STRATEGIC PERSPECTIVES

NAADSN
North American and Arctic Defence and Security Network

naadsn.ca

October 27, 2020

Cyber Capacity Building in the Canadian Arctic and the North

Kristen Csenkey[1]
NAADSN Graduate Fellow
2020 WiDS-CGAI Fellow

Maj. Bruno Perron[2]
Canadian Intelligence Corps
2019 Masters Graduate, University of London SOAS, CISD

Executive Summary

- The Canadian Arctic cyber domain is set to rapidly expand in the next decade with emerging security vulnerabilities that would benefit from a multi-stakeholder Arctic Cyber Security Ecosystem.
- Great power competition will affect the Arctic as the United States, Russia, and now China seek to influence the resource rich region.
- Cyber is not only a matter of defence, but it is interconnected with education and economic development.
- The threat of disinformation is an example of how new ways of warfare can impact Canada through the Arctic.
- Cyber capacity building (CCB) could include domestic cyber education, skills training, and investment in scientific and technical (S&T) and information technology (IT) infrastructure.
- A focus on CCB would need to foster growth of resources available to territorial governments and local communities, hardening the region's cyberspace and support incident response to malicious cyber actor activity.
- Information technology security (ITSEC) resources need to be combined with community-based media literacy and critical thinking education programs to increase the region's resilience to malign influence.

---

[1] The authors would like to thank Dr. P. Whitney Lackenbauer, Dr. Shannon Nash, and Carla Johnston for the discussions that led to the creation of this paper.

[2] The views expressed in this document are his alone and do not represent the Department of National Defence or the Canadian Armed Forces.

Introduction

Capacity building in the Canadian Arctic and the North should address the current and future challenges of the threat environment. Disinformation and information operations are the "next great disruptors" and can impact the resiliency of local communities. The development of an Arctic cyber security ecosystem could contribute to enhanced cyber resiliency and should be considered part of cyber capacity building (CCB). A regionally-focused cyber security ecosystem could combine defence priorities with the development of scientific and technical (S&T) knowledge and expertise. This CCB program might include:

1) Investment in information technology security (ITSEC) programs, and
2) Targeted media literacy and disinformation programs.

The objectives of CCB in the Canadian Arctic and the North should reflect an investment in regional expertise in information technology (IT) and cyber security skills. We contextualize a vision for CCB in the region by:

- Commenting on the effectiveness of capacity building,
- Briefly outlining Canada's current defence role in the Arctic and the North,
- Describing the nature of threats and the challenges it poses for an increasingly complex security environment, and
- Providing tangible examples of a regionally-focused cyber security ecosystem.

We argue that an Arctic cyber security ecosystem that encourages the development of a tech savvy workforce and expertise, invests in critical media education, and includes defense priorities, may provide another avenue for innovative cooperation between local communities and the Department of National Defence (DND) / Canadian Armed Forces (CAF).

Cyber Capacity Building

Capacity building can be used to pursue multiple objectives, including economic development, foreign policy, law enforcement, and defence and security[1]. It can also reflect political agendas and the broader geopolitical climate or setting in place foundation blocks for future expected needs.

There are many actors involved in capacity building programs including international organizations (IOs), national governments, non-governmental organizations (NGOs), private sector actors, academic institutions, local communities, and individuals. This may result in competing or overlapping frameworks that can cause fragmentation in program implementation and impact effectiveness[2]. In order to reduce the disconnect between program objectives, frameworks, and actors, capacity building programs should be dynamic and focus on creating linkages between multiple stakeholders.

Cyber is a part of capacity building and usually focuses on increasing resiliency against cyber attacks and developing norms at a domestic or international level[3]. It also includes "all types of activities (e.g. human resources development, institutional reform or organisational adaptations) that safeguard and promote the safe, secure and open use of cyberspace"[4]. Generally, the effectiveness of CCB programs is increased when the parameters, context, and objectives of the program are clearly defined[5]. It is also argued that CCB programs are most effective when they include multiple actors through partnerships, reflect the needs of the recipients,

and focus on the technological, human, and organizational aspects of security and development[6].

