Centre for
International and
Defence Policy
at Queen's University

Policy Brief

November 2024 | Volume 9, Issue 9

The Arctic Online:

Cybersecurity is Quintessential for Canada's Arctic Security

Claire Parsons
CIDP Researcher

Andrew Heffernan
CIDP Researcher

**The Centre for
International and Defence Policy**

138 Union Street, Suite 403. Queen's University,
Kingston, Ontario Canada K7L 3N6

cidp@queensu.ca

Introduction

The Arctic is a hallmark of Canadian identity; the tundra landscape and the frigid temperatures are a point of pride for the resilient and frosted Canuck. In fact, Arctic territory makes up 40% of Canada's sovereign land and the Northern Arctic coastline is a key facet of Canada's borders[1]. Canada has also pursued further Arctic territory recognition through its 2019 submission to the Commission on the Limits of the Continental Shelf at the United Nations. In addition, there are 200,000 people, the majority of whom are Indigenous, who live in the Arctic. The Arctic is an essential part of Canada's economy as well as its identity with the famous Northwest passage flowing through the islands of Nunavut and monitored by Canadian Rangers and other search and rescue teams[2]. As a result, the Arctic has become a beloved and vital part of Canada's nationhood and statecraft—one which it places high priority on protecting [3] [4].

Concerningly, threats to the Arctic are on the rise. The most traditional of these threats include Russian and Chinese posturing and dual-use, meaning it can respond to both civil issues and security threats, development of former Cold War bases, new missile systems, and monitoring buoys. In particular, the Russian invasion of Ukraine has straightened the spines of other Arctic nations concerned about their own sovereign and contested lands being targeted. However, threats from other states are not the only concern in the Arctic: the greatest threat the Arctic faces is deterioration from the rapidly accelerating consequences of climate change. The Arctic is warming at a rate four times the global average, and the melting of ice in the region has increased traffic of maritime vessels in the Northwest passage. Increased traffic not only contributes to climate deterioration but also prevents proper regulation and could cause safety risks for both sailors and Arctic residents. The final threat is the lack of critical infrastructure and stable industry in the Arctic. The local Indigenous populations have faced severe challenges due to lack of healthcare, education, stable internet and energy, and more. While there are plans and funds to improve the infrastructural security of Arctic communities, further climate deterioration will bring extreme weather events which will create new vulnerabilities in critical infrastructure.

The existing Canadian Northern strategies have all been released in the past five years. The first framework, outlining the basics of how Canada seeks to treat the Arctic, is *Canada's Arctic and Northern Policy Framework*. The strategy does not just outline the sovereign security of the Arctic but also the development of the region as a whole. The North American Aerospace Defense Command (NORAD) has also released an *Executive Strategy* to modernize the alliance to protect the Arctic and its subsequent planned development[5]. The Arctic is also a consistent theme in the latest Canadian Defence Policy update, *Our North, Strong and Free*. Lastly, the Canadian senate recently released a report entitled *Arctic Security Under Threat* which analyzes the security and climate implications of the region. Notably missing from these documents are specific answers to the intelligence collection approaches of Canadian adversaries. Canada is prepared to tackle climate change, support alliances, and ensure the development of local communities. What Canada is not prepared for is the continual pressures on the Arctic from the cyber domain and the harm that could be done to the critical infrastructure that it founds the rest of its Arctic strategy upon.

The Increased Relevance of Arctic and Cyber Politics

The intersections between shifting geopolitics, climate change, and technological advancements have elevated the importance of both Arctic and cyber politics on the global stage. This section explores the evolving dynamics in these arenas, focusing on the Arctic Council, Canada as a middle power and its cyber vulnerabilities, and the involvement of state adversaries in both Arctic and cyber domains.

The Arctic Council

The Arctic region, long characterized by its extreme climate and remote geography, has become a focal point of international cooperation and competition 6 7 8. The Arctic Council, established in 1996, exemplifies collaborative efforts among Arctic states and Indigenous communities to address environmental protection and sustainable development in the region 9. Comprising eight Arctic states—Canada, Denmark (including Greenland and the Faroe Islands), Finland, Iceland, Norway, Russia, Sweden, and the United States—the Council provides a platform for these nations to discuss and coordinate policies concerning the Arctic.

