



Royal United Services Institute of Nova Scotia Dispatches 24 December 2020

The Royal United Services Institute of Nova Scotia provides a forum for the study, promotion and debate of defence and security issues.

Dispatches is a weekly collection of links and news of current interest, included those tweeted and posted by the Institute on social media. Links to articles are checked at the time they are put into *Dispatches* but may be unavailable at a later date or in some states other than Canada.

If you are not a routine recipient of *Dispatches* but wish to be so, email the Institute's Chief Information Officer (CIO) at RUSINovaScotia@gmail.com. If you do not want to receive *Dispatches*, or wish to receive it at some different frequency, please inform the CIO. If you wish to receive *Dispatches* at a different address (i.e., not your work address), please inform the CIO. Past editions of *Dispatches* may be requested by contacting the CIO.

Everyone is encouraged to email to the CIO links and other content to be included in *Dispatches*.

Submissions and feedback are welcome anytime. Comments to articles can be from members or non-members of RUSI(NS). Any comment in *Dispatches* is the sole opinion of the author and does not necessarily represent the views of the Canadian Department of National Defence, the Canadian Armed Forces, the Royal Canadian Mounted Police or the Royal United Services Institute of Nova Scotia

RUSI(NS) also publishes:

1. a weekly Dimensions Newsletter, (formally called *Defence & Security Newsletter*) aimed at opinion leaders and industry. If you are interested in receiving this newsletter, email admin@duncom.ca; and
2. a weekly *China Open Source Newsletter* of articles curated from Chinese military-related websites based inside mainland China. If you are interested in receiving this newsletter, email RUSINovaScotia@gmail.com.

The President, Board and members of the Royal United Services Institute of Nova Scotia wish you and yours a Merry Christmas and Happy Holiday Season. Keep safe, and we look forward to getting together with you in 2021.

Picture from "Holiday traditions in the Navy"
(<https://tridentnewspaper.com/holiday-traditions-navy/>),
CFB Halifax Trident Newspaper.



Events:

To list an event in *Dispatches*, email the CIO by noon Thursday. If you have an idea for a topic or speaker, please email RUSINovaScotia@gmail.com. RUSI(NS) events may be cancelled at short notice – email RUSI(NS) if there is a question of an event occurring.

12 January, Tuesday - RCN presentation "Canadian Surface Combatants - the RIGHT ship for the Royal Canadian Navy, the RIGHT ship for Canada" by Captain(N) Christopher Nucci, Director Naval Strategy. To register, email Kray Robichaud Kray.Robichaud@forces.gc.ca – please include your full name and professional details (position/title & organization).

20 January 2021, Wednesday – RUSI(NS) Distinguished Speaker Major-General Michel-Henri St-Louis, titled "Against Daesh, and for the World Order": An Update on Operation IMPACT in the COVID-19 Era." 1300-1500, via Zoom. Call-to-meeting and invitations will be sent later. Registration will commence in the New Year.

27 January, Wednesday - RCN presentation "A portrait of an artist - Sculptor-in-Residence, Royal Canadian Navy, Mr. Christian Corbet." In 2012, Christian Corbet was named SiR for the RCN. Attendees to this virtual presentation will have access his workshop and a once-in-a-life time opportunity to learn more about the RCN SiR and the worldwide work of Christian Corbet, widely recognized as one of Canada's pre-eminent artists. Invitation to follow.

Recent Publications:

RUSI(NS) Presentation "Renewing Coast Guard's Fleet" by Derek Moss, CCG, 9 December 2020
https://rusi-ns.ca/renewing_ccg_fleet/





RUSI(NS) Information Note "Ship Sponsor," 7 December 2020
<https://rusi-ns.ca/sponsor/>

RUSI(NS) Presentations "Arctic Continental Defense: Canada and US Perspectives" by LCol Burke, JTFN, and Mr Davis, NORAD and NORTHCOM, 18 November 2020
https://rusi-ns.ca/arctic_continental_defence/

The United Services Institute of Nanaimo and North Island (USINNI) Newsletter Vol 28 No 12 December 2020 is available on request to RUSINovaScotia@gmail.com.

New: The Military Institute of Windsor Communiqué, Volume XXXIX Number 1 January 2021 is available on request to RUSINovaScotia@gmail.com.