From a national defence and security perspective, CCB is often used to build cyber resiliency and manage cyber governance. This type of CCB often reflects national security objectives through a focus on sovereignty. Yet, this objective alone does not guarantee success. It is important that CCB reflects a holistic focus on cyber governance by strengthening national cyber education and S&T knowledge and skills. This is because a focus on cyber solely as a military objective does not necessarily result in enhanced cyber capacity[7]. Instead, programs should recognize the regional perspectives, or 'textures'[8], to defence and security challenges. They also need to recognize the dual nature of CCB as a nexus of cyber defence and development. For the Canadian Arctic, solutions should concentrate on empowering local communities and increasing the cyber defense resiliency of territorial governments and populations. A Canadian Arctic-focused CCB is a step towards defining current and future defence priorities while strengthening cooperation between actors.

Canada's Defence Role in the Arctic and the North

The DND / CAF approach to capacity in the region is primarily focused on the maintenance of sovereignty. As per Strong, Secure, Engaged (SSE), DND seeks to increase its long term presence in the Arctic and cooperation with relevant regional actors in order to "enhance the Canadian Armed Forces' ability to operate in the Arctic and adapt to a changed security environment." There is an emphasis on surveillance and control with the aim to detect, deter, and defend against threats to Canadian sovereignty and security.

Current CAF engagement in the Arctic and the North takes the form of exercises, regionally-specific operations, and collaboration with local populations. The Joint Task Force North (JTFN) — as part of the Canadian Joint Operations Command (CJOC) — is assigned with overseeing the Arctic region in Canada. The JTFN works closely with various detachments and units, including the 1st Canadian Rangers Patrol Group (1 CRPG) spanning the Territorial North and northern British Columbia, which contribute substantively to the defence and security of the Arctic and northern regions in Canada.

The Rangers are the "military's eyes, ears, and voice in remote communities", especially in the North. They undertake a variety of tasks on behalf of the CAF, but the role of the Rangers goes beyond maintaining sovereignty. The Rangers integrate regional and cultural diversity into defence objectives and therefore enhance CAF capabilities[9]. Their community-based presence and influence places them in a unique position. As others have argued, the Rangers' positioning could allow them to address emerging challenges in their communities. Without overburdening their current roles and responsibilities, perhaps their community influence could include CCB initiatives and training.

The CAF also conducts operations in the region — some are focused on specific Arctic areas, while other operations encompass the region as part of the JTFN authority. Operation NANOOK is one such example. Op NANOOK is a year-round northern and cold weather operation that aims to enhance "Canada's surveillance and presence across its northernmost regions, strengthens coordination with whole-of-government partners and the way Canada's military operates in arctic conditions". In addition to Op NANOOK, Operation NEVUS and to some extent, Operation LIMPID, seek to enhance Canada's presence and commitment to the Arctic

with the aim of maintaining sovereignty. Yet, the geostrategic environment has changed since SSE was published and there are new threat areas to address.

New Threats: Disinformation is an Emerging Threat in the Region

Disinformation is a part of hybrid warfare and present in the global security environment[10]. The Arctic region is not immune to such threats and, as General O'Shaughnessy, former Commander of U.S. Northern Command (USNORTHCOM) and North American Aerospace Defense Command (NORAD), argues: "The Arctic is no longer a fortress wall". In addition, the Arctic is frequently seen as a key location of great power competition[11], linking it to larger geopolitical objectives. This makes addressing the threat of disinformation especially relevant to defence priorities in the Arctic and the North in Canada.

A 2011 Senate report entitled "Sovereignty and Security in Canada's Arctic" did not contain the words misinformation, disinformation, or hybrid warfare. The threat portion of the report concentrated on great power competition for resources and access to the Arctic. This may still be fundamentally true, however the 'means' used by potential adversary States, notably Russia, have evolved greatly during the subsequent decade. The widely attributed Russian invasion of Eastern Ukraine and Crimea in 2015 is the prototype for new conflicts. A doctrine broadly attributed to Russian Chief of the General Staff – General Valery Gerasimov uses an agile combination of non-military and military measures to achieve political objectives[12]. NATO calls this hybrid warfare[13]. Interestingly, Russian authorities claim this approach to be inspired by alleged Western interference in a series of "Colour Revolutions" throughout the former Soviet sphere of influence after its collapse.

