way Forward for Studying Cybersecurity Incidents in Organizations," *Computers & Security*, 134 (November 2023): 103435. https://doi.org/10.1016/j.cose.2023.103435.

result of the maturity of both sectors. As a field, cybersecurity is relatively young compared with a century of commercial air travel.

In this subsection, we identify cybersecurity-specific and aviation sector–appreciative best practices from key related standards, guidance, and models: the *NIST Cybersecurity Framework (CSF) 2.0*[75] and its guidance (especially the GV.RR-01 and GV.RM-05 outcomes[76]),[77] and the ICAO's *Global Aviation Cybersecurity Framework* (including the ICAO's *Cybersecurity Action Plan*, Annex 17: Standard 4.9.1).[78] Within each of these key documents, we examine the following: first, whether and how a human-centric approach to cybersecurity is incorporated as part of cyber resiliency and, second, how these documents envision a cybersecurity culture that appreciates the complex security needs of the aviation sector.

International Standards: NIST and ICAO

NIST released the second version of its framework[79] in February 2024 to provide guidance to industry, government agencies, and other organizations to manage cybersecurity risks. The NIST framework serves as a generalized guide that is scalable to organizations of any size and understandable to diverse stakeholders. The framework is composed of six core functions[80] that "help organizations of all sizes and sectors... manage and reduce their cybersecurity risks."[81] These six core functions are decomposed into a set of 134 non-prescriptive outcomes that are relevant to any organization that leverages modern digital technologies in any capacity. The NIST framework uses non-prescriptive outcomes to ensure that it can be tailored and adapted to protect against adversaries. In applying the NIST framework, an organization will review all the functions and categories to determine which ones are relevant, and then work toward achieving the outcomes that relate to its functions and core mission. The benefit of the NIST framework is

75 Haney et al., "NIST Unveils Newly Named Human-Centered Cybersecurity Program."

76 Governing roles, responsibilities, and authorities (GV.RR) and governing risk management strategy (GV.RM).

77 L. Johnson et al., *Guide for Security-Focused Configuration Management of Information Systems,* NIST Special Publication 800-128, National Institute of Standards and Technology Computer Security Resource Center, US Department of Commerce, https://csrc.nist.gov/pubs/sp/800/128/upd1/final.

78 International Civil Aviation Organization, *Annex 17 to the Convention on International Aviation: Aviation Security*, 12th ed., July 2022, "International Standards and Recommended Practices," section 4.9.1.

79 National Institute of Standards and Technology, *NIST Cybersecurity Framework (CSF) 2.0*, NIST Computer Security Resource Center, 26 February 2024, https://doi.org/10.6028/NIST.CSWP.29.

80 The six functions are Govern, Identify, Protect, Detect, Respond, and Recover.

81 National Institute of Standards and Technology, *NIST Cybersecurity Framework (CSF) 2.0*, 4.

that while it is a high-level concept comprising six core functions, most people, with a bit of cybersecurity training, can understand these functions and see how they can relate to their day-to-day jobs. While there is substantial detail in the outcomes and the way in which cybersecurity professionals can achieve these outcomes, individuals can still use the ideas associated with the six core functions as a way to frame any conversation related to a cybersecurity concern.[82]

The NIST framework is less about the technical details of cybersecurity and more about the human-centric organization. Some of the outcomes, such as in the governance function, relate to stakeholders and communication and are relatable to the human-centric aspect we are arguing for in this paper. Of particular note is the GV.RR-01 outcome,[83] which identifies an organization's leaders as being responsible for fostering a culture that is risk-aware. Also relevant to the human-centric element are the outcomes associated with the Protect: Awareness and Training (PR.AT); Identify: Risk Assessment (ID.AM); and Govern: Roles, Responsibilities, and Authorities (GV.RR) core functions and categories, which focus on human resource policy. Other outcomes, such as GV.RM-05, speak to the importance of establishing a dialogue across organizations, stating that the "Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties."[84] In this statement, the scope of this outcome is contained within the organization and does not address the potential to seek full integration with suppliers and other third parties. The outcome itself is framed as influencing the risk level within the organization instead of the broader aviation ecosystem. This framing is problematic because it focuses on controlling risks within one's own technological supply chain and does not place any emphasis on learning from the shared experiences of all participants in the aviation ecosystem. Additionally, it does not focus on extracting lessons learned or incorporating best practices into the cybersecurity culture of the integrating or contracting organizations.

The ICAO is a United Nations agency that assists with the coordination between countries to ensure that global air travel is safe and reliable. The agency provides an international forum to develop policies and standards to regulate the day-to-day operations of aircraft around the world.

---

82 The NIST website has a success stories page on its website (https://www.nist.gov/cyberframework/success-stories) "explaining how diverse organizations use [version 1] of the Framework to improve their cybersecurity risk management." A common element of these stories is the improvement in the education, training, and subsequent awareness of the participants and stakeholders of the various organizations that implemented the framework.

83 GV.RR-01 (governing roles, responsibilities, and authorities) of the *NIST Cybersecurity Framework 2.0* (Appendix A, page 17) states: " Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving."

84 National Institute of Standards and Technology, *NIST Cybersecurity Framework (CSF) 2.0*, Appendix A, 16.

The ICAO *Cybersecurity Action Plan*[85] is most relevant to our discussion because, similar to the NIST framework, the ICAO's *Cybersecurity Action Plan,* has a human-centric component.[86] There are seven pillars that comprise the *Cybersecurity Action Plan;* however, the first pillar, International Cooperation, is especially relevant to our argument, as it emphasizes a culture of cooperation that extends beyond the confines of an individual organization. This pillar explicitly calls for national and international cooperation at all levels and between all stakeholders.[87] Annex 17, section 4.9.1 is also of relevance. It indicates that states should "develop and implement measures to protect their critical information, communications technology systems, as well as data used for civil aviation purposes from unlawful interference."[88]

While the NIST framework offers a human-centric approach, it does not include the broader imposition of state-wide responsibilities and cooperation that is recommended in the ICAO's *Cybersecurity Action Plan.* Conversely, the ICAO *Cybersecurity Action Plan* prescribes how a national cybersecurity strategy should be implemented, including the legal aspects of an effective strategy. Generally, guidance on aviation cybersecurity focuses on cooperation among government agencies and authorities. This emphasizes intra-organizational policies and practices, yet more collaboration is needed to create a cohesive framework for the continued safety and security of the air domain.

