National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

CYBER MISSION ASSURANCE

LCol D.W. Brown

JCSP 42

Service Paper

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

PCEMI 42

Étude militaire

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES
JCSP 42 – PCEMI 42
2015 – 2016

JCSP SERVICE PAPER – PCEMI ÉTUDE MILITAIRE

CYBER MISSION ASSURANCE

LCol D.W. Brown

Word Count: 2547

Compte de mots: 2547

CYBER MISSION ASSURANCE

AIM

1. The successes of essentially all current Royal Canadian Air Force (RCAF) operations are dependent on information communicated in and through the cyber environment. Command and control systems, air weapons systems, and sensors are all examples of systems that interact with the cyber environment and are integrally part of in the delivery of air force kinetic and non-kinetic mission effects. This dependence on information and communications technologies (ICT) means that the degradation or denial of the cyber environment can result in mission degradation or even failure.[1] As aviation ICT systems continue to grow in complexity and interconnectedness, existing security and safety efforts do not adequately protect against evolving cyber threats unique to aviation.[2] The aim of this service paper is to identify the need for the RCAF to establish a Cyber Mission Assurance loss prevention programme to safeguard it's capabilities against cyber threats.

INTRODUCTION

Existing Programmes: Generate and Shield

2. Generate. Aviation is an inherently risky business. Generating and employing RCAF capability always involves a degree of risk which may lead to loss of life, casualties, or loss of equipment. Outlined in our Generate doctrine, the RCAF has long established loss prevention programmes to prevent the accidental loss of its limited aviation resources. The Airworthiness and FS programmes enable the generation of operational capabilities while reducing the

[1] Michael D. Pritchett, "Cyber Mission Assurance: A Guide to Reducing the Uncertainties of Operating in a Contested Cyber Environment," (2012): 1, 11; Philippe Legere, "Cyber Is the Commander's Business," *The Canadian Air Force Journal* 4, no. 4 (2011): 59.

[2] American Institute of Aeronautics and Astronautics, *The Connectivity Challenge: Protecting Critical Assets in a Networked World, A Framework for Aviation Cybersecurity*, (n.p.: American Institute of Aeronautics and Astronautics, 2013); Kerri A. Heitner, "Cyber Threats within Civil Aviation," (Ann Arbor, MI: ProQuest, 2014). iii.

accidental attrition of personnel and materiel. These two programmes work jointly, almost exclusively in the physical realm, to enhance the safety of flight.[3]

a. Flight Safety (FS). FS programme strives to eliminate the accidental loss of aviation resources, while enabling the RCAF to accomplish its missions with an acceptable level of risk. The FS programme aims to systematically forecast and identify the risks to air operations and then develop methods to minimize these risks.[4]

b. Airworthiness. The Airworthiness programme ensures that a tolerable level of aviation safety is achieved and maintained for military aviation, as obliged by the Aeronautics Act. The fundamental principles of airworthiness are to ensure maintenance activities are completed to accepted standards, by authorized individuals, within accredited organizations, and using approved procedures.[5]

3. Shield. When considering the cyber environment, the RCAF Shield function deals with the protection of information and allowing that information to be used without interference. Efforts to protect and capitalize on information can be conducted in both the physical and cyber environments. Traditionally electronic warfare effects come from the physical domain and electronic protection measures are used, "to shield friendly forces from the degradation, neutralization, or destruction of their own electronic systems." Alternatively, computer network

[3] Department of National Defence, *B-GA-400-000/FP-000, Canadian Forces Aerospace Doctrine*, 2nd ed. (Trenton, ON: Canadian Forces Aerospace Warfare Centre, 2010): 49-51; Department of National Defence, *B-GA-405-000/FP-001, Canadian Forces Aerospace Shield Doctrine*, 1st ed. (Trenton, ON: Canadian Forces Aerospace Warfare Centre, 2012): 31; Department of National Defence, *A-GA-135-001/AA-001, Flight Safety for the Canadian Forces*, 5th ed. (Ottawa: DND Canada, 2012): 1-1 - 1-8; Department of National Defence, *A-GA-007-000/AF-008, Air Force Vectors*, 1st ed. (Trenton, ON: Canadian Forces Aerospace Warfare Centre, 2014). 44.

[4] Department of National Defence, *A-GA-135-001/AA-001, Flight Safety for the Canadian Forces*, 5th ed. (Ottawa: DND Canada, 2012): 1-1 - 3.

