Journal of Military and Strategic Studies

VOLUME 19, ISSUE 4

Notes from the Field

Close Encounters of the Military Kind: A Civilian's Perspective

Dr. Thomas P. Keenan, FCIPS, I.S.P, ITCP[1]

In 2004, the author was privileged to join a Department of National Defence/Canadian Forces familiarization visit for business and academic stakeholders to Kabul, Afghanistan. This sparked a long-term interest in military operations, culture, and especially technology. This brief report highlights some of the lessons learned from that visit as well as more recent experiences at sea with the Royal Canadian Navy's *Canadian leaders at Sea* program and at the first-ever Aviation Village at the 2019 DEFCON hacker conference.

****

I don't come from a military background, though I have a keen appreciation of the role and importance of our armed forces as well as the special demands that are placed on military members. I've had three fascinating encounters that taught me a lot

[1] Professor, School of Architecture Planning and Landscape
Adjunct Professor, Department of Computer Science
Senior Fellow, Centre for Military and Strategic Studies, University of Calgary
Research Fellow, Canadian Global Affairs Institute

ISSN : 1488-559X

from the viewpoint of an informed civilian, with a particular interest in all things technological.

1. DND/CF Familiarization Visit to Kabul Afghanistan, 27 November to 09 December 2004

Public affairs outreach programs are an important strategic tool that has been used by Canada's Department of National Defence (DND) for many years. As noted by Ellen Huijgh in her 2019 book, *Public Diplomacy at Home: Domestic Dimensions:* "The DND's outreach to Canadians (includes)…familiarization visits to the DND and Canadian Forces' installations and operations at home and abroad."[2]

This explains the letter I received in November 2004 from DND's then-Director of External Communications and Public Relations. It invited me to join a group of Canadians from the business and academic sectors on a trip to Kabul, Afghanistan "to give stakeholders firsthand knowledge about Canada's diplomatic, defence and development contributions to the stabilization and reconstruction of Afghanistan."[3]

Despite this being fifteen years ago, I have vivid and indelible memories of that trip, starting with signing the waiver form, which I believed mentioned "death" about ten times. It also noted that Canadian Forces operational needs took absolute priority over individual wishes. The paperwork stated that, while there was every intention of bringing us back to Canada, we might wind up somewhere else if that's where the plane had to go. The needs of the mission and the group took precedence.

In a way, this military mindset is the polar opposite of life as a University professor where we have a great deal of freedom, from choosing our research topics to the details of how we teach our classes. We even get to plan our working schedule, subject to showing up for those classes and honoring our other commitments.

[2] E. Huijgh, "Public Diplomacy at Home**:** Domestic Dimensions," *Diplomatic Studies,* no. 15, Brill, 2019, ISBN 9789004394254.

[3] Personal communication from Rachel J. Boyer, DND Director of External Communications and Public Relations, 16 November 2004.

I quickly came to appreciate the need for rigor and discipline in a military setting during the rough and pretty turbulent flight to Kabul on a Hercules aircraft. We were in full body armor as the pilot performed some pretty aggressive evasive maneuvers over Afghanistan. "If you can't reach the barf bag, throw up in your helmet," we were told. "Your own helmet, not your buddy's."

Soon after arrival at Camp Julien, we were taken into a tent for a security briefing. While it was hard to stay awake after all the travelling, we all knew this was important stuff. And, indeed, a few nights later we heard a loud bang. Some of the members of our group, which included some prominent Canadians that I won't name for privacy reasons, were told that a propane BBQ tank had exploded. Those of us who dug further learned that someone had managed to lob an explosive device over the Camp Julien fence, narrowly missing the place where the ammunition was stored. I wouldn't be writing this if his or her aim was better.

When we went "outside the wire," we were transported in LAV IIIs or similar vehicles and guarded by several soldiers. They certainly treated us as precious cargo. I did learn that there was something even more precious, though. Sometimes, two soldiers would carry a case which I was told contained security-related data on DVDs. They went into the LAV III before us, grabbing the safest spots. In fact, when we were flying home to CFB Trenton, our aircraft made a special stop at Ottawa solely for those soldiers and their cargo to disembark.

The base had a small Internet café which we were allowed to use alongside the military members. One thing that struck me was the wide range of atmospheres there. When it was early evening in Canada, we would find soldiers earnestly chatting with their families back home. A few hours later, when the folks in Canada were sleeping, the attention turned to more earthy websites. While DND tried to ban porn sites and even blacklisted playboy.com, soldiers are innovative. They found things like the "hot babe of the day" sites sponsored by US radio stations to amuse themselves.

I tried an experiment, asking a friend to geolocate me from that café, based on my IP address. I was pleased to see it come up as an address in Ottawa. Even back in 2004 we knew that this type of information could reveal your location if not handled properly.