Points of Collaboration and Gaps in Approaches

The above-mentioned standards and guidance focus on adopting a strict IT approach to cybersecurity; however, as explained in the previous section examining the nexus of cyber and air domains, the aviation ecosystem is a mix of IT and operational and platform technologies. In the aviation sector, these technologies exist in different operating environments and use various cybersecurity approaches. For instance, IT cybersecurity generally follows guidance that is based on controls[89] and compliance, whereas aviation safety encompasses a mixture of certification and

85 International Civil Aviation Organization, *Cybersecurity Action Plan*.

86 The seventh pillar of the International Civil Aviation Organization's Cybersecurity Strategy is "Capacity Building, Training and Cybersecurity Culture."

87 International Civil Aviation Organization, *Cybersecurity Action Plan*, p. 5.

88 International Civil Aviation Organization, *Annex 17 to the Convention on International Aviation: Aviation Security*.

89 For example, NIST publication 800-53, *Security and Privacy Controls for Information Systems and Organizations* (https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final) is a controls-based approach to cybersecurity and often cited as the IT industry's standard for effective cybersecurity. Similarly, the Canadian Centre for Cyber Security's guide, *IT Security Risk Management: A Lifecycle Approach (ITSG-33)*, is

risk-based regulations.[90] In the IT operating environment, devices and servers have a persistent connection, air-gapped (generally, removable storage) devices shuffle data between systems and system software is updated regularly; usually, only some of these updates include firmware. Platform technologies also require firmware updates are usually air-gapped and rarely achieve persistent connectivity. Software updates for IT systems that have persistent connectivity are different because, when a patch is released, installation is just a few mouse clicks away or accomplished automatically. On the other hand, for platform technology systems, the update must be scheduled along with regular maintenance. It is difficult for current international standards and guidance to address aviation-specific technology considerations and cybersecurity-specific risks, all while meeting the growing need for a cybersecurity culture that views humans as the solution.

In the preceding section, we identified and assessed the existing theoretical and practical frameworks relating to aviation and cybersecurity—singularly and in combination. In our assessment, a human-centric approach to aviation cybersecurity is generally lacking, either in terms of clarity or in the meaningful integration of such an approach in practical standards and guidance at organizational, national, and international levels. The human-as-problem view is still dominant within the practical approaches to cyber resilience, although we have argued for the meaningful incorporation of humans as part of the solution for addressing the complex and interconnected aviation and cyber ecosystem. In the next section, we take the best practices we have identified within the above-mentioned standards and guidelines and consider a human-centric approach to cyber resiliency so that we can build a more holistic cybersecurity culture and develop a new framework for use in aviation.

Introducing the Inter-Organization Learning Culture Framework for Aviation Cybersecurity

We propose a new framework for aviation cybersecurity: the Inter-Organization Learning Culture (IOLC). This framework is meant to develop the capacity of organizations that have a common interest in observing and fixing the deficiencies in their cybersecurity resilience and distributing these learned experiences to others. The path to developing and incorporating the IOLC starts with organizations elevating cybersecurity resilience by seeing humans and technologies as solutions to the specific challenges within the aviation cybersecurity landscape.

primarily a catalogue of security controls that government departments need to achieve an authority to operate (https://www.cyber.gc.ca/en/guidance/it-security-risk-management-lifecycle-approach-itsg-33).

[90] The International Air Transport Association has a safety management system that includes two types of audits (a standard safety audit and an operational safety audit) focused on identifying hazards and generating a risk assessment (https://www.iata.org/en/programs/safety/safety-management-system/).

Our framework draws on elements from the NIST framework, the ICAO *Cybersecurity Action Plan*, the concept of *coopetition*, and the model of a learning organization. We describe each of these elements in this section and demonstrate their connection to cyber resiliency in a model that embeds a human-as-solution approach to cybersecurity.

For the IOLC framework to succeed, its adoption must extend beyond a single organization, and all actors within the aviation ecosystem must be compelled to participate, interact, and learn from each other. The implementation of the framework is accomplished through three steps:[91]

- implement broad cybersecurity education
- grant relative immunity and confidentiality in reporting, and
- encourage leadership that engenders a culture of active learning about cybersecurity.

In the first step, organizations would need to familiarize their employees with the NIST framework. This would help them understand, at a level applicable to their work, the concepts and terms associated with cybersecurity. Furthermore, the NIST framework provides a structure, particularly its six core functions, that employees can connect to their day-to-day jobs. This education needs to not only identify cybersecurity risks but also demonstrate how cybersecurity incidents occur and how they can be prevented by an individual who is aware and empowered at the right time and place. This employee education needs to extend beyond the simple identification and reporting of risks to focus on the uniqueness of humans in the security process, leverage the potential for creative thinking, and extend into an examination of potential risk conditions.