Some of the key challenges facing the Arctic Council are the impacts of climate change. Rapidly melting sea ice has opened up new shipping routes and access to previously unattainable resources, such as oil and gas reserves. This has intensified competition for territorial claims and resource extraction, raising concerns about environmental degradation and Indigenous rights10. Furthermore, geopolitical tensions have also seeped into Arctic affairs. Russia, for instance, has been assertive in its Arctic policy, bolstering military presence and infrastructure in its Northern territories11. This militarization has sparked debates among Arctic Council members regarding security implications and the potential for conflict escalation in the region.

The Arctic Council's significance extends beyond environmental and security issues to economic opportunities and global trade routes[12]. As ice melts, the Northwest Passage and Northern Sea Route are increasingly viable for shipping, offering shorter transit times between Asia and Europe[13]. This potential economic boon underscores the Arctic's growing importance in international trade and maritime logistics.

While the Arctic Council promotes cooperation on environmental stewardship and sustainable development, geopolitical rivalries and economic interests continue to shape Arctic politics. The Council remains a critical forum for dialogue and multilateral engagement, yet it faces ongoing challenges in balancing environmental conservation with economic development and security concerns.

Canada as a Middle Power and Cyber Vulnerabilities

Canada, recognized as a middle power, plays a significant role in Arctic governance and international relations. As an Arctic state and member of the Arctic Council, Canada is committed to environmental protection and sustainable development in its Northern territories. However, Canada's geopolitical position also exposes it to cyber vulnerabilities, which have become increasingly relevant in present-day international politics[14]

Cyber threats pose significant risks to Canada's national security, economy, and critical infrastructure, and all of these are particularly susceptible to changing conditions in the fragile and remote regions of the Canadian Arctic[15]. As a highly digitized economy, Canada relies heavily on information and communication technologies (ICT), making it susceptible to cyber espionage, ransomware attacks, and misinformation campaigns. The sparsity in the network of government agencies, businesses, and citizens in the North amplifies the potential impact of cyber incidents on Canadian society[16].

Canada's role as a middle power in an era displaying some characteristics of a return to great power politics amplifies its vulnerability in cyberspace. While not a major global military power, Canada's participation in international peacekeeping missions and diplomatic engagements makes it a potential target for state-sponsored cyber attacks. Adversarial states may seek to exploit Canada's cyber vulnerabilities to gather intelligence, disrupt operations, or undermine public trust in democratic institutions[17]. Once again, all these vulnerabilities are multiplied in the Arctic where Canada has been unable and/or unwilling to solidify sovereignty over its vast Northern territory.

In response to these challenges, Canada has prioritized cybersecurity as a national security imperative. The Canadian Centre for Cyber Security (CCCS) coordinates efforts to protect against cyber threats, enhance resilience, and promote cybersecurity awareness among government agencies, private sector entities, and the general public[18]. Collaborative initiatives with international partners, including NATO and the Five Eyes intelligence alliance, strengthen Canada's cybersecurity posture and mitigate risks in a globally interconnected digital landscape.

Canada's dual role as an Arctic stakeholder and middle power underscores the interconnected nature of Arctic and cyber politics. Addressing cyber vulnerabilities is essential to safeguarding Canada's national interests and upholding its commitments to international cooperation and security.

State Adversaries and Their Involvement in Arctic and Cyber Realms

State adversaries play a pivotal role in shaping Arctic and cyber politics through strategic investments, military activities, and cyber operations. The intersection of these domains reflects broader geopolitical ambitions and rivalries among global powers.

Russia, as a prominent Arctic state, has pursued an assertive Arctic policy aimed at expanding its territorial claims and securing access to strategic resources. The Russian military has modernized its Arctic infrastructure, establishing military bases and conducting large-scale military exercises in the region[19]. These actions underscore Russia's commitment to safeguarding its Arctic interests and projecting power in the North.

In the cyber domain, Russia has been accused of engaging in state-sponsored cyber operations targeting Western democracies, including Canada[20]. Russia has employed cyber espionage, disinformation campaigns, and disruptive cyber attacks to influence public opinion, undermine democratic processes, and gather sensitive information about both its partners and adversaries[21]. The integration of cyber capabilities into Russia's broader geopolitical strategy highlights the dual use of technology for both defensive and offensive purposes.

Similarly, China has emerged as a significant player in Arctic affairs and cyberspace. Despite not being an Arctic state, China has shown interest in the region's economic potential and maritime routes. Through its Belt and Road Initiative (BRI), China seeks to enhance infrastructure connectivity and expand global trade networks, including Arctic shipping routes[22]. This economic ambition aligns with China's broader strategy of global influence and resource acquisition.