[5] Department of National Defence, *A-GA-135-003/AG-001, Airworthiness Investigation Manual* (Ottawa: DND Canada, 2013): i, 2.

operations (CNO) emanate from the cyber environment and computer network defence is used to protect against the disruption of air operations through the cyber environment.[6]

Threats: Physical, Cyber, and Cyber-Physical

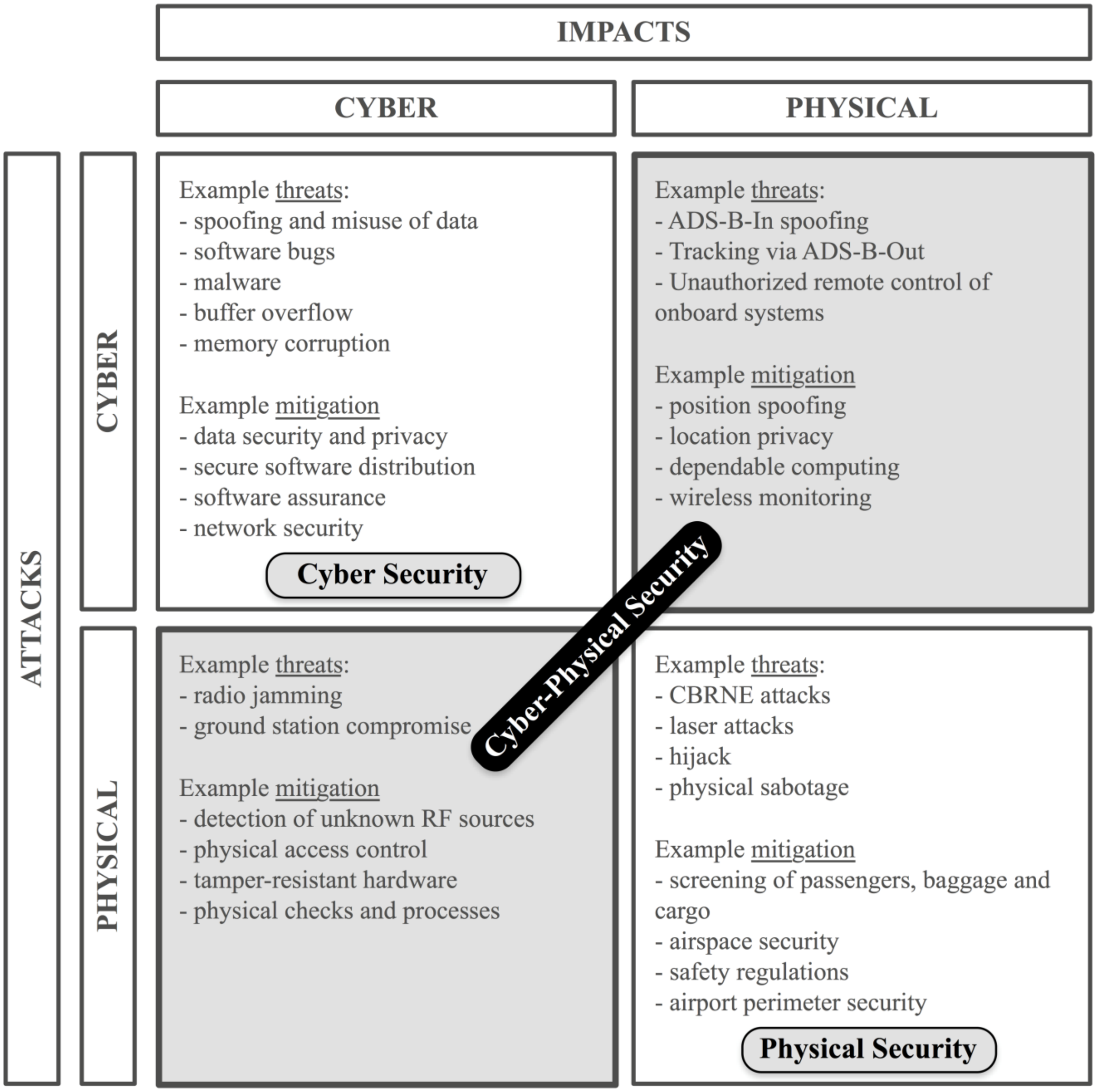
4. The challenge for any air force is to maintain a technological advantage while also countering the vulnerabilities that are inherent with new technology - the leading edge conundrum. The aviation industry at large has already been targeted by cyber-attacks:[7] air traffic management facilities, viruses spreading on electronic flight bags, unmanned aerial vehicles grounded by computer viruses, incidents caused by misuse of maintenance laptop applications, and potential backdoors on embedded processors. Particularly in the realm of aviation, these cyber-attacks have devastating results; they can occur in the physical world, the cyber environment, or in both. Table 1 provides a model for this combined cyber and physical threat to aviation.[8]

Table 1 - Threat model for Aviation Cyber-Physical Security

[6] Department of National Defence, *B-GA-405-000/FP-001, Canadian Forces Aerospace Shield Doctrine,* 1st ed. (Trenton, ON: Canadian Forces Aerospace Warfare Centre, 2012): 20-24.

[7] “An attack is one or more malicious or unintentional actions that exploit one or more vulnerabilities.”
Krishna Sampigethaya and Radha Poovendran, "Aviation Cyber–Physical Systems: Foundations for Future Aircraft and Air Transport," *Proceedings of the IEEE* 101, no. 8 (August 2013): 1849, doi:10.1109/jproc.2012.2235131.

