TITLE GPS and NATO
Date: Nov. 10, 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

The following events have raised concerns about the impact of potentially unsecured Global Positioning Satellites which are vulnerable to cyber attacks. Event 1. Nato's Trident Juncture 2018 military exercise is the largest since the Cold War. [1] Event 2 NOTAM (Notice to Airmen) pilot announcement by Finland and Norway warning flight crews to be prepared to fly without GPS[2], and Event 3 Russian and Bulgarian military exercise *Zapad- 2017* which created GPS signal loss of Eastern Finnmark.[3]

NATURE OF DISCUSSION

The current focus on GPS navigation threats to aircraft can also apply to ship navigation systems. A GPS failure on a tanker may result in a crash and subsequent environmental oil disaster. In Canada, the "Port of Vancouver sees about 30 to 50 crude oil tankers per year, out of a total of about 3,160 vessel calls annually [into the Port of Vancouver]. With the Kinder Morgan pipeline expansion project approved, this number could increase to about 400 tankers per year, or about 11 per cent of total vessel traffic."[4] In order for these tankers to safely navigate Canadian waters, the ship's navigation officer relies upon, in part, GPS data. Canada is also actively involved in producing space satellites such as Sapphire & NEOSSat. These two satellites mark Canada's entry into military purposed satellites. These two issues, the GPS ship navigation, and military satellites may be of interest to Russia and China.

BACKGROUND

GPS provides data which supports governments, critical infrastructure, and economies[5]. Attacks against GPS can deny NATO, and commercial entities access to GPS data effectively making them blind.

---

[1] OPPDAL (2018). NATO holds its biggest exercises since the cold war. *The Economist (Nov 8th, 2018).*
[2] Nilsen, T. (2018). Pilots warned of jamming in Finnmark. *the Barents Observer (Nov 2, 2018).* Retrieved from https://thebarentsobserver.com/en/security/2018/11/pilots-warned-jamming-finnmark
[3] Nilsen, T. (2017). Norway well prepared to meet Russian jamming. *The Barents Observer (Dec 14, 2017).* Retrieved https://thebarentsobserver.com/en/node/3327
[4] Port of Vancouver (n.d.) Petroleum products and tanker safety https://www.portvancouver.com/about-us/topics-of-interest/petroleum-products-and-tanker-safety/
[5] Fidler, D. (2018) Cybersecurity and the New Era of Space Activities (Apr 03, 2018) https://www.cfr.org/report/cybersecurity-and-new-era-space-activities

According to the commander of Air Force Space Command, General John E. Hyten, told Congress in 2016 that "adversaries are developing . . . cyber tools to deny, degrade, and destroy" U.S. space capabilities that support war fighting, critical infrastructure, and economic activity. Other countries likely believe the United States is preparing to conduct cyber espionage, disruption, and attack operations against the space assets of rival states."[6]

A similar threat may exist in Canada's space satellite program. "Known as Canada's "Sentinel in the Sky", NEOSSat [Near- Earth Object Surveillance Satellite] is the world's first experimental microsatellite designed to detect and track space objects, debris and satellites. Funded and managed jointly by the Canadian Space Agency (CSA) and Defence Research and Development Canada (DRDC), NEOSSat performs multiple tasks, while carrying out two distinct missions serving the needs of the science and defence communities."[7]

A 2013 press release from the Canadian Armed Forces notes that "on May 29. The Sapphire System officially achieved its Commissioning Results Review and marked the entry into service of Canada's first dedicated operational military satellite."[8] The press release further notes that "The Sapphire satellite is able to detect and collect observations on space objects including other operational satellites, unstable or defunct satellites and other space debris."[9] Allowing for situational awareness in space and a monitoring of space assets.

KEY POINTS OF DISCUSSION AND WEST COAST PERSPECTIVES

Key Point #1 Did Canada test Sapphire for cybersecurity vulnerabilities?

Key point #2 Can you build a test image of the Sapphire operating system and conduct hacking tests?

[6] Ibid
[7] Canadian Space Agency (2018) Canadian Space Milestones http://www.asc-csa.gc.ca/eng/about/milestones.asp
[8] National Defence and the Canadian Armed forces (2013) Sapphire Satellite in space http://www.forces.gc.ca/en/news/article.page?doc=sapphire-satellite-in-space/hj9odjxf
[9] Ibid