Tweeted by @RUSI_NS: RUSI(NS) tweets may also be viewed by clicking on the icon at <https://RUSI-NS.ca>. To have something tweeted or retweeted, email the CIO at RUSINovaScotia@gmail.com. Original article title in parentheses.

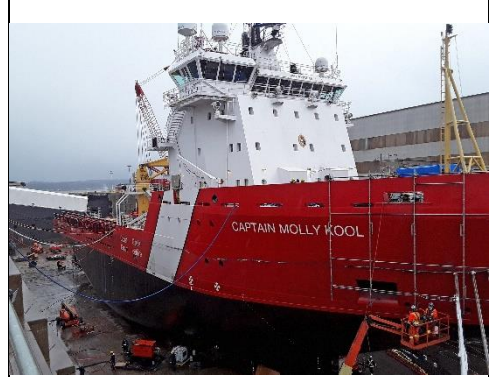
<p>Harjit Sajjan @HarjitSajjan 23 Dec tweeted: I want to congratulate Vice-Admiral Art McDonald as Canada's new Chief of the Defence Staff. He will continue to do important work to make sure that the @CanadianForces remain ready to support our government's efforts in the fight against #COVID19.</p>	
<p>Naval Association CA @navalassn 19 Dec tweeted and RUSI(NS) retweeted: Learn more about the partnership between the Royal Canadian Navy and the Canadian Coast Guard. http://ow.ly/72pI50CIUac @RoyalCanNavy @CoastGuardCAN (The Royal Canadian Navy and The Canadian Coast Guard https://www.navalassoc.ca/wp-content/uploads/2020/06/BN22-CCG-RCN-final.pdf)</p>	
<p>MARLANT @RCN_MARLANT 19 Dec tweeted: On July 31, 2020, we proudly welcomed the arrival of our first new Arctic and Offshore Patrol Ship, #HMCSHarryDeWolf, from @IrvingShipbuild to #HMCDockyardHalifax. The ship will build its operational capability as it readies for a commissioning ceremony in the summer of 2021. RUSI(NS) retweeted: Commissioning = The traditional and major public ceremony marking the entry of the ship into active service with the Navy. ("Events in a Warship's Life" https://rusi-ns.ca/events-in-a-warships-life/)</p>	
<p>Brian Santarpia @BrianSantarpia 19 Dec tweeted and RUSI(NS) retweeted: Fascinating discussion that every Canadian military member should consider. A clear argument for integrated air defence, counter UAV, and electronic warfare for operations now and future force development. The drone threat will become more ubiquitous. (Warfare and Technology https://podcasts.google.com/feed/aHR0cDovL2ZlZWRzLnNvdW5kY2xvdWQuY29tL3VzZXJzL3NvdW5kY2xvdWQ6dXNlcnM6MjMyMzY3L3NvdW5kcy5yc3M/episode/dGFnOnNvdW5kY2xvdWQsMjAxMDp0cmFja3MvOTUwMTIxNTk1?hl=en-CA&ved=2ahUKEwjIpoqGttrtAhU6GVkFHduwD4wQjrkEegQIJxAH&ep=6)</p>	

Canadian Coast Guard @CoastGuardCAN🇨🇦 21 Dec tweeted: CCGS Captain Molly Kool is back in action! It returns to service after undergoing planned maintenance refit as part of the #NationalShipbuildingStrategy.

Learn more about this ship and the rest of our fleet on our YouTube channel! <http://ow.ly/nOtX30rpyzX> @chantierdavie (Canadian Coast Guard fleet

https://www.youtube.com/playlist?list=PLt02c9yYrzqy_hyhryASrC6bv06et_Ccz)

RUSI(NS) retweeted: Derek Moss @CoastGuardCAN🇨🇦 spoke to RUSI(NS)&guests 9Dec20 with "Renewing Coast Guard's Fleet" https://rusi-ns.ca/renewing_ccg_fleet/



(Canada buys Israeli drone for Arctic maritime surveillance <https://www.rcinet.ca/eye-on-the-arctic/2020/12/22/canada-buys-israeli-drone-for-arctic-maritime-surveillance/>)

RUSI(NS) retweeted: MSOC = Marine Security Operation Centre <https://tc.canada.ca/en/marine-transportation/marine-security/marine-security-operation-centres> Multi-agency information sharing centres at Halifax, Niagara & Victoria staffed with members of CAN🇨🇦 federal departments to collaborate in identifying marine activity threats



Brian Santaripa on Twitter: "@navalassn I agree and asked the MSOC Team in Halifax that has responsibility for arctic MDA to look at how we will do exactly that."