[8] Philippe Legere, "Cyber Is the Commander’s Business," *The Canadian Air Force Journal* 4, no. 4 (2011): 60; Krishna Sampigethaya and Radha Poovendran, "Aviation Cyber–Physical Systems: Foundations for Future Aircraft and Air Transport," *Proceedings of the IEEE* 101, no. 8 (August 2013): 1849, doi:10.1109/jproc.2012.2235131; Silvia Gil Casals, Philippe Owezarski, and Gilles Descargues, "Generic and Autonomous System for Airborne Networks Cyber-Threat Detection,", in 32nd Digital Avionics Systems Conference (n.p.: IEEE, 2013), 4A4–1.



		IMPACTS	
		CYBER	PHYSICAL
ATTACKS	CYBER	Example threats: - spoofing and misuse of data - software bugs - malware - buffer overflow - memory corruption Example mitigation - data security and privacy - secure software distribution - software assurance - network security	Example threats: - ADS-B-In spoofing - Tracking via ADS-B-Out - Unauthorized remote control of onboard systems Example mitigation - position spoofing - location privacy - dependable computing - wireless monitoring
	PHYSICAL	Example threats: - radio jamming - ground station compromise Example mitigation - detection of unknown RF sources - physical access control - tamper-resistant hardware - physical checks and processes	Example threats: - CBRNE attacks - laser attacks - hijack - physical sabotage Example mitigation - screening of passengers, baggage and cargo - airspace security - safety regulations - airport perimeter security

Source: Sampigethaya and Poovendran, "Aviation Cyber–Physical Systems: Foundations for Future Aircraft and Air Transport," 1850.

5. Physical Threats. These threats are purely physical: the attack is physical and the target is physical. A physical threat may be unintentional or naturally occurring: human errors, wind gusts, imprecise weather forecasts, solar flares, RF emissions, or even bird strikes. These threats are mitigated by means of a physical security programme (e.g. the FS program).[9]

[9] Krishna Sampigethaya and Radha Poovendran, "Aviation Cyber–Physical Systems: Foundations for Future Aircraft and Air Transport," *Proceedings of the IEEE* 101, no. 8 (August 2013): 1849, doi:10.1109/jproc.2012.2235131.

6. Cyber Threats. These are cyber-attacks that have a cyber-impact. A cyber-attack is comprised of malicious actions in the cyber environment that introduce or exploit vulnerabilities of cyber assets. This type of threat can also include unintentional or accidental acts (e.g. mistakes made when coding software, incorrect software updates) but has the result of the corruption or misuse of data that can disrupt cyber components. Cyber threats are mitigated via a cyber-security programme (e.g. Canadian Forces Network Operations Centre activities as part of Operation LIMPID).[10]

7. Cyber-Physical Threats. These are complex attacks that are either cyber or physical and target the opposite environment. This is a new class of threat. A major concern regarding the cyber–physical threat vector is the negligible resources required by a malicious actor in making a cyber-attack that would have catastrophic impacts in the physical world. Corresponding to the other two threat classes, cyber-physical threats include unintentional or accidental acts. Since accuracy and timeliness are necessary traits of close cyber-physical integration, errors and delays in even well-meaning efforts can have catastrophic consequences. A comprehensive security programme will be required to thwart these cyber-physical threats.[11]

DISCUSSION

8. In order to outline the necessity for an RCAF Cyber Mission Assurance programme, the following issues will be discussed: aviation-specific cyber considerations, limitations of the Airworthiness and FS programmes regarding the cyber environment, and an introduction to

[10] Krishna Sampigethaya and Radha Poovendran, "Aviation Cyber–Physical Systems: Foundations for Future Aircraft and Air Transport," *Proceedings of the IEEE* 101, no. 8 (August 2013): 1849, doi:10.1109/jproc.2012.2235131; ‘Operation LIMPID’, National Defence and the Canadian Armed Forces, October 20, 2015, accessed February 4, 2016, http://www.forces.gc.ca/en/operations-canada-north-america/op-limpid.page.

[11] Krishna Sampigethaya and Radha Poovendran, "Aviation Cyber–Physical Systems: Foundations for Future Aircraft and Air Transport," *Proceedings of the IEEE* 101, no. 8 (August 2013): 1848-9, doi:10.1109/jproc.2012.2235131.

cyber mission assurance. Finally, a vignette will show how a Cyber Mission Assurance programme would accompany the FS and Airworthiness programmes.

Cyber Considerations for Aviation

9. Aeronautical products have become immersed in the intangible cyber environment for the control of onboard electrical, mechanical, structural, thermal, and hydraulic components; the coordination and communication among aircraft and ground stations (e.g. radio communications, radar, data link); the manipulation of intelligence, surveillance and reconnaissance (ISR) systems; and the delivery of kinetic effect. Tighter integration between aircraft, air weapons systems, and off-board systems increases the importance of cyber and cyber-physical security.[12] Cyber considerations specific to the aviation include:

a. <u>Physical threats to cyber</u>. As aeronautical products operate within the distinctive air environment, the performance of cyber systems must be ensured for operation in these conditions: bad weather, high altitude, icing, winds, solar flares, etc.[13]

b. <u>Cyber threats to the physical</u>. The cyber layer is now widely and deeply rooted into the physical components of aeronautical products to sense and control their physical behaviours. The integration is so complete that, in modern aircraft, the cyber layer is an enabler of aircraft systems instead of a mere performance enhancer. Cyber threats must be evaluated for their probable impact on physical behaviour and performance gains of aircraft, air weapons systems, and other associated systems. Security measures designed

[12] K. Sampigethaya and R. Poovendran, "Cyber-Physical System Framework for Future Aircraft and Air Traffic Control,", in 2012 IEEE Aerospace Conference (n.p.: Institute of Electrical & Electronics Engineers (IEEE), 2012), 1, 6, doi:10.1109/aero.2012.6187151.