The second step is about encouraging a subtle culture shift within the organization to give employees permission to identify and report incidents and any risks related to cybersecurity. Every employee assumes some personal risk when they find the courage to report something that may be within the ordinary but that does not feel right or that they believe may rise to the level of a cybersecurity incident. They need to feel psychologically secure, knowing their reporting will not endanger their status or employment. Furthermore, they need to understand the guidelines and boundaries for sharing information and the lessons learned outside their immediate organization. This recognition of the human as an active participant helps not only the organization, it also contributes to the betterment of the aviation ecosystem as a whole. Workers

[91] These three steps broadly replicate the three building blocks that reinforce learning—psychological safety, concrete learning processes, and practices and leadership—advocated by Garvin et al. in "Is Yours a Learning Organization?" *Harvard Business Review*, March 2008, https://hbr.org/2008/03/is-yours-a-learning-organization.

need to feel psychologically safe before they can learn and grow. For an organization to thrive and adapt, its people need to be able to take risks without fear of reprisal.[92]

The third step is to promote leadership that reinforces learning throughout the organization, both laterally and vertically. The full realization of the IOLC framework cannot happen unless leaders at all levels of an organization are willing to inculcate the change needed to develop a cybersecurity culture. Cybersecurity education comes from a culture of learning and a willingness to examine what constitutes a potential cyber threat to the organization. Leaders need to promote open questioning and analysis with the goal of fostering a dialogue. Once again, this furthers a human-as-solution approach, one that makes the best use of people as active nodes where they see themselves as part of an ongoing conversation about the cybersecurity problem rather than as an impediment to reducing cybersecurity risks. A culture of active observation, learning, and dialogue will aid in improving the overall resiliency of the aviation cybersecurity ecosystem.

Cyber resiliency is an important outcome of a cybersecurity culture that needs to be learned, practised, and led by people as part of interconnected digital–packed infrastructures. Broad-based cyber resiliency comes from communication and collaboration.[93] One person or one small team will not have all the answers to solve every cyber problem; however, everyone will benefit if employees are given the opportunity to share their knowledge with others, both within and outside their domains of excellence and areas of concern, including with colleagues who are solving the same problem. As noted under the first pillar of the ICAO's *Cybersecurity Action Plan*, involved stakeholders must recognize that the aviation ecosystem includes interconnected technologies that enable the flow of information to spread between organizations.[94]

Thus, cyber resiliency must include a cooperative community that extends well beyond the organization itself and thrives within the tangled web of private companies, government entities, and interested citizens. This includes extending the learning beyond the immediate technological domain of concern.[95] Community cooperation is not always easy, especially among

---

92 Adam Grant, "Building a Culture of Learning at Work," *Strategy + Business*, 3 February 2021, https://www.strategy-business.com/article/Building-a-culture-of-learning-at-work.

93 Bobbie Stempfley, "Cybersecurity Collaboration as a National Imperative," National Cybersecurity Alliance, 5 October 2022, https://www.staysafeonline.org/articles/cybersecurity-collaboration-as-a-national-imperative.

94 International Civil Aviation Organization, *Cybersecurity Action Plan*, p. 5.

95 As mentioned earlier, cybersecurity can be broadly divided into three technological domains: platform, operational and informational.

actors who may seek to compete with each other. Drawing on the concept of "coopetition"[96] provides an opportunity to frame effective community cooperation within the aviation cybersecurity ecosystem.

Coopetition, simply stated, is a collaboration between competing firms.[97] According to Bengtsson and Kock,[98] this unlikely combination of cooperation between businesses in some activities while still competing in other—usually money-generating—activities would seem to be a paradox at first glance, but it occurs regularly in many markets. Coopetition is important to the IOLC framework because we need firms to be able to work collaboratively—in this case, in cybersecurity—while at the same time respecting their need to generate revenue through their regular business. Coopetition occurs when business leaders seek to form limited partnerships with other businesses in the same industry, with the understanding that through various cooperative behaviours, the industry as a whole will benefit. However, as Bouncken and Fredrich[99] note, the degree to which competing firms will engage in cooperative behaviour is a function of the trust relationship with the other firm(s). Notably, in their research, the authors found that greater trust relationships increase incremental innovation. Bridging this concept from the business literature to cybersecurity, stakeholders should engage in cooperation to ensure their sector remains secure from a cyberattack. In applying coopetition to aviation cybersecurity, all actors from all levels within the ecosystem would share a common understanding of the shared benefit of working toward reducing cybersecurity risks. The role of coopetition within the IOLC framework is to foster collaborations to establish communities and develop a shared culture of cybersecurity while still permitting businesses to pursue their economic goals.

From the NORAD perspective and its mission to monitor and defend North America, this means leveraging the "deter" component of its mission and engaging with the aviation ecosystem to become an active participant. Following the human-centric premise of the IOLC framework, cyber specialists within NORAD would need to be selected specifically to interact with and

---

96 Ricarda B. Bouncken et al., "Coopetition: A Systematic Review, Synthesis, and Future Research Directions," *Review of Managerial Science*, 9 (24 March 2015): pp. 577–601, https://doi.org/10.1007/s11846-015-0168-6.

97 Paavo Ritala, "Coopetition Strategy: When Is It Successful? Empirical Evidence on Innovation and Market Performance," *British Journal of Management*, 23, no. 3 (September 2012): pp. 307–332, https://doi.org/10.1111/j.1467-8551.2011.00741.x.

98 Maria Bengtsson et al., "'Coopetition' in Business Networks: Cooperate and Compete Simultaneously," *Industrial Marketing Management* (September 2000); pp. 411–426, https://doi.org/10.1016/S0019-8501(99)00067-X.

99 Ricarda Bouncken et al., "Coopetition: Performance Implications and Management Antecedents," *International Journal of Innovation Management*, 16, no. 05 (November 2012); pp. 1–28, https://doi.org/10.1142/S1363919612500284.

become participants in specific communities within the aviation ecosystem. This is an opportunity for NORAD to provide leadership and encourage the various players in this ecosystem to engage and begin thinking through the organizational benefits of the IOLC framework. Since the IOLC framework depends on the aforementioned concept of competition, the success of which is based on trust relationships, this is a role that NORAD could fulfill as an impartial player to bring otherwise uncooperative organizations together. Furthermore, individuals within NORAD could be engaged to leverage their own cybersecurity expertise and experiences[100] to assist the aviation ecosystem toward achieving outcomes that result in a more cyber-resilient posture. Any activity that increases the security of North American air traffic and the services that manage it is in the interest of NORAD. A properly managed airspace reduces the potential for a domestically sourced attack and helps NORAD function in a modern world with multi-domain threats. Given that NORAD is a binational military command organization formalized by a defence agreement that spans two countries with a single, jointly managed airspace, its involvement in and active cultivation of the IOLC framework within the aviation ecosystem would support its mission of defending North America and maintaining air sovereignty.