National Defence @NationalDefence 23 Dec tweeted: Meet the first new CA made armoured combat support vehicle. These vehicles will provide the #CAF with ambulance, mobile repair or other combat support services in high threat environments. #WellEquipped

RUSI(NS) retweeted: ACSV - 360 general-utility combat support vehicles for @CanadianArmy, with wide variety of support roles including but not limited to protected command vehicle, ambulance & mobile repair team, for employment in domestic & expeditionary operations

<http://dgpaapp.forces.gc.ca/en/defence-capabilities-blueprint/project-details.asp?id=1013>



Posted on Facebook Royal United Services Institute NS with comments:

Marine Infantry Training Shifts From 'Automaton' to Thinkers, as School Adds Chess to the Curriculum

<https://news.usni.org/2020/12/15/marine-infantry-training-shifts-from-automaton-to-thinkers-as-school-adds-chess-to-the-curriculum>



Teaching people to act automatically during conflict, especially when they are tired, hungry, cold and wet, has value. Teaching people to think, independently, is a layer of value on top of that. Especially for these fast-moving, information-rich times.

And considering the global geo-strategic situation, I think military schools would do well to teach the Chinese game of Go in addition to chess...

Army long-range cannon gets direct hit on target 43 miles away

<https://www.airforcetimes.com/land/2020/12/21/army-long-range-cannon-gets-direct-hit-on-target-43-miles-away/>



The land battlefield is getting increasingly spread. Long range, precise artillery can make for challenging tactics and operations (many yet to be developed). Without such a capability (and it's more than just the guns), might the Canadian Army find itself at a disadvantage in a near peer-to-peer conflict? Will the Canadian Army acquire such a capability?

How the Army Out-Innovated the Islamic State's Drones

<https://warontherocks.com/2020/12/how-the-army-out-innovated-the-islamic-states-drones/>



"Both academics and policymakers should consider the role of experimentation, problem-solving, prototyping, diffusing knowledge and scaling up solutions in warfare. Anticipating and disrupting capabilities, even high-tech ones, is critical to building asymmetric advantages against peer competitors. On future battlefields, the Army will have to not just out-fight, but also out-think and out-innovate its enemies."

What is the Canadian Armed Forces' approach to and arrangements for innovation? We have the smart people, serving at all levels. Take advantage of them!

Russian hypersonic 'Dagger' demands rethink of North American defences, experts say

<https://www.rcinet.ca/eye-on-the-arctic/2020/12/21/russian-hypersonic-dagger-demands-rethink-of-north-american-defences-experts-say/>



A changer in the correlation of forces in the North: "... the arrival of hypersonic missiles removes the element of distance, therefore decision time, once provided by geography."

RUSI(NS) is planning a Distinguished Speaker event on NORAD and the modernization of the North Warning System, the event to be conducted spring 2021.

In Europe, US Air Force Brings Back Cold War Mobility Concept

<https://www.defenseone.com/technology/2020/12/europe-us-air-force-brings-back-cold-war-mobility-concept/171007/>



"... pivoting away from counter-terrorism to great power competition means reverting to Cold War concepts such as highly mobile command centers."

"Dispersal among several bases was standard operating procedure during the Cold War..."

"You (mitigate the risk) by improving your ability to move command centers, communication nodes, and other wing pieces to friendly bases faster."

What capability does the Canadian Armed Forces and Royal Canadian Air Force have to move command centres and other vital but vulnerable elements quickly and far?

Posted on Facebook Royal United Services Institute NS: RUSI(NS) postings may be viewed by clicking on the icon at <https://RUSI-NS.ca>. To have something posted or commented, email the CIO by noon Thursday.