[13] Krishna Sampigethaya and Radha Poovendran, "Aviation Cyber–Physical Systems: Foundations for Future Aircraft and Air Transport," *Proceedings of the IEEE* 101, no. 8 (August 2013): 1836, doi:10.1109/jproc.2012.2235131.

to counteract the cyber threat must not compromise aircraft performance or safety of flight.[14]

c. Lifecycle. Compared to ICT systems, aircraft have a very long lifecycle. New aircraft will undergo significant ICT updates and reconfigurations over the potential 30 year lifespan of an airframe. Presently, ICTs systems and software will become outdated in a timeframe of weeks or months. Upgrading the cyber layer of avionics after such a short period of time is challenging due to safety concerns, regulatory requirements, and the impact on aircraft availability. However, these frequent updates will only increase in importance as software becomes pervasive in avionics.[15]

d. Certification. Certification is a mainstay of aviation safety. Certification ensures that the fundamentals of airworthiness are adhered to throughout the life of an aircraft: work is done to a common safety and performance standard, by authorized individuals, of accredited organizations, and with accepted methods.

e. Common safety and performance standards. Aircraft must be certified to have the least risk from threats. While most physical standards are precise and prescriptive, the few standards available concerning the cyber or cyber-physical lack definition. Current regulations, policy and guidance from the Federal Aviation Administration (FAA),

[14] Silvia Gil Casals, Philippe Owezarski, and Gilles Descargues, "Generic and Autonomous System for Airborne Networks Cyber-Threat Detection,", in 32nd Digital Avionics Systems Conference (n.p.: IEEE, 2013), 4A4–12; Krishna Sampigethaya and Radha Poovendran, "Aviation Cyber–Physical Systems: Foundations for Future Aircraft and Air Transport," *Proceedings of the IEEE* 101, no. 8 (August 2013): 1836, doi:10.1109/jproc.2012.2235131.

[15] American Institute of Aeronautics and Astronautics, *The Connectivity Challenge: Protecting Critical Assets in a Networked World, A Framework for Aviation Cybersecurity*, (n.p.: American Institute of Aeronautics and Astronautics, 2013); Krishna Sampigethaya and Radha Poovendran, "Aviation Cyber–Physical Systems: Foundations for Future Aircraft and Air Transport," *Proceedings of the IEEE* 101, no. 8 (August 2013): 1841, doi:10.1109/jproc.2012.2235131.

Transport Canada (TC), and the RCAF are insufficient concerning the cyber security of aircraft networks and systems.[16]

f. Authorized Individuals. In order to design, build, and maintain aeronautical products with a high level of confidence in their safety of flight, these activities demand engineers and technicians; professionals that are regulated, certified, and require apprenticeship and continuing education. Unfortunately, the practice of present-day software development demands none of these hallmarks of its workers and it is not even a regulated occupation in Canada. Inside the RCAF, there exists no trade or occupation for software development or software engineering and very few civilian software developers are employed by the Department of National Defence (DND).[17]

Cyber Limitations of Existing Loss Prevention Programmes

10. Scope. The FS and Airworthiness programmes are primarily concerned with safety of flight using the aircraft itself as the frame of reference. This focus is exhibited in the two predominate definitions used by both programmes: aeronautical product[18] and air weapons

[16] K. Sampigethaya and R. Poovendran, "Cyber-Physical System Framework for Future Aircraft and Air Traffic Control,", in 2012 IEEE Aerospace Conference (n.p.: Institute of Electrical & Electronics Engineers (IEEE), 2012), 6, doi:10.1109/aero.2012.6187151; Krishna Sampigethaya and Radha Poovendran, "Aviation Cyber–Physical Systems: Foundations for Future Aircraft and Air Transport," *Proceedings of the IEEE* 101, no. 8 (August 2013): 1836, doi:10.1109/jproc.2012.2235131; Peter Skaves, "Information for Cyber Security Issues Related to Aircraft Systems Rev-A,", in 32th Digital Avionics Systems Conference (n.p.: IEEE, 2013), 4A1–1.

[17] Ian Bogost, *Programmers: Stop Calling Yourselves Engineers* (n.p.: The Atlantic, 2015), http://www.theatlantic.com/technology/archive/2015/11/programmers-should-not-call-themselves-engineers/414271/; Krishna Sampigethaya and Radha Poovendran, "Aviation Cyber–Physical Systems: Foundations for Future Aircraft and Air Transport," *Proceedings of the IEEE* 101, no. 8 (August 2013): 1846, doi:10.1109/jproc.2012.2235131; ‘Job Market Report: Computer Programmers and Interactive Media Developers’, Job Bank, January 22, 2016, accessed February 5, 2016, http://www.jobbank.gc.ca.