We further show the usefulness of our concept by drawing on our hypothetical scenario from the Introduction section of this paper and applying it within the context of addressing the growing need for cybersecurity cooperation in North America.

Applying the IOLC Framework

If we return to the hypothetical example presented earlier, we can examine the multiple points of failure that demonstrate the interconnection of humans, technologies, and digital–physical infrastructures generally, and air safety and security. We will limit our analysis to three parts: the supply chain, the avionics architecture, and the flight crew.

In the first part of the example, the aircraft maintenance company made a poor choice when it selected its avionics supplier. (The importance of having strong risk-management processes for the supply chain is discussed in the NIST framework.[101]) Leaders who discover their organization's supply chain has been compromised would start a conversation with employees about the organization's process for selecting components and check to see whether any of the

[100] While the IOLC framework works best when information is shared and transparency is maximized, we recognize that classified military information would not be shareable.

[101] Specifically, all the outcomes related to GV.SC (Cybersecurity Supply Chain Risk Management). *NIST Cybersecurity Framework (CSF) 2.0*, pp. 17–18.

NIST framework's outcomes related to supply chain management had been achieved. Leadership would be a key part of this process, directing an open and honest dialogue with everyone involved in the acquisition and handling of the supplied parts, without fear of reprisal. Employees who are further empowered by the IOLC framework would reach out to their colleagues in other maintenance companies to learn from their experiences in supply chain integrity and how they achieve the outcomes of the NIST framework. Following that step, they would seek to change, at their level, the processes that manage their supply chain. Employees would be encouraged to be active security managers of the supply chain, continuously seeking to make it more secure at every step. Changes to the process and the reasons behind it would be shared with current and potential suppliers. These changes would be shared with other maintenance companies while explaining how the affected company improved the security of its supply chain. This knowledge would flow back to the others involved to enable them to further their internal dialogue and, in turn, ask their questions about their supply chain. These businesses would relay their experiences about what transpired to government authorities, which could lead to changes to relevant government regulations. Government entities would seek their own investigations into aspects of North American supply chain integrity, especially if this is not an isolated incident. NORAD could find a place for itself by being the catalyst for sparking dialogue on supply chain integrity and leveraging its contacts within constituent-supporting maintenance organizations in the Royal Canadian Air Force and the US Air Force and their civilian counterparts to build a community of practitioners. In this part of the hypothetical example, the maintenance companies would have leaders who recognize the value of conversations and communication and encourage this not just within their company, but also externally. The human participants of the organizations would thus form the core of the solution and continuously participate in a cycle of improvement. NORAD could be the impartial arbiter of any agreements and feed the community of practice by providing a set of cloud-based services that would host digital tools, venues, and spaces to facilitate the formal and informal collaboration required to make the IOLC work.

The next point of examination in the hypothetical example would be the manufacturer of the avionics system and its connections to the in-flight entertainment system. Following the incident in our hypothetical example, engineers would evaluate their organization in the context of the outcomes described in the NIST framework[102] to help them determine how they could have engineered their system to be more resilient. Similar to the supply chain part of this example, the leadership would encourage frank and honest discussions about their company's engineering

[102] The six outcomes under the Protect core function in the Platform Security (PR.PS) category would be applicable. *NIST Cybersecurity Framework (CSF) 2.0*, 20.

processes using the people-as-solution perspective. Not only could they reach out to their colleagues in the same business, but they could also leverage ideas and inputs from the academic world on more resilient designs (i.e., the cybersecurity platforms) and deployment techniques. Upon learning and incorporating principles related to a more resilient design, they could share these principles (if not the details) with their competitors who, in turn, could leverage them in their own designs or find defects that would have otherwise been overlooked. In an expanded cybersecurity culture, these engineers would be empowered to share their knowledge with the other two domains (i.e., operational and informational) so they could potentially increase their cybersecurity resiliency and, ultimately, the safety of all aircraft in general.

The last area in this example involves the flight crew on the affected aircraft. While one would not expect crew members to be cybersecurity experts, they are full participants in the safety of the aircraft and, by proxy, its cybersecurity resilience. Specific parts of the NIST framework[103] apply in this case, and specific outcomes and general cybersecurity practices would therefore need to be taught to the flight crew. In our hypothetical example, a review of the incident would likely show the members of the flight crew were unaware of how passengers could physically gain access to sensitive aircraft systems (e.g., using a hidden port), or perhaps they were unaware of what constitutes suspicious behaviour in a cyber context. Such activity, if observed by the flight crew, could be cause for restraining the passenger(s), alerting the flight deck, and warning air traffic control authorities. Suspicious aircraft performance and other deviations might be cause for alerting NORAD. Addressing this could involve a review of crew procedures for the active monitoring of passengers in all phases of flight, and leadership could, once again, inspire the flight crew to construct meaningful questions about all aspects of safety and how they conduct their jobs. The crew-specific cybersecurity community could be engaged to learn new ways of managing passengers, and the government could be consulted for advice and information sharing.

The details in these examples show that the cybersecurity resiliency of an aircraft and its capacity for safe and controlled flight within NORAD airspace is dependent on the active participation of many different actors with vastly different roles within the North American aviation ecosystem. While NORAD is not necessarily a proactive participant in all of these situations, it is still responsible for ensuring that air traffic is safe and carefully managed. The active participation of NORAD would enable the US and Canada to leverage this framework and foster an open dialogue and continual engagement. In our example, given that NORAD would have been informed so that it could respond to and deal with the threat, it is implicit that NORAD

[103] Two outcomes under the Protect core function in the Awareness and Training (PR.AT) category would apply in this specific case. *NIST Cybersecurity Framework (CSF) 2.0*, page 20.

would also perform its own after-action analysis. Assuming that NORAD has, per the IOLC, built bridges to its civilian partners, the reflection and feedback loops within its partner network would be primed to seize upon NORAD's experience and insights and promulgate—within and beyond their organizations—the lessons learned from the after-action report to prevent the situation from reoccurring.