2020 in Review

<https://mailchi.mp/rusi.org/rusi-2020-in-review?e=813c0cd331>



Hackers Tied to Russia Hit Nuclear Agency; Microsoft Is Exposed

<https://www.bloomberg.com/news/articles/2020-12-17/u-s-states-were-also-hacked-in-suspected-russian-attack>



Russia is developing a helicopter drone to destroy other drones

<https://www.defensenews.com/unmanned/2020/12/17/russia-is-developing-a-helicopter-drone-to-destroy-other-drones/>



Top of the line Canadian-made naval equipment shut out of \$70-billion warship program

<https://ottawacitizen.com/news/national/defence-watch/top-of-the-line-canadian-made-naval-equipment-shut-out-of-70-billion-warship-program>



Battle diary: a Canadian soldier looks back on a year commanding NATO troops in Iraq

<https://www.cbc.ca/news/SOMNIA-1.5848191>



China tails US warship as it sails through Taiwan Strait

<https://www.foxnews.com/world/china-tails-us-warship-sails-taiwan-strait>



China says aircraft carrier group on way to South China Sea for drills

<https://www.reuters.com/article/us-china-taiwan/china-says-aircraft-carrier-group-on-way-to-south-china-sea-for-drills-idUSKBN28V03C>



Japan sets record \$52 billion military budget with stealth jets, long-range missiles

<https://www.reuters.com/article/japan-defence-budget/japan-sets-record-52-billion-military-budget-with-stealth-jets-long-range-missiles-idUSKBN28V03X>



Ottawa eyeing second-hand market to replace VIP and cargo fleet

<https://www.cbc.ca/news/SOMNIA-1.5850140>



US Navy announces nuclear submarine passed through Strait of Hormuz amid tensions with Iran

<https://www.navytimes.com/news/your-navy/2020/12/21/us-navy-announces-nuclear-submarine-passage-of-strait-of-hormuz-amid-tensions-with-iran/>



Britain's Capita nabs \$1.3 billion deal for Royal Navy personnel training

<https://www.defensenews.com/global/europe/2020/12/21/britains-capita-nabs-13-billion-deal-for-royal-navy-personnel-training/>



Britain has one last contract for its Sentinel spy planes: Breaking them up

<https://www.defensenews.com/global/europe/2020/12/22/british-defense-ministry-has-one-last-contract-for-its-sentinel-spy-planes-breaking-them-up/>



Fighter jets scramble in response to Chinese, Russian aircraft, Seoul says

https://www.upi.com/Top_News/World-News/2020/12/22/Fighter-jets-scramble-in-response-to-Chinese-Russian-aircraft-Seoul-says/2721608648467/



Other Sources: Recommendations for ‘themes’ (e.g., #drones) to list in this section are welcome.

#Arctic

Melting Sea Ice Makes Canada More, Not Less Dependent on Icebreakers

<https://clearseas.org/en/blog/melting-sea-ice-makes-canada-more-not-less-dependent-on-icebreakers/>

#airpower #drones

Airpower by novel means - Drones over Nagorno-Karabakh

<https://ukdefencejournal.org.uk/airpower-by-novel-means-drones-over-nagorno-karabakh/>

#biosecurity

People's Warfare against COVID-19: Testing China's Military Medical and Defense Mobilization Capabilities

<http://www.understandingwar.org/report/peoples-warfare-against-covid-19-testing-china's-military-medical-and-defense-mobilization>

#defence industry

Exploring Australian Sovereign Capability to Scale up in Critical Times

Would be nice to read a similar Canadian analysis: <https://researchcentre.army.gov.au/library/research-reports/exploring-australian-sovereign-capability-scale-critical-times>

#drones

Countering drones: looking for the silver bullet

<https://www.nato.int/docu/review/articles/2020/12/16/countering-drones-looking-for-the-silver-bullet/index.html>

UK 'no intention' of developing lethal autonomous weapons

<https://ukdefencejournal.org.uk/uk-no-intention-of-developing-lethal-autonomous-weapons/>

#Iraq

Battle diary: a Canadian soldier looks back on a year commanding NATO troops in Iraq

<https://www.cbc.ca/news/politics/carignan-iraq-nato-1.5848191>

#NATO

China's Rise Can Unite NATO

https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/PP8-13_2020-EN.pdf

NATO agrees 2021 civil and military budgets

I wonder what Canada's share: https://www.nato.int/cps/en/natohq/news_180185.htm

#policing

Predictive Policing: Proceed, but with Care

https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/PP8-14_2020-EN.pdf

Data-Informed Predictive Policing Was Heralded As Less Biased. Is It?