[18] “Any aircraft, aircraft engine, aircraft propeller or aircraft appliance or part or the component parts of any of those things, including any computer system or hardware.” Department of National Defence, *Defence Administrative Orders and Directives (DAOD) 2015-1, DND/CF Airworthiness Program*, (2015), http://www.forces.gc.ca/en/about-policies-standards-defence-admin-orders-directives-2000/2015-1.page.

system.[19] This limitation on the scope of both programmes results in other, often ground-based, aspects of flight safety and mission assurance to be overlooked. As ICT is pervasive and interconnected across all aspects of the aviation ecosystem, neither of these programmes can adequately contend with the cyber threats. The following are three simple example of areas that the FS and Airworthiness programmes pay little attention to yet have significant cyber impact on mission accomplishment:[20]

a. Ground services. Ground services are the backbone of flight operations and are highly dependent on ICT systems for maintenance, security screening, departure control, cargo handling, etc.

b. Aerodrome infrastructure. The aerodrome ICT infrastructure enables many tasks critical for the continuity of operations: security, power, fuelling systems, and aircraft servicing.

c. Supply chain. With the advent of just-in-time logistics, ICT systems are heavily leveraged in the management of the modern supply chain.

11. Embedded systems. An embedded system is a computer processor with a dedicated role within a greater electrical or mechanical system. These embedded systems form a pervasive, often networked, cyber layer within the aircraft or air weapons system. Researchers and hackers have already demonstrated that networked embedded systems are vulnerable to remote cyber-

[19] “A system containing armament computers, mechanical, electromechanical and electronic components, that is part of an aircraft’s permanent equipment or installed as a mission kit and is used to suspend, launch, release or re ammunition / explosives and / or pyrotechnics in support of the mission being flown” [Emphasis provided]

Department of National Defence, *A-GA-135-001/AA-001, Flight Safety for the Canadian Forces*, 5th ed. (Ottawa: DND Canada, 2012): 1-2.

[20] Department of National Defence, *A-GA-135-001/AA-001, Flight Safety for the Canadian Forces*, 5th ed. (Ottawa: DND Canada, 2012): 1-2; Department of National Defence, *Defence Administrative Orders and Directives (DAOD) 2015-1, DND/CF Airworthiness Program*, (2015), http://www.forces.gc.ca/en/about-policies-standards-defence-admin-orders-directives-2000/2015-1.page; American Institute of Aeronautics and Astronautics, *The Connectivity Challenge: Protecting Critical Assets in a Networked World, A Framework for Aviation Cybersecurity*, (n.p.: American Institute of Aeronautics and Astronautics, 2013).

attack and can lead to physical damage. With the increase of networked embedded systems used in avionics and other aviation-related systems, cyber security efforts to thwart malicious intrusion are required to ensure continued safety of flight.[21]

12. Expertise and experience. At this time, there is limited cyber expertise or experience in the Canadian Armed Forces (CAF) and only negligible cyber efforts have been made within the RCAF towards safety of flight or mission assurance. Based on a recent study by the Director General Cyberspace,[22] cyber education and training within the CAF is available to only a handful of trades and occupations. Within the RCAF, only the Communications and Electronics Engineering - Air (CELE(Air)) Officers and Aerospace Telecommunications and Information Systems Technicians (ATIS Tech) were identified as occupations receiving any cyber training. Extremely few CELE(Air) Officer and ATIS Techs are involved in the FS or Airworthiness programmes. While the majority of RCAF leadership have working knowledge of the FS and Airworthiness programmes, there are few leaders today with a sufficient understanding of the cyber environment to best understand its benefit and importance to operations.[23]

Cyber Mission Assurance

13. The RCAF is a cyber-enabled force requiring a Cyber Mission Assurance programme to mitigate the risk of cyber and cyber-physical threats in order to effectively conduct and sustain operations in both the physical and cyber environments. The USAF defines cyber mission assurance as,

[21] John Croft, "Darpa Program Benefit: Cyber-Secure Software," *Aviation Week & Space Technology* May 19, 2014; "High-Assurance Cyber Military Systems (HACMS)," Defense Advanced Research Projects Agency (DARPA), accessed February 2, 2016, http://www.darpa.mil/program/high-assurance-cyber-military-systems.

[22] D. C. Hawco, *CAF Cyber Education and Training*, (Director General Cyberspace: file 4500-6, 2015): A3.

[23] David S. Fadok and Richard A. Raines, "Driving towards Success in the Air Force Cyber Mission: Leveraging Our Heritage to Shape Our Future," *Air & Space Power Journal*, no. September–October (2012): 7; Michael D. Pritchett, "Cyber Mission Assurance: A Guide to Reducing the Uncertainties of Operating in a Contested Cyber Environment," (2012): 40.