Unlike Western powers that are evolving militarized cyberspace capabilities primarily from an extension of cyber security, Russia sees it primarily as an enabler of information operations[14]. What may seem like a nuance is quite impactful as it aims to exploit liberal democratic principles of freedom of expression, a free press, and the right to participate in the public discourse. Rather than using computer-network exploitation (CNE) to obtain intellectual property for economic gain like Chinese cyber-actors, Russian malicious actors tend to focus on the acquisition of "kompromat" that aims to embarrass, sow dissent, or degrade cohesion. The most notable example is the Democratic National Convention hack attributed to Russia malicious cyber actors in 2015-16 and subsequent release of compromising material through WikiLeaks to influence the US Presidential election. Reported activity has only increased since the seminal 2016 election.

A resilient cybersecurity environment would protect Canada's ability to provide Arctic governance in this growing threat environment. The extensive list of known victims of one Russian linked malicious cyber actor, namely Fancy Bear or APT 28, reveals the plausibility of operations conducted to degrade unity and sow discord in Canada's Arctic region. Potential targets could include stakeholders like Crown-Indigenous Relations and Northern Development Canada (CIRNAC), Public Safety Canada, the territories' Governments, and even local community governments or online data or notable personalities with an Arctic connection. There is likely a wide range of documents that could be inflammatory if misused, leaked, or released out of context through proxies, or anonymized disclosure platforms like WikiLeaks.

Another emerging tactic associated with malicious influence is the internet "troll" farm, which creates large

volumes of misinformation and disinformation exploiting natural inflection points in society like race, inequality, regionalism, etc. This term also rose to prominence in the aftermath of the 2016 US Presidential election through the indictment[15] of the St-Petersburg based Internet Research Agency troll farm[16]. This tactic is difficult-to-attribute[17], which makes its proliferation relatively low-risk, low-cost, and difficult to counter by conventional State tools, especially in liberal democracies that value the free exchanges of ideas. It is widely agreed that malicious State-sponsored trolls are linked to anti-vaxxers[18], efforts to incite violence around the Black Lives Matter (BLM) movement, inciting tensions during the Catalonian referendum, and degrading cohesion between the Russia diaspora and NATO in the Baltic States. The latter includes information confrontation against Canada's deployment in Latvia.

The current Kremlin regime has stated a keen interest in dominating the Arctic sphere of influence, which could be treated as a warning of impending malign influence[19] in the Canadian Arctic. Evidence suggests that Russia is targeting fellow NATO member, Denmark and its Arctic communities of Greenland and the Faroes, which should serve as a bellwether for interference in Canada's North[20].

Foreign Influence and Interest in the Arctic

The Arctic's natural resources make it especially attractive to foreign state and private sector investment. Public perception of foreign and private sector actor involvement is an important factor in the threat landscape in the region. Foreign investment, through state-owned enterprises (SOEs), remains controversial in the region and is often regarded as a threat to national security. Chinese investment in Arctic resources is a notable example of foreign investment and could be a possible source of disinformation campaigns in the future. Disinformation campaigns could be used to sway public opinion on this issue area. For example, the Hope Bay Mining Project in Nunavut is set to be bought by the Chinese SOE, Shandong Gold Mining. While this project has raised concern for its impact on the local ecology, community, and economy, another issue remains: China's use of disinformation as part of its ambitions and power projection in the region.

Arctic governance is part of China's ambitions in the region. The use of disinformation may aid in achieving these ambitions and projecting their geopolitical power. As a Non-Arctic State Observer, China does not have voting power in the Arctic Council, but the state's interests in regional governance raises some questions among Arctic states[21]. The White Paper on China's Arctic Policy outlines the country's plan for Arctic governance. This includes economic investment, rule 'making' and norms 'shaping', scientific research, and engagement with Indigenous communities. China is also involved in IT infrastructure development through the Polar Silk Road Strategy (PSR), part of the Digital Silk Road (DSR) and the Belt and Road Initiative (BRI) projects. The Chinese focus on Arctic digital connectivity and IT development through the PSR is argued to have provided an opportunity for China to further advance its cyber goals, especially in the wake of COVID-19. Although subsea cables have been the focus on infrastructure and connectivity in the Arctic region, other linkages such as the emerging relationships between data, cyber security, and the Arctic (as part of the PSR and DSR) have become more apparent[22].