<https://themarkup.org/ask-the-markup/2020/08/20/does-predictive-police-technology-contribute-to-bias>

#reading

Christmas 2020 PME Wavell Room Short Read

<https://wavellroom.com/2020/12/17/christmas-2020-pme-reading-list/>

#Royal Canadian Navy

The 3rd Canadian Women to ever Command a Canadian Naval Warship

podcast: <https://galeforcewins.com/2020/12/22/4-michele-tessier-only-the-third-woman-to-ever-command-a-canadian-naval-warship/>

#RUSI(UK)

2020-2021: The RUSI Year in Review and the Year Ahead

<https://rusi.org/rusi-news/2020-2021-rusi-year-review-and-year-ahead>

#seapower

How Good Order at Sea is Central to Winning Strategic Competition

<http://cimsec.org/how-good-order-at-sea-is-central-to-winning-strategic-competition/45247>

#strategy

Russian Military Strategy

<https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/RAD259.pdf>

#war

Reviewing The Russian Understanding of War

<https://thestrategybridge.org/the-bridge/2020/3/24/reviewing-the-russian-understanding-of-war>

#warfare

Breaking the Boom-Bust Cycle of Irregular Warfare

<https://mwi.usma.edu/breaking-the-boom-bust-cycle-of-irregular-warfare/>

Other:

The SolarWinds Hack:

According to some reports, as early as summer 2019, a software product called '**Orion**' that monitors computer networks was hacked. Malware was inserted into the process that sends updates to clients. Orion was sold as a one stop network management solution to Fortune 500 companies, U.S. Government Agencies and some UK government agencies. Reports vary however between 18,000 and 33,000 of 300,00 Orion customers have been hacked through the malware injected into the Orion updates. The company that owns Orion is a U.S. computer company called **SolarWinds**. SolarWinds is headquartered in Austin, Texas.

For more information on Orion: <https://www.solarwinds.com/solutions/orion>

Why is this important?

I quote from arstechnica: “SolarWinds by its nature has very privileged access to other parts of your infrastructure,” Chapple, a former computer scientist at the National Security Agency, said in an interview. “You can think of SolarWinds as having the master keys to your network, and if you’re able to compromise that type of tool, you’re able to use those types of keys to gain access to other parts of the network. By compromising that, you have a key basically to unlock the network infrastructure of a large number of organizations.”

Source: <https://arstechnica.com/information-technology/2020/12/18000-organizations-downloaded-backdoor-planted-by-cozy-bear-hackers/>

Who are the victims?

These are *NOT* complete lists, merely some of the best known victims.

U.S. Treasury and Commerce Departments

U.S. Department of Homeland Security

implied: FBI and Intelligence agencies linked to DHS

U.S. Department of State

U.S. National Institute of Health

FireEye (Global Computer Security Provider)

Note: We know that FireEye had a number of computer security testing and hacking tools stolen.

A number of security firms such as **GreyNoise Intelligence** were hacked as well. In the UK Orion is used by:

UK 'Home Office'

UK Ministry of Defense

Royal Navy

Royal Air Force

GCHQ

Equipment and Support Agency

UK NHS Hospitals and Hospital Trusts

UK: local city councils

For more information I recommend: <https://krebsonsecurity.com/2020/12/solarwinds-hack-could-affect-18k-customers/#more-53791>
<https://www.zdnet.com/article/microsoft-to-quarantine-solarwinds-apps-linked-to-recent-hack-starting-tomorrow/>
https://www.theregister.com/2020/12/14/solarwinds_public_sector/

Are there Canadian victims: Almost certainly.

Who Was The Attacker?

According to the Washington Post one attribution points to a Russian attacker code-named "Cozy Bear". Cozy Bear was implicated in the recent hack of the computer security company "FireEye". In plain terms, this was *probably* a Russian government attack.

Source: <https://securityaffairs.co/wordpress/112275/apt/solarwinds-supply-chain-attack.html>

What Now?

When FireEye realized they had been hacked they published related material in the computer security community. The FireEye 'hacks' are being watched and neutralized across the computer security industry.

Microsoft is working with several computer security companies to identify and neutralize command and control components of the attacks. This work was almost certainly in place before any information was provided to the media.

