The C & E Branch is dead. Long live the Cyber Branch!

This is a provocative title meant to illicit an emotional reaction and hopefully lure you into reading at least this first paragraph. You will have started reading, if for anything else, to reassure yourself that your long held core beliefs in the merits and legitimacy of the C & E branch are not under any real, serious threat. In the online community, this is generally referred to as click bait.

And since you have already started reading, you may as well carry on for a few more paragraphs. Who knows? Perhaps it is time to reconcile the terms C&E with Cyber and reflect to what degree these two terms share common grounds…

In reality, both names for the branch have merit. But for our community, I posit that it is a meaningless distinction. Neither is better at describing who and what we are. Nor are either a subset of, or subservient to, the other. Whatever we call ourselves, our role and our duties are rapidly and fundamentally being altered by external forces over which we have no control and to which we must adapt through changes that are as disruptive and radical as those we are seeing in the "IT industry" as a whole. Finally, the tradition of slow, measured, and cautious steps to implement long lasting changes over a half decade or longer will not cut it. This would be an old engineering approach. The IT industry has long since moved on to more agile methods. Nor is it a warfighter's approach which is usually bolder, more decisive and expeditious. In other words, a warfighter's approach to challenges is often more akin to the more recent development models such as SCRUM or for a more appropriate comparison, the RCAF's Mission Risk Launch Authority (MALA) that gives the power to accept risks at the lowest possible level rather than the good old waterfall development model which seems to be the modus operandi of just about every C&E Branch initiative.

Cyberspace is defined[1] as "*The element of the operational environment that consists of interdependent networks of information technology structures—including the Internet, telecommunications networks, computer systems, embedded processors and controllers—as well as the software and data that reside within them*". And given this definition, it is easy to see that C&E Branch personnel operate within it, or at the very least contribute to the subsistence of the cyber domain. But, are we all warfighters in this domain? Should we all be? To answer these question, perhaps we should start by looking at the basic essence of other warfighting domains.

As a start point, let's consider a very specific example of a more generic task carried out in all traditional domains: the lift functions provided by the Air Force. Airlift is defined[2] as: "*The transport and delivery by air of personnel and materiel in support of strategic, operational, or tactical objectives"*. It is important to note that no distinction is made as to whom will benefit from this airlift task. Naval personnel might be transported to a ship to join its crew, grenades and food may be parachuted over an army FOB, etc. Much is also implied in this definition. For one thing, the RCAF is broadly responsible for airlift operations in the CAF. When entrusted with personnel and material to airlift, the RCAF makes a commitment to safely deliver them to their destination via the air domain in a timely manner. This further implies that the RCAF will ensure the aircraft utilized is in good working conditions and will not suffer a mechanical malfunction causing delays or worst, the loss of the personnel and material. Finally, this implies that the

[1] https://www.btb.termiumplus.gc.ca/tpv2alpha/alpha-eng.html?lang=eng&i=1&srchtxt=cyberspace&codom2nd_wet=1

[2] https://www.btb.termiumplus.gc.ca/tpv2alpha/alpha-eng.html?lang=eng&i=1&srchtxt=airlift&codom2nd_wet=1

RCAF element detached to the theatre commander will be expected to gain and maintain the necessary freedom of maneuver within the air domain to safely carry out the airlift. Further implying that the aircraft in question will be equipped with defensive measures and possibly requiring escort or other offensive actions to ensure that the airspace required for the airlift is free from adversary interference.