One thing that did cause me some concerns was when I laid my hand on the major cable that supported digital communications for Camp Julien. "Is there backup?" I asked. "Yes and no," came the reply. "We do have backup links, but they go through Pakistan and that's a worry." Of course, this was 2004, and I'm sure military communications have improved vastly since then.

2. Royal Canadian Navy *Canadian Leaders at Sea*, 12 March to 14 March 2019

With the Afghanistan experience still rattling around in the back of my head, I was delighted to be invited by the Royal Canadian Navy to take part in a three-day land and sea program in Esquimalt, BC and aboard the Halifax class frigate HMCS *Calgary*.

We pretty much had the run of the ship and were even permitted to fire its weapons and drive it under close supervision. Interestingly, the one visit that was denied was my request to see the communications room. Our liaison folks dutifully took it up the chain of command and the answer came back "sorry." I was actually pleased with that outcome since that's not the kind of thing the Navy should be showing to just anyone. In a similar fashion, there were some restrictions on taking photos in certain sensitive areas, but nothing like Afghanistan where our cameras and mobile phones were locked up to prevent any photo-taking.

Again, I'll avoid naming the other seven participants in this group except for prominent Calgary businessman George Brookman, who is also Chair of the Dean's Circle of our University of Calgary School of Architecture, Planning and Landscape. He's happy for everyone to know that he slept opposite me for a few nights on this trip.

Our temporary home was a "rack," a bunk inside a 12-person mess deck, aboard the HMCS *Calgary*. The ship returned to CFB Esquimalt in December 2018 from Operation PROJECTION, a five-month deployment to the Asia-Pacific region. We also boarded the HMCS *Edmonton,* a Maritime Coastal Defence Vessel, and HMCS *Chicoutimi*, one of Canada's four long-range hunter-killer submarines. We visited land-based facilities at CFB Esquimalt including the Joint Rescue Coordination Centre Victoria and the Fleet Diving Unit and met the people and equipment who carry out those very scary mine clearing operations.

The aim of the *Canadian Leaders at Sea* program is to proactively engage with Canadian stakeholders to tell the Navy story and give them a first-hand glimpse inside the mysterious world of the Royal Canadian Navy and the people who choose to make their career in it.

What we learned ranged from the frivolous ("take your hat off before entering the mess or you have to buy a round [in theory]") to the deadly serious ("our job as submariners is to spend 29 days under the water without anyone knowing where we are"). We were extremely impressed by the intellectual depth of senior officers who were not only well-versed on geopolitics but also had thoughtful and sometimes surprising opinions about the future of Canada's military.

If an army travels on its stomach, so does the Navy, with a tradition of four meals a day. We ate everywhere from the Junior Ranks mess, the Chief and Petty Officer's mess and the Captain's suite, and yes, we put on some kilos despite the rigorous schedule. One funny tidbit is that the ship was commissioned in 1995, when most people didn't think about going to the gym. Now, by popular demand, there are treadmills and exercise bikes crammed into the weirdest places, since space on board is at a premium. On the HMCS *Edmonton*, there's even exercise gear on the bridge!

Our activities included participating in a mock boarding of a hostile ship and shooting at "pirates." One highlight was the "Damage Control Olympics" in which the crew simulated serious flooding and electrical damage to the ship and practiced their responses. We learned that this wasn't just for our benefit – exercises like this are a regular part of shipboard routine so critical actions become second nature and automatic.

We were given some physically demanding tasks like struggling to put on bulky firefighting gear and cold-water submersion suits, and a simulated firing range exercise where crew members dressed up as Ninjas came out of corners to shoot at us unless we killed them first -- using semi-automatic rifles, with paintball bullets of course.

You haven't lived until somebody rousts you from the bed in the middle of the night screaming that your cabin is flooding, and you have just seconds to rig the emergency ladder and climb through the escape hatch. Yes, we were warned that we

would be getting a "bedtime story" that night, but it still felt very real and tremendously urgent.

All of us came away with a much greater appreciation of the demands and rewards of life in the Royal Canadian Navy and the vital importance of their mission. I want to thank the Commander of the Royal Canadian Navy, Vice-Admiral Ron Lloyd for this opportunity, and our very gracious hosts, Commander Canadian Fleet Pacific, Commodore Angus Topshee, Commander Officer of HMCS Calgary, Commander Blair Saltel, and Senior Staff Officer Strategic Outreach for the Royal Canadian Navy, Lieutenant-Commander Melissa Fudge for a truly enlightening look into a built environment that few Canadians get to witness.

3. Aviation Village at DEFCON, 9 August – 11 August 2019

DEFCON is the world's largest and most famous hacker conference, taking place each year in Las Vegas in early August. It brings together some of the brightest people intent on breaking technology, as well as those from industry, government and the military who work to protect it.