In cyberspace, China has been accused of conducting cyber espionage against Western countries to steal intellectual property, gain technological advantage, and influence global governance structures[23]. The integration of cyber capabilities into China's foreign policy toolkit reflects its growing assertiveness in international relations and its willingness to challenge established norms and institutions.

State adversaries' involvement in Arctic and cyber realms underscores the complex interplay between geopolitics, technology, and national security. Understanding these dynamics is essential for Arctic Council members and other stakeholders to navigate challenges, mitigate risks, and promote cooperative solutions in both Arctic and cyber domains.

The increased relevance of Arctic and cyber politics in the 21st century reflects profound shifts in global dynamics driven by climate change, technological advancements, and geopolitical rivalries. The Arctic Council serves as a critical platform for multilateral cooperation among Arctic states, despite challenges posed by environmental changes and geopolitical tensions. Canada, as a middle power, faces cyber vulnerabilities that intersect with its Arctic interests, highlighting the interconnected nature of contemporary international politics. State adversaries, such as Russia and China, leverage Arctic and cyber domains to advance strategic interests and influence global governance, underscoring the importance of addressing these multifaceted challenges through diplomacy, innovation, and international cooperation.

The Arctic Needs Cyber

The Arctic is set to benefit from NORAD's $38.6 billion modernization plan, with a new Over-The-Horizon radar, expanded military infrastructure, and other critical infrastructure developments tied to quality of life of local civilians working on such developments and service members posted to maintain them. In addition to this development, procurement operations for ground-based air defences and new ships for the Royal Canadian Navy are underway24. There are noted risks in Canada's NORAD and Northern strategies, including the continual issue of climate change as well as adversarial nations with which Canada and the United States are actively competing25 26.

The name of the game in the Arctic is surveillance, and at present the combination of a lack of investment in NORAD and the effects of climate change are putting Canadian territory into positions vulnerable to foreign spying. There have been previous records of state-sponsored Russian and Chinese attacks on Canadian infrastructure that is far more protected than its Northern counterparts27. The reactivation of Russian Cold War bases and increased investment in Chinese Arctic technology make it clear that Canada's primary adversaries are interested in the movements of NORAD and NATO ally behaviour in the North. While Canada's Five Eyes allies are vital to its surveillance prevention, only the United States is a pertinent Arctic ally28. As a result, NORAD's investment in security is Canada's most logical pathway towards the new era of climate change-informed surveillance and intelligence in the Arctic.

Climate change has directly impacted the ability of Canada's adversaries to make headway in the Arctic: the continual melting of ice has made the Arctic increasingly accessible, and the current military infrastructure is remnant of the Cold War. The new military infrastructure required must be dual-use. This can be done through simultaneously providing for the local Arctic population and coordinating with their knowledge of the region to preserve the ecosystem. A better-preserved ecosystem will mean that the infrastructure required will not be harmed by extreme weather. Critical infrastructure like energy, food services, further healthcare, and more communications technology are all needed to increase the quality of life and the quality of service for both citizens and service members in the Arctic. Part of this process will require the essential protection of new critical infrastructure from potential attacks which is complicated by the fact that these kinds of critical infrastructure are made vulnerable by climate change, thus making them easier targets for adversaries29 30.

For Canada, the biggest risk to infrastructure developed through its Arctic strategies is extreme weather. Climate change in the Arctic has increased extreme weather events which pose distinct challenges to critical infrastructure projects and emergency management. For instance, infrastructure that is not cold weather resilient has less of a livelihood in Arctic temperatures. Thus, Canada is presented with the challenge of developing critical infrastructure constantly at risk for damage and targeting by both climate change and adversaries.

Policy Recommendations

1. **Enhancing Cybersecurity Measures in Canada's Arctic Regions:** Given Canada's vulnerability to cyber threats in its Arctic territories, it is crucial to bolster cybersecurity infrastructure and resilience in these remote areas. This could involve:
    - Increasing investment in cybersecurity resources specifically tailored for the Arctic regions.
    - Establishing specialized cybersecurity training programs and support for local communities and businesses.
    - Implementing comprehensive monitoring and response mechanisms to detect and mitigate cyber threats effectively.