If there are such things as airlift and sealift functions for the air and maritime domains, is there such a thing as cyberlift? Is there something that we are entrusted with, to care for, protect, and deliver safely in support of strategic, operational, or tactical objectives? There is! Signed order that are scanned and emailed, conversations transported over VOIP, ship positional data, SITREPS, Full motion video for ISR feeds, etc. All of which can ultimately be reduced to a single definition[3]: "*Data: reinterpretable representation of information in a formalized manner suitable for communication, interpretation, or processing*". If we accept that our community is responsible for transport and delivery through cyberspace of data in support of strategic, operational, or tactical objectives, then we are in effect providing cyberlift. A function analogous of airlift in every aspects. For example:

- The RCAF has to build and maintain a capable workforce and the infrastructure to enable airlift. So does the C&E Branch to enable cyberlift.
- The RCAF has to develop processes and mitigations to reduce the environmental risks[4] associated with operating in the air domain. So does the C&E Branch to enable cyberlift.
- The RCAF must ensure that defensive[5] and offensive[6] capabilities are in place in order to maintain freedom of maneuver in the air domain to ensure successful airlift operations. So does the C&E Branch to enable cyberlift.

The last bullet is where we have been challenged the most in the last decade and a half. We have been pretty good at keeping up with the evolution of technologies as it pertains to our ability to meet the cyberlift requirements levied on us by the other warfighting domains. Whenever we failed, it was usually due to an environmental threat (See footnote 4 for examples) which was not adequately mitigated. We learned, improved and over time became better at mitigating environmental threats which translated into fewer outages from the point of view of the warfighters in the other domains relying on our cyberlift capabilities to carry out their own operations.

But then came on the scene a new kind of threat. One that our brethren in arms have always had to face but that was totally new to us in the cyber domain. A threat that was more difficult to deal with because it was built with the deliberate intent to challenge our freedom of maneuver. This threat will therefore be referred to in this essay as the "deliberate threat".

[3] https://www.btb.termiumplus.gc.ca/tpv2alpha/alpha-eng.html?lang=eng&srchtxt=data&i=&index=alt&sg_kp_wet=2121272&fchrcrdnm=4

[4] Examples of environmental threats in the air domain are weather, bird strikes, operator/mechanic errors, mechanical failures, amateur UAV operators etc.
Environmental threat equivalency in cyber domain includes BGP routing issues, accidental cable cuts, user/sysadmin errors, hardware failures, indiscriminate release of computer viruses by criminal organizations

[5] Passive defence such as RWR and flares. Or more active measures such as Griffons escorting Chinooks in Mali

[6] Through Suppression of Enemy Air Defence (SEAD) or degradation of Integration of Air Defence Systems (IADS) using Air domain capabilities but also possible through effects delivered from another domain

The deliberate threat in cyber is not unlike how an adversary builds fighter aircraft and missiles backed up by processes, tactics, infrastructure, and a C2 construct specifically designed to take away their enemy's freedom of manoeuver in the air domain. But in cyberspace, this threat is even more insidious due to the fact that the greatest wins for our enemies is not yet to deny us our freedom of manoeuver in cyberspace. Instead, their greatest wins thus far have been in stealing copies of the payloads in our cyberlifts, all the while remaining undetected. A situation that is far more prevalent to the cyber than any other domains. This leads to a situation where it is not readily apparent to traditional domains warfighers that we are being contested, on a daily basis and below the level that they would consider the threshold of an armed attack. Therefore, it is far more difficult to assess the outcome of data loss as it pertains to tangible outcomes because a clear link between data loss (that is often never detected) and an adversary action in another domain is virtually impossible to make without expensive and lengthy investigation and even then there are no guarantees of a solid attribution. As a consequence, we are far less convincing in our arguments that we are under-equipped and under manned to face this well organized, well financed deliberate threat.

This is not to say that we did not try to bolster our cyber operations capabilities to safeguard our cyberlift missions. We did, and we are. That is the driving factor behind Cyber Force Development. CFNOC is our equivalent of a maritime patrol aircraft. It can detect and engage a threats at the tactical level just like a CP-140 can use sonobuoy to find a submarine and drop a torpedo to engage it. And a whole semi-formal parallel organization (the Joint Forces Cyber Component Command (JFCCC)) was grafted to DGIMO to address the deliberate threat at the operational level. For a while it has been the right approach because in our Branch, system availability is king and we have developed the natural reflex of prioritizing return to operation above everything else. Therefore, we have often been guilty in the past of neglecting any task that distracted from this primary objective. Had we not identified and set aside personnel specifically intent on conducting cyber defence activities, they too would have been consumed with restoring any and all outages regardless of the cause.