While the concept of the IOLC framework is comprehensive, it still has its limitations. The biggest limitation is the capacity of the leadership within organizations to drive genuine change. Human-centric systems require the active participation of individuals at all levels and in all disciplines. If we are focused on motivating people to see themselves as part of the solution, the IOLC framework must have enlightened, engaged supporters in all divisions of a company. Cybersecurity is everyone's responsibility; an organization cannot implement effective cybersecurity measures in pieces. Another limitation is the need for cybersecurity professionals to relate the outcomes of the NIST framework to the specific roles of the individuals within the organization. The outcomes from the framework are deliberately non-prescriptive so as to be universal in their application, but they still require expertise in both the cybersecurity domain and the area of relevance to which they are applied. One other area worth mentioning in the context of NORAD modernization and all-domain awareness is the limitations of current technology. Ideally, all enabled cyber devices would be networked with intrusion detection systems that could learn of potential intrusions in either the flying platforms or the operational systems on the ground and report this back to NORAD. This sort of advanced reporting is limited by the processing and connectivity limitations inherent in platform technology. As for operational technology, it may very well be constrained by the limits of authority between military and civilian operators. One could envision a limited system on aircraft that could sense a cyber intrusion and then transmit any issues through Automatic Dependent Surveillance-Broadcast or related transponder technology, but that would remain the subject for future discussion.

Finally, leaders need to promote sustained and continuous cybersecurity awareness. If the pathways of communication and the cycles of self-analysis are broken, then the dialogue will stagnate and the resilience will decay. Our adversaries are engaged in a relentless attack on our infrastructure; they will never rest, and nor should we.

Summary and Concluding Thoughts

At the beginning of this paper, we opened with two real-world examples and one hypothetical scenario regarding cybersecurity-related incidents, threats, and actors that are seemingly specific to the aviation ecosystem. During the course of this paper, we gradually demonstrated that aviation cybersecurity is a complex endeavour. Current approaches to ensuring safety and security at the nexus of the air and cyber domains are challenging for states and non-state actors within the aviation ecosystem. In our analysis of existing theoretical frameworks and practical approaches, we found there was an opportunity to advance aviation cybersecurity by positioning humans as part of the solution. In light of this aim, we proposed a new framework for consideration: the IOLC. By combining best practices from existing guidance, standards, and human-as-solution concepts, we created and applied the IOLC framework to our hypothetical scenario. The goal of this paper was ultimately to recognize the importance of cooperation between state and non-state actors within the aviation ecosystem, with an emphasis on strengthening NORAD cooperation. This cooperation can be seen as interoperable, with a focus on technology and human- and cyber-centric design, resulting in a shared cybersecurity culture between allies.

In closing, we would like to emphasize the importance of leaders and practitioners moving forward strategically using an aviation cybersecurity framework such as the IOLC. We acknowledge that our framework will not solve every problem and that connecting leaders, practitioners and ideas to complex and challenging areas is a challenge in itself. Nevertheless, our framework provides an opportunity to continue important discussions on the topic of North American air safety and security writ large, with the intention that the IOLC framework could be tailored and adapted to context-specific needs.

References

American Institute of Aeronautics and Astronautics. "Aerospace Cybersecurity: Enduring Challenges Enduring Solutions." Accessed 31 December 2024. https://www.aiaa.org/docs/default-source/uploadedfiles/issues-and-advocacy/policy-papers/whitepaper-cybersecurity-based-on-research-study-2021-srl.pdf/1000.

Antoniuk, Daryna. "Suspected Iranian Hackers Target Israeli Shipping and Logistics Companies." *The Record Recorded Future News*, 23 May 2023. https://therecord.media/israel-shipping-logistics-watering-hole-cyberattacks.

Badawey, Vance. "A Study of Aircraft Certification in Canada in Light of Two Incidents Involving Lion Air Flight 610 and Ethiopian Airlines Flight 302." *Report of the Standing Committee on Transport, Infrastructure and Communities, 43rd Parliament, 2nd Session.* Ottawa: Government of Canada. June 2021. https://www.ourcommons.ca/DocumentViewer/en/43-2/TRAN/report-2/page-39.

Baltuttis, Dennik, Timm Teubner, and Marc T. P. Adam. "A Typology of Cybersecurity Behavior Among Knowledge Workers." *Computers & Security*, 140 (May 2024): 103741. https://doi.org/10.1016/j.cose.2024.103741.

Barno, David and Nora Bensahel. "Drones, the Air Littoral, and the Looming Irrelevance of the US Air Force." *War on the Rocks*, 7 March 2024. https://warontherocks.com/2024/03/drones-the-air-littoral-and-the-looming-irrelevance-of-the-u-s-air-force/.

Bengtsson, Maria and Sören Kock. "'Coopetition' in Business Networks: Cooperate and Compete Simultaneously." *Industrial Marketing Management* (September 2000): pp. 411–426. https://doi.org/10.1016/S0019-8501(99)00067-X.

Bouncken, Ricarda and Viktor Fredrich. "Coopetition: Performance Implications and Management Antecedents." *International Journal of Innovation Management*, 16, no. 05 (November 2012): pp. 1–28. https://doi.org/10.1142/S1363919612500284.

Bouncken, Ricarda B., Johanna Gast, Sascha Kraus, and Marcel Bogers. "Coopetition: A Systematic Review, Synthesis, and Future Research Directions." *Review of Managerial Science* (24 March 2015): pp. 577–601. https://doi.org/10.1007/s11846-015-0168-6.