Other Chinese SOE's have set their sights on the Arctic and seek to link their objectives to Canadian priorities. For example, Huawei has shown interest in expanding internet access in the Canadian Arctic. It could be the most cost-effective solution to meet the Canadian Government's promise to provide high-speed internet

access to all households by 2031 in a region still highly dependent on legacy satellite communications. Huawei has competition from a UK-based project called OneWeb, who are launching a constellation of small modern satellites like SpaceX's starlink service. Although supply chain is an important factor, the bigger take-away is the rapid proliferation of internet access in the region. An increasingly complex security environment requires creative and collaborative solutions to address emerging threats.

An Arctic Cyber Security Ecosystem

Disinformation, foreign interference, and information operations are all a part of hybrid warfare. Adversarial actors can use these tactics to execute their own objectives. Current Canadian defence priorities need to evolve to reflect the changing nature of warfare and the importance of robust regional S&T expertise. In order to address threats and support cyber education and skills, defence priorities should focus on a CCB that engages local communities and provides avenues for economic growth. The development of a regionally-focused cyber security ecosystem will enhance resiliency, support defence priorities, and economic development. A focus on ITSEC and media literacy programs will help Canada address disinformation, increase security, and expand collaborative partnerships in the region, while effectively addressing the threats associated with hybrid warfare.

A High-Tech Arctic

IT infrastructure development and investment in S&T in the Arctic and the North is important for establishing a cyber security ecosystem. This will aid in regional economic development and foster local expertise through education and training. This ecosystem could take shape as a partnership between the territories, local community institutions and organizations, select private sector actors, and DND.

CyberNB is an example of a regional-focused cyber security ecosystem based on multi-stakeholder collaboration. CyberNB partners with government, academia, and private sector actors to address security and economic challenges in Canada and regionally. It also aims to engage and invigorate the Atlantic region through economic investment and a focus on skills development. An investment in an Arctic cyber security system, similar to CyberNB, could help increase local resiliency, focus on ITSEC programs, and support an interest in STEM fields, in which women and Indigenous peoples are underrepresented[23].

This type of ecosystem could also diversify investment, invigorate the digital economy, and foster entrepreneurship. For example, programming could encourage a local startup culture that recognizes the needs, creativity, and innovation of Indigenous communities. This could also be an opportunity for academic institutions in the region to develop their program offerings to include cyber security components. This may aid in fulfilling plans to create a polytechnic university in the Canadian Arctic region and provide opportunities for collaboration with neighbouring US academic institutions in Alaska[24]. Although this may not fulfil the calls for an unified Arctic security institution, a regional-focused cyber security ecosystem, as part of CCB, may help address the key issue areas and threats in the Arctic and the North.

Engagement, Operations, and Operators

Cyber-related skills and expertise are needed to address the threats associated with hybrid warfare. These skills are also important for CAF recruitment initiatives, diversification, as well as meaningful engagement with local communities.

CAF engagement with Northern and Indigenous communities is shown to strengthen networks and cooperation, but engagement needs to go beyond social media outreach[25]. Currently, the Aboriginal Leadership Opportunities Year (ALOY), Canadian Forces Aboriginal Entry Program (CFAEP), and summer training programs[26] focus on general recruitment. A CCB program that focuses on engagement with Northern and Indigenous communities might entail investment in ITSEC expertise through IT specialist certification, and cyber security programs through practical and skills-based courses and media literacy workshops. This type of program could incorporate a bridging program to the CAF's recently established cyber operator position. This could be another venue of engagement and meaningful relationship building with northern Indigenous communities[27] as well as a way to encourage skills-based recruitment and retention[28].

Increasing ITSEC expertise in Northern Canada would limit the potential for damaging information compromises, but it is unlikely to completely stop the threat of disinformation. The CAF experience with information warfare rose to a peak in Afghanistan[29], but this expertise has been far more controversial in domestic settings. The Department was criticized for an early effort to use its influence tools and tradecraft in an attempt to track the spread of COVID-19 and counter harmful disinformation. Perhaps the role of a military should be at arm's length from the domestic discourse. This should not restrict CAF from implementing a program that delivers media literacy and critical thinking skills, creating a more resilient information environment for Northern Communities. The important community role of CAF's Rangers makes them attractive candidates for such training. Rangers could be well suited as allies to a wider Arctic cybersecurity ecosystem program bringing evidence-based[30] media literacy education to small and dispersed Northern classrooms.