WARNING:

Top tier hacking organizations, and Cozy Bear is certainly a top tier hacking organization, put backup systems in place. It usually works something like this: If a primary Command and Control system is removed, a timer is started in the software. After X days (a period of time decided by the hackers) the secondary system is activated. It checks for Internet access, and then tries to 'call home' using a backup system.

The implication is that this hack is far from over.

SolarWinds Update

Background: 1. Two weeks ago 'FireEye' an American cyber security company announced that it had been hacked. Fireeye warned that advanced tools it used for Penetration Testing (Security Testing) of client networks had been stolen. FireEye published the details of the stolen tools to the computer security world in order to reduce the impact of their use - and to aid in identifying anyone using the tools. FireEye also began a forensic investigation of its network to determine how they were hacked.

Sources:

Source ThreatPost: [FireEye Cyberattack Compromises Red-Team Security Tools](#)

also

Source SecurityWeek: [FireEye Says 'Sophisticated' Hacker Stole Red Team Tools](#)

also

Source New York Times: [FireEye, a Top Cybersecurity Firm, Says It Was Hacked by a Nation-State](#)

2. FireEye discovered that they were attacked through a Software Platform they used to manage their computer networks. The Orion IT Monitoring Platform is sold internationally by a American company named SolarWinds based in Austin, Texas.

Company information: [SolarWinds](#)

Information on Orion: [Orion IT Monitoring Platform](#)

3. What makes the hack important is that the Orion IT Monitoring System "has very privileged access to other parts of your infrastructure." Chapple, a former computer scientist at the National Security Agency, said in an interview. "You can think of SolarWinds as having the master keys to your network, and if you're able to compromise that type of tool, you're able to use those types of keys to gain access to other parts of the network. By compromising that, you have a key basically to unlock the network infrastructure of a large number of organizations."

Source (arsTechnica): [~18,000 organizations downloaded backdoor planted by Cozy Bear hackers](#)

Current Situation:

4. Microsoft has announced that their systems were compromised through SolarWinds Orion platform.

Source TheStreet: [Microsoft Discovers Malware Related to SolarWinds Cyber Attack](#)

Microsoft also announced that 40 of its customers had been compromised. "The tech company said that 80% of those victims are in the US while the rest are in seven other countries: **Canada**, Mexico, Belgium, Spain, the United Kingdom, Israel and the United Arab Emirates." Further: "It is a certainty that the number and location of victims will keep growing," said Microsoft President Brad Smith, who added that the company has worked to notify the affected organizations.

Sources CNN: [Microsoft identified more than 40 organizations targeted in massive cyber breach](#)

also

thehackernews: [Microsoft Says Its Systems Were Also Breached in Massive SolarWinds Hack](#)

5. How bad can this 'hack' get? According to the UK Security publication the 'Register':

"This situation is properly scary because a supply chain attack that poisons product updates issued by a major security vendor suggests that 'Cozy Bear' (the hackers) could be deep inside of all sorts of systems and vendors. If that doesn't freak you out maybe SolarWinds' customer list will:

- More than 425 of the US Fortune 500
- All of the top 10 US telecommunications companies
- All five branches of the US military
- The US Pentagon, State Department, NASA, NSA, Postal Service, NOAA, Department of Justice, and the Office of the President of the United States
- All of the top five US accounting firms

A SolarWinds update claims 'only' 18,000 clients updated the patch containing the malware.

Source The Register: [US Treasury, Dept of Commerce hacks linked to SolarWinds IT monitoring software supply-chain attack](#)

6. Other reports indicate that the 'hack' has a wide scope. Reuters is reporting that Cox Communications, a U.S. cable company and Pima County, Arizona were hacked. A separate report says Cisco Systems was also hacked through the SolarWinds attack.

Source Reuters: [SolarWinds hackers broke into U.S. cable firm and Arizona county, web records show.](#)

also

CRN: [Cisco Hacked Through SolarWinds As Tech Casualties Mount](#)

Will This Get Worse?

Yes. Although there are aggressive efforts to neutralize the hack AND identify victims secondary victims are already being identified.

Source ThreatPost: [Sunburst's C2 Secrets Reveal Second-Stage SolarWinds Victims](#)

7. Worse, most top tier hackers have backup systems so that if their 'hack' gets compromised, the malware will wait and attempt to 'call home' at a later date. The hackers behind this attack are certainly capable of that level of engineering. The way they targeted SolarWinds and other security companies indicates a high level of sophistication.