> …measures required to accomplish essential objectives of missions in a contested environment. Mission assurance entails prioritizing mission essential functions, mapping mission dependence on cyberspace, identifying vulnerabilities, and mitigating risk of known vulnerabilities.[24]

14. Cyber mission assurance is a risk management pursuit with an aim to guarantee mission capabilities against the degradation or loss of cyber capabilities. Cyber mission assurance is the confidence that a cyber, or cyber-enabled, system will function properly in consideration for the consequences if that system did not function properly. It is made up of managerial, operational, and technical activities that relate to the cyber systems themselves as well as the information held and processed by ICT systems. It does not focus principally on the safety of flight but on the accomplishment of air force missions. From a user perspective, cyber mission assurance is simply the confidence that the system will work, enabling them to accomplish their assigned mission and get home.[25]

Vignette: Electronic Flight Bag

15. An electronic flight bag (EFB) is an electronic device that assists aircrew perform flight management tasks and intends to diminish, or eliminate, traditional paper-based references. The most common EFB form factor is a tablet device (e.g. an Apple iPad). EFBs can be used for many in-flight tasks such as: display of aeronautical charts, weather forecasts, electronic aeronautical information publications (eAIP), maintenance manuals and weight and balance

[24] Department of the Air Force, *AFDD 3-12, Cyberspace Operations*, Topline Coordination Draft v4 ed. (Washington: HQ USAF, 2010).

[25] Philippe Legere, "Cyber Is the Commander's Business," *The Canadian Air Force Journal* 4, no. 4 (2011): 63; Michael D. Pritchett, "Cyber Mission Assurance: A Guide to Reducing the Uncertainties of Operating in a Contested Cyber Environment," (2012): iv, 9; John Norman, "Assuring Mission Assurance in a Tactical-Cyber Environment,", in 2010 Military Communications Conference (n.p.: Institute of Electrical & Electronics Engineers (IEEE), 2010), 2316-7, doi:10.1109/milcom.2010.5680359; Kerri A. Heitner, "Cyber Threats within Civil Aviation," (Ann Arbor, MI: ProQuest, 2014). 1.

reports. The majority of EFBs have internet connectivity and others EFBs offer an interface with an aircraft's avionics system (FAA Class 2 and 3 devices).[26]

16. FS concerns for EFBs. The FS programme is concerned with the general usability of the device (e.g. size of device, layout of information, use of colour, etc.) and the conduct of a human factors assessment.

17. Airworthiness concerns for EFBs. The Airworthiness programme looks at the mounting arrangement of an EFB within the cockpit, its crashworthiness, risks associated with electromagnetic interference to existing avionics systems, risks associated with the power connection or the use of batteries, and overheating of the device. There are concerns regarding EFB data connectivity but these concerns are often limited to non-interference of data with aircraft systems.

18. Cyber Mission Assurance concerns for EFBs. A Cyber Mission Assurance programme would concern itself with the cyber and cyber-physical risks that an EFB may bring into the aircraft:[27] Are the EFB's software applications certified for use and up-to-date? Are the digital aeronautical charts used by the EFB validated? If the EFB integrates into aircraft systems in flight, what steps have been made to mitigate the remote control of the device? Is the electronic process of flight planning secured throughout its lifecycle, on the ground and while airborne?

CONCLUSION

[26] Peter Skaves, "Information for Cyber Security Issues Related to Aircraft Systems Rev-A,", in 32th Digital Avionics Systems Conference (n.p.: IEEE, 2013), 4A1–10.

[27] TA and FAA do not currently have prescriptive guidance or policy for EFB cyber security. Airline operators are only required to demonstrate that 'adequate' security measures are in place.

Peter Skaves, "Information for Cyber Security Issues Related to Aircraft Systems Rev-A,", in 32th Digital Avionics Systems Conference (n.p.: IEEE, 2013), 4A1–10.

19. The full repercussions of the RCAF’s increased interconnectivity and reliance on ICTs must be truly appreciated as cyber and cyber-physical threats further develop to ensure continued confidence in military aviation. The RCAF requires a Cyber Mission Assurance programme to address these threats as a complement to the existing FS and Airworthiness programmes. Such a program would satisfy three of the five objectives within the RCAF Cyber Strategic Plan:

> fully integrate cyber capabilities and awareness throughout the RCAF; identify, educate, train, and employ RCAF personnel to ensure mission essential cyber functions for today and tomorrow; and maximize cyber continuity, availability, and resilience.[28]

20. Today’s technological innovations bring us within reach of self-aware aircraft able of effortlessly navigating an global information network spread across ground, air, and space to consume and source information anywhere and at any time. These aircraft will incorporate off-the-shelf technology, sensors, information sharing via tactical data links, and formidable air weapons systems. Roughly 90 percent of the Joint Strike Fighter’s functionality requires software. This requires more than 10 million lines of embedded code on the aircraft and another 15 million lines of code for the ground-based Autonomic Logistics Information System. The RCAF must institutionalize a vigorous cyber mission assurance capability to protect these capabilities.[29]

[28] Author was unable to find a published or draft of the RCAF Cyber Strategic Plan despite many references to this plan across the RCAF. It is possible that the plan was never published.