Realizing Connectivity and Fulfilling Mandates

The establishment of an Arctic cyber security ecosystem is in-line with several policy frameworks and objectives in Canada. For example, it could be incorporated as part of the Government's commitment to realize the High-Speed Access for All: Canada's Connectivity Strategy and invest in IT infrastructure. The Canadian government recently released plans to improve broadband internet services in some parts of the region as part of the Canadian Radio-television and Telecommunications Commission (CRTC) Broadband Fund over the next ten years. This is especially important for Indigenous communities to connect and benefit from advanced and reliable internet connectivity. Yet, an investment in IT infrastructure must also be paired with an investment in education, S&T, and skills training to truly benefit Canadians in the Arctic and the North as well as DND's defence priorities.

In addition, Canada's Arctic and Northern Policy Framework (ANPF) and the Safety, Security, and Defence chapter, aims to "support science, knowledge and research that is meaningful for communities and for decision-making" and "ensure that Canada and our northern and Arctic residents are safe, secure and well-defended". A regionally-focused cyber security ecosystem will provide a tangible way for Canada to realize the ANPF, which has received criticism and skepticism for appearing to lack a defined path to implementation. The

ANPF and the Safety, Security, and Defence chapter does not place enough emphasis on addressing cyber threats as part of the objective to "strengthen Canada's domain awareness, surveillance, and control capabilities." As we have shown, strategic planning in the region needs to recognize cyber threats and reflect the current and future security environment. It also needs to empower local actors by focusing on regional collaboration.

Conclusion

The purpose of an Arctic cyber security ecosystem is twofold: to address threats from a complex and evolving threat environment and promote investment in S&T knowledge and skills training. The Arctic region poses unique security challenges, and these will become amplified in the future. We have shown that disinformation is a security challenge that could permeate the region. Canada should combine defence priorities with a focus on ITSEC training and education through CCB programs. There are five main benefits to this type of CCB program:

1) Proactively addresses the threat of disinformation,
2) Promotes economic development through S&T and IT investment,
3) Focuses on cyber education and skills training,
4) Supports local creativity and entrepreneurship, and
5) Fulfils numerous policy priorities and mandates, such as SSE, ANPF, and the Connectivity Strategy.

This program may also aid in recruitment initiatives within the CAF by engaging with underrepresented groups.

CCB in the Arctic and the North is a long-term investment and is not without constraints. IT infrastructure development and maintenance, funding, coordination, and support for this type of initiative are just a few possible setbacks. There also needs to be careful consideration as to the types of private sector actors who could engage in this program, the organization, the ecosystem, and the representation (on board of directors, executive positions, amplify local decision-making, etc.). The European Union (EU) has engaged in the development of CCB programs through the establishment of a Cyber Capacity Building Task Force (through a joint partnership with the EU Institute for Security Studies). While the Task Force mainly focuses on external and international CCB programs, their Operational Guide provides frameworks, organizational structures, and applications for CCB activities. A Canadian CCB Task Force may aid in beginning to address some of the challenges associated with this type of development in the region.

As Canada deals with the ongoing COVID-19 pandemic, DND / CAF will certainly be faced with difficult capacity-building decisions. The future of capacity building within this context could focus on fulfilling domestic defence priorities, addressing future threat areas from foreign actors, and proactively manage the impending economic impacts and budget constraints exacerbated by the pandemic. However this project manifests, it is important that regional actors are consulted and included in the decision-making process.

