

points of interest

# CYBER IS THE COMMANDER'S BUSINESS

By Major Philippe Legere, CD

CF Photo



CF Photo



CF Photo



CF Photo



CF Photo

**A**n Inuit hunting party is stranded on the ice in the Eastern Arctic, wind chill is estimated at -46 degrees Celsius and one member requires immediate medical attention. Fortunately, a CP140 is on patrol nearby in contact with Canadian North American Aerospace Defence Command (NORAD) Region / Canadian Air Defence Sector (CANR/CADS), operating a pre-planned secure high frequency (HF) radio data link. It also has onboard access to Iridium Satellite Phone communications. The call for help arrives in the Joint Task Force (North) joint operations centre. They immediately phone the CANR/CADS mission crew commander (MCC) with the coordinates and request that all the nearest Canadian Forces (CF) assets' "tracks" (track data; location, heading, altitude, speed, etc.) be "pushed" (sent via Internet Protocol [IP] connection) to the CF common operating picture (COP). The CADS MCC receives coordinating instructions from the CANR Combined Air Operations Centre and then choreographs a response. The MCC directs the CADS Regional Interface Control Cell (RICC) to send coordinates to the patrolling CP140 and the CF COP as a data track fixed on the ice floe where the stranded Inuit await, representing a search and rescue event. The RICC also pushes all CF asset tracks within 150 nautical miles to the CF COP via secure IP connection, and to the CP140 via the HF link, as symbology representing track data.

**The CP140 then supports a Transport Canada Ice Patrol Flight which is re-tasked to overfly the area to confirm the Inuit status and position, and to vector in a helicopter to eventually pick them up. Meanwhile, the whole event is viewed as it occurs, in real time, by national authorities and various agencies possessing the CF COP and to those with the Remote Tactical Air Picture connected via a secure IP connection with the CADS Battle Control System. Once again the CANR/CADS stands on guard for all Canadians.**

The above scenario demonstrates how the Royal Canadian Air Force (RCAF) today operates within an information technology-rich environment, touching practically

everything and every member every day. The security and operational necessity of the networks employed in the RCAF require a dependence on freedom of access to and freedom of action within the cyber environment.

The RCAF dependence on the cyber environment to accomplish its mission is an extension of its traditional use and application of leading edge technology. Command and control (C2) systems, weapon systems, and sensors are examples of mission-oriented components that exist within the cyber environment that is integrally involved in the delivery of kinetic and non-kinetic mission effects supporting the commander's intent. Reliance on the cyber environment demands greater vigilance of its current cyber capabilities and the vision



CF Photo

to operationally exploit future cyber potential. The realization of air force mission effects is thereby contingent on operator ownership of its cyber environment. *Cyber is the commander's business.*

The challenge for the RCAF is maintaining the advantage of exploiting rapidly evolving cyber capabilities while countering the numerous inherent vulnerabilities at an equal pace. The cyber threat is asymmetrical, involving state and non-state actors, with a minimal cost of entry, requiring little technical expertise and experience to create effects due to the ease of access and proliferation of online malicious products.

To address the RCAF cyber challenge, the Canadian Forces Aerospace Warfare Centre, in collaboration with the CF Cyber Task Force as well as various RCAF and other Department of National Defence (DND)/CF agencies, is developing an RCAF Cyber Strategic Plan (CSP). The CSP, consistent with the goals set out in the Canada First Defence Strategy and the Government of Canada Cyber Security Strategy, will provide commander's guidance and intent, outlining objectives to help shape RCAF actions over the near future.

### RCAF Cyber Strategic Plan

The CSP will outline RCAF cyber efforts to complement those of other cyber partners, providing maximum benefits to ongoing joint cyber initiatives, and contribute significantly to the national cyber effort. As a result, the intent of the RCAF CSP will be to:

1. position the RCAF to operate within the cyber environment;
2. position the RCAF with enhanced and unique defensive cyber capabilities complementing those under joint DND/CF command and authority ;
3. assure mission success by protecting and defending RCAF cyber systems;
4. establish RCAF cyber requirements and re-engineer acquisition processes; and
5. institutionalize an RCAF cyber culture and mindset.