ASSESSMENT: I assess that it is highly likely that the hackers have installed backup command and control systems in victims networks.

8. We will almost certainly never know how bad this hack got. U.S. Intelligence agencies will probably never report publicly how badly they were affected. In other jurisdictions such as Canada, many organizations don't report cyber security breaches. Editorial Comment: In Canada there is neither the political will nor the cyber security infrastructure to prosecute them.

Who Did The Hacking?

9. Neither FireEye nor SolarWinds has said who hacked them. Other cyber security organizations have looked at the mounting technical data and identified 'APT 29' also known as 'Cozy Bear' as the attacker. APT is a computer security industry abbreviation for 'Advanced Persistent Attacker'. 'Cozy Bear' is a hacker group linked to Russian Intelligence Organizations. There are disagreements as to which organization. There is agreement in the computer security industry that APT 29 works for the Russian government.

How Is This Going To Get 'Cleaned Up'?

10. Microsoft and FireEye are just two of the companies countering the hack. They are looking for the infrastructure the malware uses to communicate with 'Cozy Bear'. Those processes are being systematically blocked and shutdown. SolarWinds is responsible for the Orion platform and the mess it made. I expect there are limitation to SolarWinds liability in the contracts clients signed when they purchased Orion. Ultimately it is the responsibility of each client that uses Orion to make sure their network has been cleaned up.

11. I am not aware of any international accountability for state sponsored 'cyber-attacks'. For example Russia has attacked a number of countries, Georgia and Estonia come to mind, with no significant repercussions. I expect that the Cozy Bear hackers will be rewarded for a successful operation, moving onto other cyber tasks once data from SolarWinds has been cut off. Expect to see more state sponsored cyber attacks every bit as intrusive as the SolarWinds attack.

This cyber-intelligence product is produced by David Swan as an information service. It is copyright ©David Swan 2020. It MAY be circulated.



https://cscis.org/dt_team/12/

Australian Army Research Centre Strategic Assessment (Quarter 4, 2020)

<https://researchcentre.army.gov.au/library/other/strategic-assessment-quarter-4-2020>

Christmas

Holiday traditions in the Royal Canadian Air Force

<https://rcf-arc.forces.gc.ca/en/article-template-standard.page?doc=holiday-traditions-in-the-royal-canadian-air-force/iiedmlr>



Origins of The Soldiers Dinner

<https://www.canada.ca/en/departement-national-defence/services/military-history/history-heritage/origins-soldiers-dinner.html>



Naval Association of Canada Weekly News

<https://www.navalassoc.ca/naval-affairs/nac-news/>

2021 Navy Command and Senior Appointments

CANFORGEN 171/20 RCN 033/20 211300Z DEC 20

https://mobile.caf-fac.ca/canforgens/page.php?path=171-20_e

Commander RCN delivers Holiday Greeting and End-of-Year Update



Dear Friends of the Royal Canadian Navy,
Season's Greetings, Shipmates!

I hope this message finds you and yours well, keeping healthy, and as happy and consumed by the Season as possible in what has been an absolutely unprecedented year – a year in which we not only grappled with COVID complicating every aspect of our work and domestic lives, but also with the staggering loss of six shipmates when Stalker 22 crashed, the most significant maritime loss in decades. Denied, owing to ongoing pandemic response, the usual opportunities this year to celebrate the Season and to recount the Navy's activities with you through a series of get-togethers/kitchen-parties, I hope you'll appreciate this written expression of Season's Greetings and rapid resume of unprecedented adversity and challenge squarely met by the RCN and our extended family!

Obviously, this Season's story rightly begins with last week's uniquely bittersweet homecoming of HMCS WINNIPEG which has now returned home with honour after a deployment of some 140 days which regrettably included the tragic, heartbreaking loss of one of their own, MS Duane Earle, just days before arriving home in an incident that really stung us all. Indeed, across the naval family, we mourned as "one with the strength of many" as WINNIPEG hosted Duane's family onboard for a commemoration upon arrival. We then saluted and welcomed home WINNIE as they closed-out the deployment alongside in Esquimalt – so very proud of them for how they remained resilient, professional and yet human even when facing the most intense of challenges. They've returned home from Operation PROJECTION (Indo-Asia Pacific) and Op NEON (UNSCR enforcement off DPRK) as proven warriors, compassionate shipmates and some of Canada's best ambassadors.

