Russian Deep-Sea Operations and Canadian Cybersecurity Issues

Date: August 30, 2018

Disclaimer: this briefing note contains summaries of open sources and does not represent the views of the Canadian Association for Security and Intelligence Studies.

Key Events

Attacks on computer networks have been traced to Russian cybercrime organizations which are alleged to be sponsored by the Russian government, moreover, it is alleged that Russia leads the world in cybercrime and is a sanctuary for the most advanced cybercriminals (Lewis, 2018).

Russia also reportedly maintains special mission submarines and surface ships dedicated to deep sea operations against sea lines of communication. These operations are coordinated by the secretive Main Directorate Deep Sea Research organization (GUGI) (Pike, 2016).

Russian threats against power grids have been linked to cybersecurity breaches of US power grid control rooms by DragonFly APT (Robinson, 2018) and GUGI capabilities (Buchanan, 2018) to disrupt computer networks and service delivery occurred in Crimea and Ukraine in 2013 (Nilsen, 2018). It is alleged the GUGI fleet surface ship *Yantar* has sailed the east coast of Canada (sometime between 2015 and present) (Nilsen, 2018).

Russian deep-sea submarines have the ability to covertly place sensors in the Arctic Ocean and along the shelf and basin at depths of 1,000 meters. This will provide Russia with the intelligence capabilities to detect and monitor Arctic Ocean submarines and sea cable signals (Sutton, 2016).

Nature of Discussion

This note explores the potential link between GUGI threats to Canadian and NATO sea lines of communication. This exploration is relevant to Canada's Arctic Sovereignty initiative.

Background

The threat to sea lines of communication has been explored during a tabletop exercise conducted by the Centre for a New American Security in 2017. That tabletop exercise considered the impact of a Russian attack on NATO sea lines of communication off the coast of Ireland. According to public sources, "participants struggled to determine whose responsibility it was to restore the cables – the grey zone between state and private ownership of sea cables was a significant hurdle for policy-makers" (Buchanan, 2018).

Melting ice and developments in technology have prompted a range of feasibility studies into the viability of a trans-Arctic sea cable route. Arctic Council permanent members Canada, Russia, the US, Norway, and Denmark have all, to varying degrees, undertaken assessments of potential Arctic data highways. To date, two Arctic routes have been touted, yet only one has made it to the development stage. The first route treks along the Northwest Passage, along Canada's Arctic coastline. This cable links data from London to Tokyo and is well into development. Dubbed "Arctic Fibre", and consisting of approximately 16,000 kilometres of cable, this route was originally a Canadian venture. In 2016 Arctic Fibre was acquired by Alaska-based firm Quintillion (Buchanan, 2018).

Key Points of Discussion and West Coast Perspectives

Canada's Renewed Arctic Sovereignty (Government of Canada, 2017) efforts include:

- New patrol ships that will be capable of sustained operation in first-year ice to ensure we can closely monitor our waters as they gradually open up and maritime activity increases.
- Expanding the size and capabilities of the Canadian Rangers, drawn primarily from indigenous communities, that provide a military presence and Canada's "eyes and ears" in remote parts of Canada.
- A new Canadian Forces Arctic Training Centre is also being established in Resolute Bay.
- Canadian Forces 2018, Operation Nanook will include collaboration with Denmark in order to increase interoperability and exercise a collective response to emerging cross-border challenges (Government of Canada, 2018).
- June 8, 2017 Defence Minister Harjit Sajjan unveiled the Liberal government's long-awaited vision for expanding the Canadian Armed Forces in Ottawa which included acknowledging NATO is paying increased attention to Russia's ability to "project force" from the Arctic and says Canada will be ready to "deter and defend," should a situation arise (Frizzell, 2017).
- Russian GUGI unit has the capability to monitor CAF deployment, interfere with underwater cables affecting Canadian telecommunications infrastructure.

What is Not Known?

How does CAF or NATO conduct monitoring of GUGI type disruption or covert monitoring? Can these be distinguished from normal disruption of sea lines of communication?

Should CAF employ Rangers in cyberwarrior model to identify Russian undersea cable threats? What does that training encompass?

What risk/threat assessments need to be conducted to ensure cybersecurity issues are addressed which result from cable cutting, and signals intelligence gathered by Russia deep submarine and surface ship activity?

References

Buchanan, E. (2018). Sea cables in a thawing Arctic. *The Interpreter* (Feb 1, 2018). Retrieved from https://www.lowyinstitute.org/the-interpreter/sea-cables-thawing-arctic

Frizzell, S. (2017). In new defence policy, Liberals turn focus on Arctic sovereignty. *CBC* (Jun 8, 2017). Retrieved from https://www.cbc.ca/news/canada/north/arctic-sovereignty-defence-policy-1.4150888

Government of Canada. (2017). *Statement on Canada's Arctic Foreign Policy: Exercising Sovereignty and Promoting Canada's Northern Strategy Abroad.* Government of Canada: Ottawa, ON. Retrieved from http://international.gc.ca/world-monde/international_relations-relations_internationales/arctic-arctique/arctic_policy-canada-politique_arctique.aspx?lang=eng

Government of Canada. (2018). Operation NANOOK. *Canadian Armed Forces.* Retrieved from http://www.forces.gc.ca/en/operations-canada-north-america-recurring/op-nanook.page

Lewis, J. (2018). A map of the most dangerous sources of cybercrime. *McAfee* (Mar 6, 2018). Retrieved from https://securingtomorrow.mcafee.com/business/map-dangerous-sources-cybercrime/

Nilsen, T. (2018). From this secret base, Russian spy ships increase activity around global data cables. *The Barents Observer* (Jan 12, 2018). Retrieved from https://thebarentsobserver.com/en/node/3381

Pike, J. (2016). Main Directorate of Deep-Sea Research (Military Unit 40056). *GlobalSecurity.org (Russia)* (Apr 18, 2016). Retrieved from https://www.globalsecurity.org/intell/world/russia/gugi.htm

Robinson, T. (2018). Russian DragonFly hackers accessed electrical utilities control rooms in lengthy campaign. *SC* (Jul 24, 2018). Retrieved from https://www.scmagazine.com/home/security-news/apts-cyberespionage/russian-dragonfly-hackers-accessed-electrical-utilities-control-rooms-in-lengthy-campaign/

Sutton, H. (2016). Analysis – Russia seeks submarine advantage in Arctic. *Covert Shores* (Sept 20, 2016). Retrieved from

www.hisutton.com/Analysis%20Russia%20seeks%20submarine%20advantage%20in%20Arctic.html

Published by the Journal of Intelligence, Conflict and Warfare and Simon Fraser University, Volume 1, Issue 2.

Available from: https://jicw.org/