Bureau d'Enquêtes et d'Analyses [BEA] pour la sécurité de l'aviation civile. *Final Report on the Accident on 1st June 2009 to the Airbus A330-203 Registered F-GZCP Operated by Air France*

Flight AF 447 Rio de Janeiro – Paris. Translated by BEA from French. 11 July 2012. https://bea.aero/docspa/2009/f-cp090601.en/pdf/f-cp090601.en.pdf.

Canada. Department of National Defence. "Fact Sheet: Funding for Continental Defence and NORAD Modernization." Last modified 21 July 2022. https://www.canada.ca/en/department-national-defence/services/operations/allies-partners/norad/facesheet-funding-norad-modernization.html.

Canada. Department of National Defence. *RCAF [Royal Canadian Air Force] Strategy: Agile,·Integrated,·Inclusive*. February 2023. Ottawa: Government of Canada. https://www.canada.ca/content/dam/rcaf-arc/documents/reports-publications/royal-canadian-air-force-strategy-portrait.pdf.

Canada. Department of National Defence. "Canadian Armed Forces Digital Campaign Plan." Last modified 28 February 2023. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/canadian-armed-forces-digital-campaign-plan.html.

Canada. Department of National Defence. "Annex C: Canada's NORAD Modernization Plan." Last modified 17 April 2024. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/north-strong-free-2024/annex-c-canada-norad-modernization-plan.html.

Canada. Department of National Defence. "Fact Sheet: NORAD Modernization Project Timelines." Last modified 9 May 2024. https://www.canada.ca/en/department-national-defence/services/operations/allies-partners/norad/norad-modernization-project-timelines.html.

Canada. Department of National Defence. *Our North, Strong and Free: A Renewed Vision for Canada's Defence*, Government of Canada, 2024. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/north-strong-free-2024.html.

Canadian Centre for Cyber Security. *IT Security Risk Management: A Lifecycle Approach (ITSG-33)*, Government of Canada. Last modified 1 November 2012. https://www.cyber.gc.ca/en/guidance/it-security-risk-management-lifecycle-approach-itsg-33.

Canadian Centre for Cyber Security. "Alert: Distributed Denial of Service Campaign Targeting Multiple Canadian Sectors." Ottawa: Government of Canada. September 15, 2023. https://www.cyber.gc.ca/en/alerts-advisories/distributed-denial-service-campaign-targeting-multiple-canadian-sectors#fn1-rf.

Charron, Andrea. "Responding to 'Hardening the SHIELD: A Credible Deterrent and Capable Defense for North America.'" In *Shielding North America: Canada's Role in NORAD Modernization*, edited by Nancy Teeple and Ryan Dean. Peterborough, ON: North American and Arctic Defence and Security Network, 2021: pp. 84–89. https://www.naadsn.ca/wp-content/uploads/2021/03/NAADSN-engage4-NORAD-NT-RD-upload.pdf.

Charron, Andrea and James G. Fergusson. *NORAD: In Perpetuity and Beyond* (Montreal: McGill-Queen's University Press, 2022).

Chor, Major Jason. "The CAF Digital Campaign Plan: Digital Transformation in Jeopardy." JCSP 49 Service Paper. Canadian Forces College, pp. 2022–2023. https://www.cfc.forces.gc.ca/259/290/49/192/Chor.pdf.

Cohen, Rachel S. "Pentagon's Silicon Valley Hub Is Helping NORAD Monitor US Airspace." *Air & Space Forces Magazine*, 23 October 2020. https://www.airandspaceforces.com/pentagons-silicon-valley-hub-is-helping-norad-monitor-us-airspace/.

Cooper, Pete, Simon Handler, and Safa Shahwan. *Aviation Cybersecurity: Scoping the Challenge*. Atlantic Council, 11 December 2019. https://www.atlanticcouncil.org/in-depth-research-reports/report/aviation-cybersecurity-scoping-the-challenge-report/.

Csenkey, Kristen, D. P. Genest, and Canadian Intelligence Corps. "An Opportunity for NORAD Modernization in a Joint CA-US Cyber Component." *Strategic Perspectives*, North American and Arctic Defence and Security Network, 2021. https://www.naadsn.ca/wp-content/uploads/2021/01/Strategic-Perspectives-An-Opportunity-for-NORAD-Modernization-in-a-Joint-CA-US-Cyber-Component-21jan.pdf.

Dekker, Sidney. *Safety Differently*. London: CRC Press, 2014.

Dunn Cavelty, Myriam. "The Militarisation of Cyberspace: Why Less May Be Better." in *Proceedings of the 4th International Conference on Cyber Conflict*. Tallinn, Estonia, June 5–8, 2012. CCD COE Publications: pp. 141–154. https://ccdcoe.org/uploads/2019/03/CyCon_book_2012.pdf.

Dunn Cavelty, Myriam. "Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities." *Science and Engineering Ethics,* 20 (2014): pp. 701–715. https://doi.org/10.1007/s11948-014-9551-y.

Ebert, Nico, Thierry Schaltegger, Benjamin Ambuehl, Lorin Schöni, Verena Zimmermann, and Melanie Knieps. "Learning from Safety Science: A Way Forward for Studying Cybersecurity Incidents in Organizations." *Computers & Security*, 134 (November 2023): 103435. https://doi.org/10.1016/j.cose.2023.103435.

Femath, Juan. "Reoptimization for Great Power Competition." US Air Force, March 2024. https://www.af.mil/reoptimization-for-great-power-competition/.

Freiherr, Greg. "Will Your Airliner Get Hacked?" *Smithsonian Magazine*. Air & Space Magazine, February 2021. https://www.smithsonianmag.com/air-space-magazine/will-your-airliner-get-hacked-180976752/.

Garvin, David, Amy Edmonson, and Francesca Gino, "Is Yours a Learning Organization?" *Harvard Business Review*, March 2008. https://hbr.org/2008/03/is-yours-a-learning-organization.

Grant, Adam, "Building a Culture of Learning at Work," *Strategy + Business*, 3 February 2021. https://www.strategy-business.com/article/Building-a-culture-of-learning-at-work.