Also identified in the CSP will also identify objectives for the RCAF to achieve as it moves toward positioning itself as a modern cyber-enabled force. These objectives, as tabled below, will aid the RCAF to prioritize resources and measure the effectiveness of its cyber efforts within the context of the Air Force mission.

<b>Objective 1</b>	<b>Fully integrate cyber capabilities and awareness throughout the RCAF</b>
<b>Objective 2</b>	<b>Identify, educate, train, and employ RCAF personnel to ensure mission essential cyber functions for today and tomorrow</b>
<b>Objective 3</b>	<b>Maximize cyber continuity, availability, and resilience</b>
<b>Objective 4</b>	<b>Establish and/or maintain cyber relationships</b>
<b>Objective 5</b>	<b>Initiate the delivery of cyber capabilities at the "speed of need"</b>

### The Current RCAF Posture

Today's RCAF is a cyber-enabled force, dependent upon mission-critical cyber capabilities and systems on a daily basis. Every air force platform contains a multitude of

sensors, systems, and networks whose linkages into the cyber environment, although transparent to the operator, are very complex yet essential for performing missions within air-to-air, air-to-land and/or air-to-sea environments.

Air force adoption of and operational reliance upon cyber capabilities has evolved over time as they have been integrated to facilitate C2, situational awareness (SA) and intelligence, surveillance and reconnaissance (ISR) collection, and the ability to realize mission effects. Advances in sensors, video compression, and mobile networking also enable the sharing of real-time operational and tactical information that can significantly enhance operational SA at all levels of command. The operational transition to Link 16 and introduction of full motion video, first operationally exploited during Operation PODIUM supporting security for the 2010 Winter Olympics in Vancouver, are allowing for real-time C2 as well as SA of the battlespace to an extent not possible five years ago.

### Future Vision

The CSP should permit the RCAF to realize its determination to exploit the benefits of a cyber-enabled force to ensure an advantage over our enemies, now and into the future, without sacrificing the success of daily national and coalition operations. The RCAF will integrate its cyber capabilities with the whole of DND/CF, other government agencies, NORAD, our Five-Eyes allies, coalition partners, research

and development communities, as well as academia to counter the cyber threat of today and into the future. An RCAF cyber authority, providing operational guidance and direction as well as oversight of cyber service provision requirements, will ensure the effectiveness of the RCAF's current and evolving cyber capabilities. Lastly, the RCAF will foster a culture of cyber defence awareness, instilling a sense of duty by all members in regards to protecting our networks and remaining vigilant to the constant and rapidly evolving cyber threat whether at home or deployed.

### The RCAF Cyber Acculturation

The RCAF cultural mindset must be cognizant of the day-to-day execution of cyber operations. Such a change in mindset will permit effective exploitation of current and future cyber capabilities while countering the rapidly evolving cyber threat. Acceptance of the cyber environment as a recognized reality and the normalization of computer network operations (CNO) concepts as tools in the commander's toolkit are essential for air force mission success. The application of cyber capabilities and effects should also consider within the operational planning process of mission planning and targeting. In addition, the RCAF should exploit to the greatest extent possible the concept of capability integration, recognizing how its own cyber capabilities may leverage or be leveraged by the capabilities of the DND/CF, other government agencies, and allied mission partners. The integration and acculturation of cyber should be apparent in all aspects supporting the RCAF mission,

from the foundations of doctrine development, professional military education and advanced training, C2, readiness training and exercises, war games, and recruitment to the day-to-day operations. Ultimately, it demands leadership at all levels that encourages creative yet critical thinking, and considers innovative activities and solutions.