The conference has large sessions, many of which are posted for all to see on a YouTube channel.[4] In recent years, DEFCON has added special interest villages organized around topics ranging from hacking wireless systems to medical device security and social engineering.

For the first time this year, there was an Aviation Village with the theme of "Securing the Skies."[5] In addition to promoting education and awareness about aviation cybersafety, this large array of people and equipment was brought there to "foster collaboration between the aviation industry and the infosec/hacker community."[6]

The Village was wildly popular and most of the time you couldn't get near things like the F-35 military flight simulator. I was fortunate enough to be given a tour

[4] https://www.youtube.com/user/DEFCONConference
[5] https://aviationvillage.org/
[6] Ibid.

by officials from a little known (at least to me) US Department of Defense agency team called the Digital Defense Service.[7]

This group brings technologists in on limited tours of duty to "to improve government services, strengthen national defense, and care for military members and their families."[8] They're the folks behind the Hack the Pentagon competition which, since 2016. has engaged ethical hackers from around the world to "help the DOD to identify and remedy thousands of security vulnerabilities."

The Digital Defense Service calls itself "a SWAT Team of Nerds" and my experience with them bears this out. The members I met had a solid level of technology knowledge and the right attitude – they know they're not perfect and they're interested in getting help from anyone who can provide it.

In the spirit of Hack the Pentagon, they've launched Hack the Air Force 3.0. [9] Available in 191 countries, it's the largest ever US government bug bounty program. Bug bounties are used by companies like Microsoft and Apple who pay cash to "white hack" hackers who alert them to critical vulnerabilities. Facebook paid out $50,000 for one vulnerability, though the US government's budget is more like $5,000 to $10,000.

While glitches in military technology are a huge worry, aviation on the civilian side has its own problems. Technical issues have forced the grounding of Boeing's 737 Max aircraft around the world, after the loss of 346 lives in two crashes.

There may be more bad news for Boeing. At the BlackHat conference, which immediately precedes DEFCON, Madrid hacker Ruben Santamarta announced that he had downloaded unprotected code from that company's website and concluded that there could be serious security vulnerabilities in the software of the company's 787 Dreamliners. He claims it could lead to unauthorized access to the critical Crew Information Service/Maintenance System (CIS/MS).

[7] https://dds.mil/
[8] Ibid.
[9] USAF announces Hack the Air Force 3.0, blog posting, accessed August 19, 2019 at https://www.af.mil/News/Article-Display/Article/1682502/usaf-announces-hack-the-air-force-30/

As security guru Bruce Schneier explained on his blog:

> An attacker could potentially pivot, Santamarta says, from the in-flight entertainment system to the CIS/MS to send commands to far more sensitive components that control the plane's safety-critical systems, including its engine, brakes, and sensors. Boeing maintains that other security barriers in the 787's network architecture would make that progression impossible."[10]

4. The Big Lesson – We Need Everybody to Help

These three experiences lead me to the conclusion that, when it comes to technology, and certainly military technology, "the more eyes the merrier" is generally a good policy. Sure, there will be some top-secret rooms on a warship, and there should be. However, by and large, all software programming and in fact hardware devices are stronger if they can be tested and tortured by the best minds in the world, some of whom don't work for you.

Even if you never have direct contact with military technology, it's a vital part of our world. And the lessons we learn from the military can often translate to the civilian world.

In the civilian world of the Internet of Things, we will may soon be worrying even more about injury and death from our reliance on technologies. As I wrote in the *Hill Times* earlier this year, the Silicon Valley culture of "Move Fast and Break Things" may be appropriate for a dating app where the worst thing that might happen is some bad matches. "Bringing in one piece of automation changes everything. We'll soon be facing these same issues with autonomous vehicles, package delivery drones, robotic surgeons, and techno-things we can't even imagine today. How can we survive them?"[11]

---

[10]Schneier on Security (blog) accessed August 19, 2019 at https://www.schneier.com/blog/archives/2019/08/software_vulner.html

[11] T.P. Keenan, "How computers kill people, or let's not 'move fast and break things'," *Hill Times*, 15 May 2019, accessed 19 August 2019 at

My recommendation, as expressed in that article, is more rigorous testing as well as enhanced education for professionals who deal with technology and those who manage them. Each of the programs described here shares that goal of improving our understanding of complex issues and helping us to be more informed citizens.

The folks at the DEFCON Aviation Village articulated their core values in a nice concise statement that could serve as a model as we move forward to build advanced systems that work safely and securely:

> The Aviation Village welcomes those who seek to improve aviation security, safety, and resilience through positive, productive collaboration among all ecosystem stakeholders.

As technologies get so complicated that even their creators can't understand them, the people who make them are going to need all the help they can get.

https://www.hilltimes.com/2019/05/15/how-computers-kill-people-or-lets-not-move-fast-and-break-things-2/199808