2. **Strengthening Multilateral Cybersecurity Cooperation:** Canada should lead efforts within international forums, including the Arctic Council, to enhance cybersecurity cooperation among Arctic states. This could include:
   - Promoting information sharing and best practices on cybersecurity resilience and response strategies.
   - Facilitating joint cybersecurity exercises and capacity-building initiatives among Arctic Council members.
   - Encouraging the development of international norms and agreements to address cybersecurity challenges in Arctic regions.
3. **Integrating Cybersecurity into Arctic Policy Frameworks:** Canada should integrate cybersecurity considerations into its Arctic policy frameworks to safeguard national interests and promote sustainable development. This involves:
   - Incorporating cybersecurity assessments into environmental impact studies and development projects in the Arctic.
   - Establishing guidelines for secure information and communication technologies (ICT) infrastructure in Arctic development initiatives.
   - Collaborating with Indigenous communities to ensure their cybersecurity concerns and interests are addressed in Arctic governance and policy-making.
4. **Engaging in Diplomatic Dialogue on Cyber Norms:** As a middle power with significant Arctic interests, Canada should actively engage in diplomatic efforts to shape international cyber norms and governance frameworks. This includes:
   - Advocating for the adoption of norms that promote responsible state behavior in cyberspace within the Arctic Council and broader international forums.
   - Supporting initiatives that strengthen cybersecurity resilience and reduce the likelihood of cyber conflict in Arctic regions.
   - Participating in multilateral dialogues to address challenges posed by state-sponsored cyber operations and strengthen international cybersecurity cooperation.
5. **Increasing Climate and Cyber Protections in NORAD:** Canada should collaborate with the United States and other NORAD members to enhance protections against climate and cyber threats. This includes:
   - Developing joint strategies and capabilities to monitor and respond to climate change impacts on continental defence infrastructure.
   - Strengthening NORAD's cybersecurity frameworks to defend against sophisticated cyber threats targeting North American defence systems.
   - Investing in advanced technologies and resilience measures to ensure continuity of operations under challenging environmental and cyber conditions.
6. **Working with Allies for Science and Technology and Protecting Those Discoveries From Allies:** Canada should forge alliances with like-minded nations to advance scientific research and technological innovations in Arctic exploration and cybersecurity. This involves:
   - Collaborating on joint research projects and sharing scientific discoveries and technological advancements for mutual benefit.

- Implementing robust mechanisms to safeguard intellectual property and sensitive information exchanged with allied countries.
- Promoting transparency and accountability in scientific and technological collaborations to mitigate risks of exploitation or misuse of shared knowledge.

7. **Addressing the Issue of the Continental Shelf:** Canada should continue to assert its sovereign rights over the continental shelf in the Arctic region through diplomatic and legal channels. This includes:
    - Strengthening scientific research and data collection to support Canada's claims to extended continental shelf areas in the Arctic Ocean.
    - Engaging in negotiations and dispute resolution processes under the United Nations Convention on the Law of the Sea (UNCLOS) to secure international recognition of Canada's extended continental shelf boundaries.
    - Promoting peaceful resolution of territorial disputes and enhancing cooperation with Arctic states to manage shared resources and protect fragile marine ecosystems.

These comprehensive policy recommendations aim to address the complex interplay of Arctic geopolitics, climate change impacts, cybersecurity challenges, and international cooperation, positioning Canada as a proactive leader in shaping resilient and sustainable Arctic and cyber policies[31].

***Claire Parsons** is a researcher with the Centre for International and Defence Policy where she works on quantum technology's effects on the defence strategies of the Five Eyes alliance and the relationship between cybersecurity and climate change. Claire holds a Master's of Arts in Political Studies with a specialization in Nationalism, Ethnicity, Peace, and Conflict from Queen's University. Her research interests pertain to military affairs, international relations, and far-right radicalization. She was also recently appointed a 2024 Capstone Laureate of the Canadian Defence and Security Network.*

***Dr. Andrew Heffernan** holds a PhD in Political Science from the University of Ottawa where he is a part-time professor specializing in International Relations and comparative politics. He is also an Associate at the Information Integrity Lab, as well as a Postdoctoral Fellow with the Digital Policy Hub at the Centre for International Governance Innovation. His major research interests include climate disinformation, African politics, global environmental governance, community-based conservation, and the politics of food.*

Endnotes

[1] Government of Canada. (2024a). “Canada and the Circumpolar Regions.” Global Affairs Canada. https://www.international.gc.ca/world-monde/international_relations-relations_internationales/arctic-arctique/index.aspx?lang=eng