Notes

[1] Pawlak, Patryk. "Capacity Building in Cyberspace as an Instrument of Foreign Policy." *Global Policy* 7, no. 1 (2016): 83-92.
[2] Pawlak, Patryk, and Panagiota-Nayia Barmpaliou. "Politics of Cybersecurity Capacity Building: Conundrum and Opportunity." *Journal of Cyber Policy* 2, no. 1 (2017): 123-44.
[3] European Union Institute for Security Studies. *Cyber Capacity Building in Ten Points*. European Union: Brussels, 2014. https://www.iss.europa.eu/sites/default/files/EUISSFiles/EUISS_Conference-Capacity_building_in_ten_points-0414.pdf
[4] Pawlak, Patryk. *Operational Guidance for the EU's international cooperation on cyber capacity building*. European Commission: Luxembourg, 2018. https://www.iss.europa.eu/sites/default/files/Operational%20Guidance%20for%20the%20EU%E2%80%99s%20international%20cooperation%20on%20cyber%20capacity%20building%20%E2%80%93%20A%20Playbook.pdf
[5] Dutton, William H., Sadie Creese, Ruth Shillair, and Maria Bada. "Cybersecurity Capacity: Does It Matter?" *Journal of Information Policy* 9 (2019): 280-306.
[6] Pawlak, Patryk, ed. *Riding the digital wave: The impact of cyber capacity building on human development*. EU Institute for Security Studies, 2014. https://www.iss.europa.eu/sites/default/files/EUISSFiles/Report_21_Cyber.pdf
[7] Calderaro, Andrea, and Anthony J.S. Craig. "Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building." *Third World Quarterly* 41, no. 6 (2020): 1-22. - OR 917-38?
[8] Triandafyllidou, Anna, ed. *Global Governance from Regional Perspectives: A Critical View*. Oxford University Press, 2017.
[9] Lackenbauer, P. Whitney. "The North's Canadian Rangers." In *Strengthening the Canadian Armed Forces through Diversity and Inclusion*. Alistair Edgar, Rupinder Mangat, and Bessma Momani (eds). University of Toronto Press, 2020.
[10] Martens, Bertin, Luis Aguiar, Estrella Gomez-Herrera, and Frank Müller-Langer. "The digital transformation of news media and the rise of disinformation and fake news." Joint Research Centre (JRC), European Commission Digital Economy Working Paper, No. 02. 2018. https://www.econstor.eu/bitstream/10419/202231/1/jrc-dewp201802.pdf
[11] Nash, Shannon. "U.S. Arctic Messaging in an Era of Renewed Great Power Competition." *NAADSN Policy Brief*. 18 November 2019. https://www.naadsn.ca/wp-content/uploads/2020/04/Nash_US-Messaging_Policy-Brief_November-20191.pdf
[12] Bartles, Charles K. "Getting Gerasimov Right." *Military Review* (January-February 2016): 30-38.
[13] Giles, Keir. *Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power*. London: Chatham House Royal Institute of International Affairs, 21 March 2016.
[14] Giles, Keir, and Anthony Seaboyer. "The Russian Information Warfare Construct". DRDC Report, March 2019. https://cradpdf.drdc-rddc.gc.ca/PDFS/unc341/p811007_A1b.pdf
[15] Department of Justice. United States v. IRA. 2018. Accessed on 12 November 2018 at: https://www.justice.gov/file/1035477/download
[16] Howard, Philip N., Bharath Ganesh, Dimitra Liotsiou, John Kelly, and Camille François. *The IRA, Social Media and Political Polarization in the United States, 2012-2018*. Oxford: Oxford University's Computational Propaganda Research Project, 2018. https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/12/IRA-Report.pdf
[17] Carr, Hope. "The power of non-attribution in modern information warfare. Stavanger, Norway: NATO Joint Warfare Centre". *The Three Swords Magazine* 33 (2018). http://www.jwc.nato.int/images/stories/threeswords/Fighting_Ghosts_2018.pdf
[18] Walter, Dror, Yotam Ophir, and Kathleen Hall Jamieson. "Russian Twitter Accounts and the Partisan Polarization of Vaccine Discourse, 2015-2017." *American Journal of Public Health* 110, no. 5 (May 2020):718-24. doi: 10.2105/AJPH.2019.305564.
[19] Sukhankin, Sergey. "The Western Alliance in the Face of the Russian (Dis)Information Machine: Where Does Canada Stand?" *Canadian Global Affairs Institute* 12, no. 26 (September 2019). https://www.cgai.ca/the_western_alliance_in_the_face_of_the_russian_disinformation_machine_where_does_canada_stand
[20] Sukhankin, Sergey. "Culture, Money, Propaganda: Russia's Approach Toward Greenland and the Faroe Islands." *Eurasia Daily Monitor* 16, no. 90 (June 2019). https://jamestown.org/program/culture-money-propaganda-russias-approach-toward-greenland-and-the-faroe-islands/