Greenberg, Andy. "Facebook Catches Iranian Spies Catfishing US Military Targets." *WIRED, 15* July 2021. https://www.wired.com/story/facebook-iran-espionage-catfishing-us-military/.

Grobler, Marthie, Raj Gaire, and Surya Nepal. "User, Usage and Usability: Redefining Human Centric Cyber Security." *Frontiers in Big Data,* 4 (2021): pp. 583723–583723. https://doi.org/10.3389/fdata.2021.583723.

Hak5. "LAN Turtle" (product). Accessed 31 December 2024. https://shop.hak5.org/products/lan-turtle.

Hak5. "Shark Jack" (product). Accessed 31 December 2024. https://shop.hak5.org/products/shark-jack?variant=21284894670961.

Haney, Julie and Jody Jacobs. "NIST Unveils Newly Named Human-Centered Cybersecurity Program." *Cybersecurity Insights* (blog). National Institute of Standards and Technology. September 28, 2023. https://www.nist.gov/blogs/cybersecurity-insights/nist-unveils-newly-named-human-centered-cybersecurity-program.

Hilowle, Malyun, William Yeoh, Marthie Grobler, Graeme Pye, and Frank Jiang. "Users' Adoption of National Digital Identity Systems: Human-Centric Cybersecurity Review." *Journal of Computer Information Systems*, 63, no. 5 (2023): pp. 1264–1279. https://doi.org/10.1080/08874417.2022.2140089.

International Air Transportation Association. *Aviation Cybersecurity Fact Sheet*, November 2023. https://www.iata.org/en/iata-repository/pressroom/fact-sheets/fact-sheet--cyber-security/.

International Air Transportation Association. "Aviation Cyber Security." Accessed 31 December 2024. https://www.iata.org/en/programs/security/cyber-security/.

International Air Transport Association. "Safety Management System." Accessed 31December 2024. https://www.iata.org/en/programs/safety/safety-management-system/.

International Civil Aviation Organization. *Security and Facilitation Strategic Objective: Aviation Cybersecurity Strategy*. October 2019. https://www.icao.int/aviationcybersecurity/Documents/AVIATION%20CYBERSECURITY%20STRATEGY.EN.pdf.

International Civil Aviation Organization. *Cybersecurity Action Plan.* 2nd ed. January 2022. https://www.icao.int/aviationcybersecurity/Documents/CYBERSECURITY%20ACTION%20PLAN%20-%20Second%20edition.EN.pdf.

International Civil Aviation Organization. *Cybersecurity Culture in Civil Aviation.* January 2022. https://www.icao.int/aviationcybersecurity/Documents/Cybersecurity%20Culture%20in%20Civil%20Aviation.EN.pdf.

International Civil Aviation Organization. *Cybersecurity Policy Guidance.* January 2022. https://www.icao.int/aviationcybersecurity/Documents/Cybersecurity%20Policy%20Guidance.EN.pdf.

International Civil Aviation Organization, *Annex 17 to the Convention on International Aviation: Aviation Security*. 12th ed. July 2022.

International Civil Aviation Organization. "Member States." Accessed December 31, 2024. https://www.icao.int/about-icao/Pages/member-states.aspx.

International Civil Aviation Organization. "Strategic Objectives." Accessed 31 December 2024. https://www.icao.int/about-icao/Council/Pages/Strategic-Objectives.aspx.

International Civil Aviation Organization. *Resolution A40-10: Addressing Cybersecurity in Civil Aviation.* Accessed 31 December 2024. https://www.icao.int/aviationcybersecurity/Documents/A40-10.pdf.

International Civil Aviation Organization, *Resolution A41-19: Addressing Cybersecurity in Civil Aviation.* Accessed 31 December 2024. https://www.icao.int/aviationcybersecurity/Documents/A41-19.pdf.

International Civil Aviation Organization. "Vision and Mission to 2025." Accessed 31 December 2024. https://www.icao.int/about-icao/Council/Pages/vision-and-mission.aspx.

Johnson, L., Kelley Dempsey, Ron Ross, Sarbari Gupta, and Dennis Bailey. *Guide for Security-Focused Configuration Management of Information Systems.* NIST Special Publication 800-128, National Institute of Standards and Technology Computer Security Resource Center. US Department of Commerce. https://csrc.nist.gov/pubs/sp/800/128/upd1/final.

Khaitan, Ashish. "Cyber Attacks on Canadian Airports Have Disrupted Operations." *The Cyber Express*, 21 September 2023. https://thecyberexpress.com/cyber-attacks-on-canadian-airports-disrupt-ops/.

Kumar, Sheetal. "The Missing Piece in Human-Centric Approaches to Cybernorms Implementation: The Role of Civil Society." *Journal of Cyber Policy* 6, no. 3 (2021): pp. 375–393. https://doi.org/10.1080/23738871.2021.1909090.

Larin, Vincent and Hugo Joncas. "Agence des services frontaliers: La panne dans les aéroports provenait bien d'une attaque informatique." [Border Services Agency: The outage at the airports was due to a cyber attack]. *La Presse*, 19 September 2023. https://www.lapresse.ca/actualites/national/2023-09-19/agence-des-services-frontaliers/la-panne-dans-les-aeroports-provenait-bien-d-une-attaque-informatique.php.

Li, Ling, Wu He, Li Xu, Ivan Ash, Mohd Anwar, and Xiaohong Yuan. "Investigating the Impact of Cybersecurity Policy Awareness on Employees' Cybersecurity Behavior." *International Journal of Information Management*, 45 (April 2019): pp. 13–24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017.

McClary, Rob, *Building Mutual Trust Between Soldiers and Leaders.* White paper. US Army Combined Arms Center. https://cdm16040.contentdm.oclc.org/digital/collection/p16040coll2/id/16.