Philippe Legere, "Cyber Is the Commander’s Business," *The Canadian Air Force Journal* 4, no. 4 (2011): 60; American Institute of Aeronautics and Astronautics, *The Connectivity Challenge: Protecting Critical Assets in a Networked World, A Framework for Aviation Cybersecurity*, (n.p.: American Institute of Aeronautics and Astronautics, 2013); Department of National Defence, *Defence Administrative Orders and Directives (DAOD) 2015-0, Airworthiness*, (2015), http://www.forces.gc.ca/en/about-policies-standards-defence-admin-orders-directives-2000/2015-0.page.

[29] Krishna Sampigethaya and Radha Poovendran, "Aviation Cyber–Physical Systems: Foundations for Future Aircraft and Air Transport," *Proceedings of the IEEE* 101, no. 8 (August 2013): 1836, doi:10.1109/jproc.2012.2235131; K. Sampigethaya and R. Poovendran, "Cyber-Physical System Framework for Future Aircraft and Air Traffic Control,", in 2012 IEEE Aerospace Conference (n.p.: Institute of Electrical & Electronics Engineers (IEEE), 2012), 1, doi:10.1109/aero.2012.6187151; Mark Maybury, "Toward the Assured Cyberspace Advantage: Air Force Cyber Vision 2025," *IEEE Security & Privacy* 13, no. 1 (January 2015): 49–56,

RECOMMENDATIONS

21. It is recommended that the RCAF establish a Cyber Mission Assurance loss prevention program to address cyber and cyber-physical risks that are unique to air operations:

a. Establish the Cyber Mission Assurance programme independent from the FS and Airworthiness programmes so as to not limit its effectiveness regarding the scope of its mandate;

b. Consider the Cyber Mission Assurance programme as a Shield function to complement and enhance existing electronic protection and CNO efforts;

c. Adopt a similar governance structure to the Airworthiness and FS programs;

d. Chiefly, the Commander RCAF should be designated as the Cyber Mission Assurance Authority and maintain residual responsibility for the oversight of the program across the full spectrum of operations, domestic or expeditionary;

e. The existing FS program pillars (Resilience, Risk Management and Program Management) could be reused in a proposed Cyber Mission Assurance programme to ensure it is proactive to cyber event prevention and sufficiently reactive to new cyber threats;[30]

f. As with the Airworthiness programme, develop an accreditation process for RCAF organizations assigned to technical cyber mission assurance functions;[31]

doi:10.1109/msp.2013.135. 49; Christopher Grandy, *Recommendations on a Royal Canadian Air Force C4ISR Strategy & Plan 2012 – 2027,* (Ottawa: DND Canada, 2012). 60.

[30] Department of National Defence, *A-GA-135-001/AA-001, Flight Safety for the Canadian Forces*, 5th ed. (Ottawa: DND Canada, 2012): 1-1 - 1-8.

[31] "Frequently Asked Questions: Technical Airworthiness," Technical Airworthiness, July 25, 2013, accessed February 1, 2016, http://www.forces.gc.ca/en/business-regulations-technical-airworthiness/faq.page.

g. Due to the physical and cyber impacts of cyber-attacks, the technical aspects of this programme will require tight coordination between the Air Maintenance and Communications and Electronics communities.[32]

[32] François Beaupré, *CELE(Air) Perspective on Cyber/ Space: Discussion with AERE Council*, n.p., October 23, 2015.

Bibliography

American Institute of Aeronautics and Astronautics. *The Connectivity Challenge: Protecting Critical Assets in a Networked World, A Framework for Aviation Cybersecurity*. n.p.: American Institute of Aeronautics and Astronautics, 2013.

Beaupré, François. *CELE(Air) Perspective on Cyber/ Space: Discussion with AERE Council.* n.p., (October 23, 2015).

Bogost, Ian. *Programmers: Stop Calling Yourselves Engineers*. n.p.: The Atlantic, 2015. http://www.theatlantic.com/technology/archive/2015/11/programmers-should-not-call-themselves-engineers/414271/

Canadian Armed Forces. 'Frequently Asked Questions: Technical Airworthiness.' July 25, 2013. Accessed February 1, 2016. http://www.forces.gc.ca/en/business-regulations-technical-airworthiness/faq.page.

Christiaan008. 'DEFCON 20: Hacker + Airplanes = No Good Can Come of This.' *YouTube*. November 21, 2012. Posted February 2, 2016. https://www.youtube.com/watch?v=CXv1j3GbgLk.

Croft, John. 'Darpa Program Benefit: Cyber-Secure Software.' *Aviation Week & Space Technology* May 19, 2014,.

Department of National Defence. *A-GA-007-000/AF-008, Air Force Vectors*. 1st ed. Trenton, ON: Canadian Forces Aerospace Warfare Centre, 2014.

—. *A-GA-135-001/AA-001, Flight Safety for the Canadian Forces*. 5th ed. Ottawa: DND Canada, 2012.