[21] Koivurova, Timo, Liisa Kauppila, Sanna Kopra, Marc Lanteigne, Mingming Shi, Malgorzata (Gosia) Smieszek, and Adam Stepien, in co-operation with Juha Käpylä, Harri Mikkola, Egill Þór Níelsson, and Matti Nojonen. *China in the Arctic; and the Opportunities and Challenges for Chinese-Finnish Arctic Co-operation*. Finish Prime Minister's Office, 2019. http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161371/8-2019-China_Arctic_andFinland.pdf

[22] Khorrami, Nima. "Data Hunting in Subzero Temperatures: The Arctic as a New Frontier in Beijing's Push for Digital Connectivity." *The Arctic Institute.* 4 August 2020. https://www.thearcticinstitute.org/data-hunting-subzero-temperatures-arctic-new-frontier-beijing-push-digital-connectivity/

[23] Cronk, Terri Moon. "Women, Minorities Underrepresented in Cybersecurity, DOD Expert Says." *DoD News.* 2 September 2020. https://www.defense.gov/Explore/News/Article/Article/2334909/women-minorities-underrepresented-in-cybersecurity-dod-expert-says/

[24] For example, the University of Alaska Anchorage's Computer and Networking Technology Department and the University of Alaska Fairbanks Community and Technical College's Information Technology programs.

[25] Landriault, Mathieu, and Jean-François Savard. "Engagement with Inuit People by the Canadian Military via social media." *NAADSN Policy Brief.* 6 March 2020. https://www.naadsn.ca/wp-content/uploads/2020/04/Policy-Brief-Landriault-and-Savard_March-9.pdf

[26] These include: Bold Eagle, Raven, Black Bear, Carcajou, and Grey Wolf.

[27] For other examples of CAF engagement with Indigenous communities in Canada, see: Kikkert, Peter, and P. Whitney Lackenbauer. "Using Civil-Military Operations to "Expand and Deepen" Relationships with Northern Communities: Examples from Alaska and Australia." *NAADSN.* July 2020. https://www.naadsn.ca/wp-content/uploads/2020/08/2020-jul-Kikkert-Lackenbauer-Civ-Mil-Northern-NAADSN.pdf; Lackenbauer, P. Whitney. *Strengthening the Canadian Armed Forces through Diversity and Inclusion.* Alistair Edgar, Rupinder Mangat, and Bessma Momani (eds). University of Toronto Press, 2020 - ALREADY CITED. PERHAPS USE Lackenbauer, "The North's Canadian Rangers"; and Lavoie, Jayde, and Jill Barclay. "Improving the Canadian Armed Forces' Recruitment and Retention of Indigenous People: Best Practices from the New Zealand Defence Force." *NAADSN Policy Brief.* 8 September 2020. https://www.naadsn.ca/wp-content/uploads/2020/09/20-September_Policy-Brief-CAF-1.pdf

[28] As per the recommendations in Fuhr, Stephen. *Improving Diversity and Inclusion in the Canadian Armed Forces: Report of the Standing Committee on National Defence*. House of Commons 42nd Parliament, 1st Session. June 2019. https://www.ourcommons.ca/Content/Committee/421/NDDN/Reports/RP10573700/nddnrp17/nddnrp17-e.pdf

[29] Harmes, David T. *International Radio Broadcasting and Post-Conflict State-Building: The Case of Canada's Rana FM*. Doctoral Dissertation, Ryerson University. 2012. https://digital.library.ryerson.ca/islandora/object/RULA%3A1167

[30] McDougall, Julian, Marketa Zezulkova, Barry van Driel, and Dalibor Sternadel. "Teaching media literacy in Europe: evidence of effective school practices in primary and secondary education". *NESET II Report*. Luxembourg: Publications Office of the European Union, 2018. http://eprints.bournemouth.ac.uk/31574/1/AR2_Teaching%20Media%20Literacy_NESET.pdf