[2] Government of Canada. (2024b). “Our North, Strong and Free: A Renewed Vision for Canada’s Defence.” Department of National Defence. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/north-strong-free-2024.html

[3] Government of Canada. (2019). “Canada’s Arctic and Northern Policy Framework.” Crown-Indigenous Relations and Northern Affairs Canada. https://www.rcaanc-cirnac.gc.ca/eng/1560523306861/1560523330587

[4] Dean, T. & Jean-Guy Dagenais. (2023). “Arctic Security Under Threat: Urgent Needs in a Changing Geopolitical and Environmental Landscape.” Standing Senate Committee on national Security, Defence, and Veterans Affairs. https://sencanada.ca/en/info-page/parl-44-1/secd-arctic-defence/

[5] NORAD and NORTHCOM. (2021). North American Aerospace Defense Command Executive Strategy. https://www.northcom.mil/Portals/28/(U)%20NORAD-USNORTHCOM%20Strategy%20EXSUM%20-%20Signed.pdf

[6] Young, Oran R. 2000. Arctic Politics: Conflict and Cooperation in the Circumpolar North. Dartmouth College Press. https://books.google.ca/b&lr=&id=qgedAwAAQBAJ&oi=fnd&pg=PP1&dq=arctic+as+focal+point+of+international+cooperation+and+competition&ots=GACf61FXIw&sig=DYcf_HkK_BvMRuab6ccJeI_83z4.

[7] Olsen, Martin Brochstedt. 2019. “Great Power Competition in the Arctic?” Basılmamış Yüksek Lisans Tezi, University of Aalborg. https://vbn.aau.dk/ws/files/306322660/Thesis_MartinBrochstedtOlsen_DIR.pdf.

[8] Knecht, Sebastian. 2013. “Arctic Regionalism in Theory and Practice: From Cooperation to Integration?” Arctic Yearbook 2013:4.

[9] Barry, Tom, Brynhildur Daviðsdóttir, Níels Einarsson, and Oran R. Young. 2020. “The Arctic Council: An Agent of Change?” Global Environmental Change 63:102099.

[10] Graczyk, Piotr, and Svein Vigeland Rottem. 2020. “The Arctic Council: Soft Actions, Hard Effects?” In Routledge Handbook of Arctic Security, 221–33. Routledge. https://www.taylorfrancis.com/chapters/edit/10.4324/9781315265797-19/arctic-council-piotr-graczyk-svein-vigeland-rottem.

[11] Lavelle, Kathryn C. 2024. “Regime, Climate, and Region in Transition: Russian Participation in the Arctic Council.” In Sustainable Development, Regional Governance, and International Organizations, 53–65. Routledge. https://www.taylorfrancis.com/chapters/edit/10.4324/9781003468998-5/regime-climate-region-transition-russian-participation-arctic-council-kathryn-lavelle.

[12] Tsvetkov, Valery A., Mikhail N. Dudin, and Anna A. Yuryeva. 2020. “Strategic Development of the Arctic Region in the Context of Great Challenges and Threats.” Ekonomika Regiona= Economy of Regions, no. 3, 681.

[13] Alvarez, Jimena, Dmitry Yumashev, and Gail Whiteman. 2020. “A Framework for Assessing the Economic Impacts of Arctic Change.” Ambio 49 (2): 407–18. https://doi.org/10.1007/s13280-019-01211-z.

[14] Trump, Benjamin D., Kamrul Hossain, and Igor Linkov. 2020a. Cybersecurity and Resilience in the Arctic. Vol. 58. IOS Press. https://books.google.ca/books?hl=en&lr=&id=EJP-DwAAQBAJ&oi=fnd&pg=PR1&dq=Canada%27s+risks+to+cybersecurity+in+the+arctic&ots=xL6ZAWIjSP&sig=NwKCQ9qY4aB8FG6b4vkXaBH0ohk.

[15] Thorisson, Heimir, Fabrizio Baiardi, Mirva Salminen, Rozelien Van Erdeghem, Rishikesh Sahay, Bob Paquin, Charlee Heath, Inna Skarga-Bandurova, Mathieu Branlat, and Aarne Hummelholm. 2020. “Cyber Security Challenges to Arctic Critical Infrastructures.” In Cybersecurity and Resilience in the Arctic, 60–91. ios press. https://ebooks.iospress.nl/doi/10.3233/NICSP200043.