—. *A-GA-135-003/AG-001, Airworthiness Investigation Manual*. Ottawa: DND Canada, 2013.

—. *B-GA-400-000/FP-000, Canadian Forces Aerospace Doctrine*. 2nd ed. Trenton, ON: Canadian Forces Aerospace Warfare Centre, 2010.

—. *B-GA-405-000/FP-001, Canadian Forces Aerospace Shield Doctrine*. 1st ed. Trenton, ON: Canadian Forces Aerospace Warfare Centre, 2012.

—. *Defence Administrative Orders and Directives (DAOD) 2015-0, Airworthiness*. n.p., 2015. http://www.forces.gc.ca/en/about-policies-standards-defence-admin-orders-directives-2000/2015-0.page

—. *Defence Administrative Orders and Directives (DAOD) 2015-1, DND/CF Airworthiness Program*. n.p., 2015. http://www.forces.gc.ca/en/about-policies-standards-defence-admin-orders-directives-2000/2015-1.page

—. 'Operation LIMPID.' October 20, 2015. Accessed February 4, 2016. http://www.forces.gc.ca/en/operations-canada-north-america/op-limpid.page.

Department of the Air Force. *AFDD 3-12, Cyberspace Operations*. Topline Coordination Draft v4 ed. Washington: HQ USAF, 2010.

Fadok, David S. and Richard A. Raines. 'Driving towards Success in the Air Force Cyber Mission: Leveraging Our Heritage to Shape Our Future.' *Air & Space Power Journal*, no. September–October (2012): 4–11.

Gil Casals, Silvia, Philippe Owezarski, and Gilles Descargues. 'Generic and Autonomous System for Airborne Networks Cyber-Threat Detection.' *32nd Digital Avionics Systems Conference*. n.p.: IEEE, 2013.

Government of Canada. 'Job Market Report: Computer Programmers and Interactive Media Developers.' January 22, 2016. Accessed February 5, 2016. http://www.jobbank.gc.ca.

Grandy, Christopher. *Recommendations on a Royal Canadian Air Force C4ISR Strategy & Plan 2012 – 2027*. Ottawa: DND Canada, 2012.

Hawco, D. C. *CAF Cyber Education and Training*. Director General Cyberspace: file 4500-6, 2015.

Heitner, Kerri A. 'Cyber Threats within Civil Aviation.' Ann Arbor, MI: ProQuest, 2014.

Johnson, Daniel P. *Civil Aviation and CyberSecurity*. n.p.: Honeywell Aerospace Advanced Technology, 2013.

Kirby, Mary. 'Most Airlines Lack EFB Cyber-Security Plan: Report - Runway Girl.' *Safety*. January 28, 2014. https://www.runwaygirlnetwork.com/2014/01/28/most-airlines-lack-efb-cyber-security-plan-report/.

Launchbury, John. 'High-Assurance Cyber Military Systems (HACMS).' Accessed February 2, 2016. http://www.darpa.mil/program/high-assurance-cyber-military-systems.

Legere, Philippe. 'Cyber Is the Commander's Business.' *The Canadian Air Force Journal* 4, no. 4 (2011): 58–63.

Maybury, Mark. 'Toward the Assured Cyberspace Advantage: Air Force Cyber Vision 2025.' *IEEE Security & Privacy* 13, no. 1 (January 2015): 49–56. doi:10.1109/msp.2013.135.

Norman, John. 'Assuring Mission Assurance in a Tactical-Cyber Environment.' *2010 Military Communications Conference*. n.p.: Institute of Electrical & Electronics Engineers (IEEE), 2010. doi:10.1109/milcom.2010.5680359.

Pritchett, Michael D. 'Cyber Mission Assurance: A Guide to Reducing the Uncertainties of Operating in a Contested Cyber Environment.' n.p., 2012.

Sampigethaya, Krishna and Radha Poovendran. ‘Cyber-Physical System Framework for Future Aircraft and Air Traffic Control.’ *2012 IEEE Aerospace Conference*. n.p.: Institute of Electrical & Electronics Engineers (IEEE), 2012. doi:10.1109/aero.2012.6187151.

—. ‘Aviation Cyber–Physical Systems: Foundations for Future Aircraft and Air Transport.’ *Proceedings of the IEEE* 101, no. 8 (August 2013): 1834–55. doi:10.1109/jproc.2012.2235131.

Shaw, Kirk. ‘Diversity of Canadian Military Airworthiness Authority Experiences and Challenges.’ *Military Airworthiness Authorities (MAWA) Forum*. n.p.: Canadian Armed Forces, 2012.

Skaves, Peter. ‘Information for Cyber Security Issues Related to Aircraft Systems Rev-A.’ *32th Digital Avionics Systems Conference*. n.p.: IEEE, 2013.

Strange, Adario. ‘This Gun Can Stop Small Rogue Drones without Destroying Them.’ *Mashable*. January 30, 2016. http://mashable.com/2016/01/30/drone-gun.

Transport Canada. *Advisory Circular: Electronic Flight Bags*. n.p., 2012.