### Guidance for RCAF Computer Network Operations

The RCAF of today and tomorrow must exploit to the extent possible the full spectrum of CNO in accomplishing its mission. Ensuring the RCAF has the capability to plan for and integrate CNO will be essential for overall mission success. However, the primary CNO focus for the RCAF should be to defend against the cyber threat, in concert with DND/CF cyber initiatives, by organizing, educating, training and equipping a computer network defence (CND) capable force structure to support the RCAF mission. The RCAF understands that the cyber environment is a contested operational area that pervades and enables capabilities and effects in all other environments. The cyber threat is persistent, real time, and inherently global. Therefore, the CSP should position the RCAF to secure and defend its cyber systems, integrating them with other environments to enable joint warfighting effects.

The ability to accomplish the RCAF mission while under attack is essential, requiring an agile and timely response across the RCAF and DND/CF. Consequently, the

RCAF must broaden its focus to defend its unique cyber systems vice simply protecting them. By establishing a determined CND posture the RCAF will be positioned to complement the required full spectrum of CNO, provided by a central DND/CF cyber authority, to counter the immediate and evolving cyber threat. To this end, it is essential that all RCAF members must embrace cyber defence in their daily functions in order to combat the cyber threat.

### RCAF Cyber Strategic Plan Concept of Operation

The RCAF is already entirely interconnected with and dependent upon the cyber environment. Therefore, a CSP will help guide the evolution of the existing mix of RCAF unique and externally provided cyber capabilities into an integrated, normalized, and operationally focused programme of cyber capabilities that will be essential for the conduct of operations. With the goals of implementing a governance structure for RCAF cyber, normalizing cyber concepts within the RCAF, implementing mission assurance and air worthiness to cyber capabilities upon which the RCAF depends, and taking responsibility to defend RCAF unique cyber capabilities, the RCAF CSP should outline a program to be implemented to evolve RCAF cyber over the coming years.

This program should focus on cyber concept development, design development, and implementation actions that will position the RCAF to exploit cyber

operational effects in support of the commander's intent. The RCAF should first evaluate current cyber defence capabilities and confirm any shortfalls while committing to a CND strategy to provide mission assurance and ensuring the airworthiness of cyber systems. Next, the RCAF should put in place measures to develop and sustain an agile and timely CND capability. Finally, the CSP should outline measures to entrench cyber concepts across the RCAF and operationalize its cyber capabilities and support structures.

### Conclusion

The RCAF is a cyber-enabled force requiring a strategic plan to address its cyber operations in order to effectively sustain mission operations in a cyber-enabled operating environment, positioning itself to counter the cyber threat today and into the future. To this end, the future RCAF CSP will be the mechanism by which the RCAF should develop and sustain an enhanced and unique cyber capability, thereby ensuring mission success into the future. The RCAF should, in concert with its varied cyber partners, continue to evolve and exploit its cyber capabilities, always cognizant of the associated cyber threat, in order to maintain advantage over its enemies. ■

Major Philippe Legere, a communications and electronics engineering – air (CELE[Air]) officer with 29 years' military experience, is a staff member within the Doctrine Development Branch at the Canadian Aerospace Warfare Centre. A graduate of the Royal Canadian Military College of Canada, he has served with 42 Radar Squadron, Cold Lake; North Atlantic Treaty Organization (NATO) Allied Air Force North Ramstein, Germany; Stabilization Force Headquarters (SFORHQ) Sarajevo, Bosnia; Canadian Forces School of Communications and Electronics as second in command (2IC) G Squadron (Technical Training); and Canadian Forces School of Communications (CFSCE) Adjutant; as well as several staff function tours at National Defence Headquarters Ottawa.

#### Abbreviations

C2	command and control
CADS	Canadian Air Defence Sector
CANR	Canadian NORAD region
CF	Canadian Forces
CND	computer network defence
CNO	computer network operations
COP	common operating procedure
CSP	Cyber Strategic Plan
DND	Department of National Defence
HF	high frequency
IP	Internet Protocol
MCC	mission crew commander
NORAD	North American Aerospace Defence Command
RCAF	Royal Canadian Air Force
RICC	Regional Interface Control Cell
SA	situational awareness