[16] Trump, Benjamin D., Kamrul Hossain, and Igor Linkov. 2020b. “Resilience in the Arctic: Infrastructure, Cybersecurity, and Society.” In Cybersecurity and Resilience in the Arctic, 1–10. IOS Press. https://ebooks.iospress.nl/pdf/doi/10.3233/NICSP200040.

[17] Myrmel, Liv Brita Hætta, and Ove T. Gudmestad. 2021. “Cyber Security for Cities and Rural Areas in the Arctic Region.” In ISOPE International Ocean and Polar Engineering Conference, ISOPE-I. ISOPE. https://onepetro.org/ISOPEIOPEC/proceedings-abstract/ISOPE21/All-ISOPE21/464531.

[18] Rahman, Md Anisur, Yeslam Al-Saggaf, and Tanveer Zia. 2020. “A Data Mining Framework to Predict Cyber Attack for Cyber Security.” In 2020 15th IEEE Conference on Industrial Electronics and Applications (ICIEA), 207–12. IEEE. https://ieeexplore.ieee.org/abstract/document/9248225/?casa_token=oNSSjQ5WBjAAAAAA:q7d3ylCe0VgHde_Kiu0uAFjb9YGI3dKIMnn5qqulESsTVi9K6tTt6EhLT-09UlTQxK7ZeCssEEn0.

19 Lackenbauer, P. Whitney, and Alexander Sergunin. 2022. “Canada’s and Russia’s Security and Defence Strategies in the Arctic.” Arctic Review on Law and Politics 13:232–57.

20 Gorian, E. 2020. “Genesis of Russian Cyber Security Legal Mechanism: An Authentic or a Trend Alike Model?” In Proceeding of the International Science and Technology Conference “FarEastCon 2019,” edited by Denis B. Solovev, Viktor V. Savaley,

21 Heffernan, Andrew. 2024. “The Climate Policy Crisis: Governing Disinformation in the Digital Age.” Centre for International Governance Innovation. 2024. https://www.cigionline.org/publications/the-climate-policy-crisis-governing-disinformation-in-the-digital-age/.

22 Petrovskiy, Vladimir E. 2024. “A New Military and Political Landscape in the Arctic: China Perspective.” SOCIAL AND ECONOMIC DEVELOPMENT, no. 54, 60–70.

23 Schia, Niels Nagelhus, and Lars Gjesvik. 2022. China’s Cyber Sovereignty. JSTOR. https://www.jstor.org/stable/pdf/resrep07952.pdf.

24 Government of Canada. (2024c). “Construction Begins for Canada’s New Warship Fleet – the River Class Destroyers.” Department of National Defence. https://www.canada.ca/en/department-national-defence/news/2024/06/construction-begins-for-canadas-new-warship-fleet--the-river-class-destroyers.html

25 Charron, A. (2015). “Canada, the Arctic, and NORAD: status quo or new ballgame.” International Journal 70(2) http://dx.doi.org.proxy.queensu.ca/10.1177/0020702015572998

26 Government of Canada. (2023). “Risk of malicious cyber activity against Ukraine-aligned nations” (AL23-001). Canadian Centre for Climate Security. Ottawa: Canada. https://www.cyber.gc.ca/en/alerts-advisories/risk-malicious-cyber-activity-against-ukraine-aligned-nations

27 Cybersecurity and Infrastructure Security Agency. (2024a). PRC State-Sponsored Cyber Activity: Actions for Critical Infrastructure Leaders. Washington, DC: USA.

28 Government of Canada. (2023b). “Canada and the Arctic Council.” Global Affairs Canada. https://www.international.gc.ca/world-monde/international_relations-relations_internationales/arctic_council-conseil_arctique/index.aspx?lang=eng&_ga=2.68250385.1489279500.1718820893-1304675024.1702600364

29 Canadian Centre for Cyber Security. 2022. “National Cyber Threat Assessment 2023-2024”. Public Safety Canada. Ottawa: Canada. https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024

30 Anderson, Gemma. (2023). Drought and Extreme Heat Impacts to Data Centers in Northern California. (LLNL-TR-852189) California: USA.

31 Alexander T. Bekker, and Valery I. Petukhov, 172:937–49. Smart Innovation, Systems and Technologies. Singapore: Springer Singapore. https://doi.org/10.1007/978-981-15-2244-4_90.