Mermoud, Alain, Marcus Matthias Keupp, Kévin Huguenin, Maximilian Palmié, Dimitri Percia David. "To Share or Not to Share: A Behavioral Perspective on Human Participation in Security Information Sharing." *Journal of Cybersecurity*, 5, no. 1 (2019), pp. 1–13. https://doi.org/10.1093/cybsec/tyz006

National Institute of Standards and Technology. "CSF 1.1 Success Stories Archive." Accessed December 31, 2024. https://www.nist.gov/cyberframework/success-stories.

National Institute of Standards and Technology. *NIST Cybersecurity Framework (CSF) 2.0*. National Institute of Standards and Technology Computer Security Resource Center. US Department of Commerce. 26 February 2024. https://doi.org/10.6028/NIST.CSWP.29.

National Institute of Standards and Technology. *Security and Privacy Controls for Information Systems and Organizations*, NIST SP 800-53 Rev. 5. Accessed 31 December 2024. https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final.

Nicols, Marc. "What a Tangled Web: Aviation Prosperity, Cybersecurity Risk." Address to the International Air Law Conference on Aviation Cybersecurity, Leiden, Netherlands, 11 May 2023. https://www.faa.gov/speeches/what-tangled-web-aviation-prosperity-cybersecurity-risk.

Nobles, Calvin, Darrell Burrell, and Tyrone Waller. "The Need for a Global Aviation Cybersecurity Defense Policy." *Land Forces Academy Review* 27, no. 1 (March 2022): pp. 19–26. https://doi.org/10.2478/raft-2022-0003.

O'Shaughnessy, General Terrence J. and Brigadier General Peter M. Fesler. *Hardening the Shield: A Credible Deterrent & Capable Defense for North America.* Washington, DC: The Wilson Center, September 2020. https://www.wilsoncenter.org/sites/default/files/media/uploads/documents/Hardening%20the%20Shield_A%20Credible%20Deterrent%20%26%20Capable%20Defense%20for%20North%20America_EN.pdf.

Pollini, Alessandro, Tiziana C. Callari, Alessandra Tedeschi, Daniele Ruscio, Luca Save, Franco Chiarugi, and Davide Guerri. "Leveraging Human Factors in Cybersecurity: An Integrated Methodological Approach." *Cognition, Technology & Work*, 24, no. 2 (May 2022): pp. 371–390. https://doi.org/10.1007/s10111-021-00683-y.

Ritala, Paavo. "Coopetition Strategy: When Is It Successful? Empirical Evidence on Innovation and Market Performance." *British Journal of Management*, 23, no. 3 (September 2012): pp. 307–332. https://doi.org/10.1111/j.1467-8551.2011.00741.x.

Roberts, Karlene H. "New Challenges in Organizational Research: High-Reliability Organizations." *Industrial Crisis Quarterly* 3, no. 2 (1989): pp. 111–125. https://doi.org/10.1177/108602668900300202.

Ross, Ron, Victoria Pillitteri, Richard Graubart, Deborah Bodeau, and Rosalie McQuaid. *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*." NIST Special Publication 800-160 Vol. 2, National Institute of Standards and Technology, US Department of Commerce. December 2021. https://doi.org/10.6028/NIST.SP.800-160v2r1.

Rozmann, Ofir, Chen Evgi, and Johnathan Leathery. "When Cats Fly: Suspected Iranian Threat Actor UNC1549 Targets Israeli and Middle East Aerospace and Defense Sectors." *Mandiant*, 27 February 2024. https://www.mandiant.com/resources/blog/suspected-iranian-unc1549-targets-israel-middle-east.

Scaife, Robert B. and Lt. Col. Packard J. Mills. "A Paradigm of Dialogue and Trust: Army Mission Command Training." *Military Review* (January-February 2015). https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20150228_art010.pdf.

Scott, Walter. *Marmion.* Edited by Thomas Bayne (Oxford: Clarendon Press), 1889.

Stempfley, Bobbie. "Cybersecurity Collaboration as a National Imperative." National Cybersecurity Alliance. 5 October 2022. https://www.staysafeonline.org/articles/cybersecurity-collaboration-as-a-national-imperative.

Ukwandu, Elochukwu, Mohamed Amine Ben-Farah, Hanan Hindy, Miroslav Bures, Robert Atkinson, Christos Tachtatzis, Ivan Andonovic, and Xavier Bellekens. "Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends." *Information* 13, no. 3 (2022): 146–. https://doi.org/10.3390/info13030146.

US Department of Defense and Department of National Defence (Canada). "Joint Statement on NORAD Modernization." Press release, 17 August 2021. https://www.defense.gov/News/Releases/Release/Article/2735041/joint-statement-on-norad-modernization/.

US Department of Justice. "Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research." Press release, 19 July 2021. https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion.

US Northern Command. *North American Aerospace Defense Command and United States Northern Command Strategy: Executive Summary*. March 2021. https://www.northcom.mil/Portals/28/(U)%20NORAD-USNORTHCOM%20Strategy%20EXSUM%20-%20Signed.pdf.

Warminsky, Joe. "Suspected Iranian cyber-espionage campaign targets Middle East aerospace, defense industries." *The Record Recorded Future News*, February 28, 2024. https://therecord.media/iran-cyber-espionage-campaign-targeting-middle-east-defense-aerospace.

World Economic Forum. *Pathways Towards a Cyber Resilient Aviation Industry: Insight Report*. April 2021. https://www3.weforum.org/docs/WEF_Pathways_Cyber_Resilient_Aviation_2021.pdf.

Zetter, Kim. "Feds Say That Banned Researcher Commandeered a Plane." *WIRED*, 15 May 2015. https://www.wired.com/2015/05/feds-say-banned-researcher-commandeered-plane/.

Zimmermann, Verena and Karen Renaud. "Moving from a 'Human-as-Problem' to a 'Human-as-Solution' Cybersecurity Mindset." *International Journal of Human-Computer Studies*, 131 (November 2019): pp. 169–187. https://doi.org/10.1016/j.ijhcs.2019.05.005.