Still, the deliberate threat continues to change. State actors are increasingly using their cyber operations capabilities to threaten data integrity and availability. While the CAF might have been spared thus far, we cannot rely on our good luck to hold forever. Eventually, a state actor will seek to degrade or deny us our freedom of maneuver in cyberspace, directly and significantly impacting our cyberlift abilities and by extension CAF operations across one or more domains. When this happens, all C&E personnel involved in the specifically affected cyberlift mission will be required to pitch in. Relying on the handful of "cyber defenders" will simply not cut it. A ship at sea that has been hit by a missile does not solely rely on its engineers to keep it afloat and complete its sealift mission. The entire crew is galvanized into action lest we risk losing the ship. In fact, every single member of the crew was playing some unique and essential role even before the missile was fired by the enemy and detected by the ship's radar operators who subsequently, but unsuccessfully took defensive actions. For example, every crew member knew of keeping hatches closed between watertight bulkheads, recognizing the real possibility and risks associated with not adhering to this practice. Each crewmen also knew exactly what they had to do once the missile hit based on their current location on the ship and their particular skills and pre-assigned damage control roles. Are all of our C&E personnel equally well prepared for an analogous eventuality in cyberspace? I think not.

And that is at the heart of the C&E Branch's future. We no longer can keep two separate yet closely linked set of activities. On one side, we are a group only trained for and focused on enabling cyberlift while protecting against environmental threats, while on the other, another smaller group is concentrating on defeating the deliberate threat. Instead, all hands must be trained to operate in a contested environment, everyone conscious that an adversary could strike at any moment and fully cognisant of what its role is in such an event and how to go about its daily duties to minimize the impact once it inevitably does.

Under such a construct, our ability to seamlessly and almost effortlessly counter environmental threats would be our minimum baseline while our measure of success would be our ability to carry out cyberlift in spite of operating in a contested environment.

That is a transformation that is now overdue. One that will start first and foremost in our collective consciousness and that will benefit from bolder and more expeditious models like "MALA" and "SCRUM" if we do not want to be left even further behind. Only then will we have flourished from an organization capable of conducting cyberlift in peacetime to one that is manned by warfighters capable of carrying out its cyberlift mission in even the most contested of environments. In the end, C&E and Cyber are one and the same regardless of the name the branch chooses to use. What is important is that we transform ourselves to be able to cope with the ever increasing and sophisticated deliberate threat. Luckily, both the Air Force and Navy offer time and battle tested models that should inspire us as we seek to structure and separate duties across occupations, each with pertinent career and training paths…

By Eric Jodoin

About the Author

LCol Jodoin joined the CAF in 1991 and spent his first decade honing his warfighting skills at the tactical and operational levels of naval and joint warfare as a MARS officer before transferring to the RCAF as a CELE (Air) Officer to pursue his other passion: IT Security. Sensing a ground swell in the IT industry and seeing many parallels between naval warfare and what was to become known as cyber warfare, he steered his educational path toward earning multiple IT/Cyber security certifications including CISSP (2009) and GIAC GSE (2015) before completing his Master of Science in Information Security Engineering (MSISE) from STI. He strove to occupy key positions in the burgeoning cyber operations field. He was employed as a Cyber Domain Chief at the NORAD-USNORTHCOM N2C2, OC A Squadron at CFNOC, 2 I/C DIMEI SEV, and planner in the Combined Cyber Unit (CCU) embedded within the Communication Security Establishment (CSE). He was deployed under Op IMPACT to the US JFHQ-C ARCYBER in 2015 as the CAF's first Offensive Cyber Operations Planner employed in a CAF named operation. He is currently the team lead of the Cyber Component Command Element (CCCE) embedded within CJOC.