And speaking of great Canadian ambassadors, as I write, only one HMC Ship remains at sea, TORONTO, which has completed NATO SNMG1 service and is expected back alongside in Halifax just in time for Christmas and the Holidays on 23 December. This return marks the first time in years that we haven't had a ship forward over the Holidays, an adjustment driven by the unusual and enormous burden that COVID places upon our sailors as individuals and as a ship's company. TORONTO returns from a 193-day Op REASSURANCE deployment – the twelfth HMC Ship to do so, all relieved in-place until this year.

These two deployments represent only the latest of a busy and successful operational year for the RCN. Facing no decrease in need for naval representation and activity at sea, the RCN – like most allied

navies – has continued to conduct operations at home and abroad in response to unrelenting demand (despite the pandemic) by keeping, ships COVID-free via appropriate protocols and procedures in ships, Dockyards and Bases, enabled by the great union-management collaboration which our Navy has made a hallmark of how we work. As a result, the year has seen us deploy 2,750 sailors for more than 800 days at sea in 15 ships (including SHAWINIGAN, GLACE BAY, SUMMERSIDE, BRANDON, SASKATOON, NANAIMO, WHITEHORSE, REGINA, CALGARY, WINNIPEG, FREDERICTON, HALIFAX, TORONTO and VILLE DE QUÉBEC, and MV ASTERIX) – all kept clean crews and delivered excellence on domestic and international operations. Our submarines, meanwhile, had their reactivation programmes slowed by COVID as maintenance routines for military, public servants and contractors were reworked and have now resulted in VICTORIA having been returned to sea off Victoria and WINDSOR in train to do the same soon on the East Coast.

Our operational successes in the COVID environment notwithstanding, there was no doubt that COVID impacted our daily routines at work and at home. This was perhaps nowhere more evident than in our celebrations and commemorations of the 75th anniversary of the end of the Battle of the Atlantic which we transitioned into a virtual activity. And, perhaps most demonstrative of our ability to succeed despite the challenge, our virtual celebrations were so poignant, reaching and effective that we saw unprecedented interest and participation – commemorating our predecessors, heroes all, appropriately!

I am so proud of the way the naval team has managed the pandemic response over the course of this past year. Since our swift response in early March, we have asymmetrically, deliberately and incrementally adapted our work environments to the evolving conditions in order to continue delivering critical support for the Government of Canada (including, for example, service in Long-Term Care Facilities in Quebec by some sailors), to continue putting ships to sea, and to advance important institutional and corporate affairs including procurement and Fleet revitalization efforts. BZ and TY to all of you who have enabled these accomplishments in such adverse conditions.

Of course, as we all know only too well, as the situation evolves in the coming months, we will continue to listen to our health experts, respect physical distancing requirements to the maximum extent possible, and take appropriate measures to provide a safe work environment from which to continue to succeed. Although it will, no doubt, remain challenging, I remain confident in your resilience and perseverance. We are operating confidently in the pandemic environment – delivering effects, executing our programme, all while making sure that you and your families are protected.

Likewise, in a Navy known not just for “what we do” but equally “how we do it” and “who we are,” we’ve been equally as busy in the sea of change in which we live. Woken by the recent, ongoing outcry against racial injustice echoing around the world, including here in Canada, we’ve had cause to reflect on our own shortcomings as an institution. What is clear is that racism, anti-Semitism, misogyny and discrimination exists within our ranks – despite the efforts of many to combat it and as much as it hurts to admit this.

For this reason and because the RCN is dedicated to being a modern and forward-looking organization in which all people are welcomed, feel safe in their workplace, and are judged solely on their competence and contribution to Canada’s defence goals, we’ve recommitted to a hateful conduct response and to having an inclusive and diverse organization. Achieving these goals is no small task. It will take a concerted effort – by each and every one of us. It will require that we help one another as we “listen, learn and act.” It will require culture change – which I have ordered. As a result, the Fall’s priority activity was the series of “culture change engagements” with our Navy’s leaders (MS thru CPO1) and (Lt(N) thru Flag) which afforded leaders at all levels with motivational testimonials, enabling discussion, and a call to arms that identified everyone as an engine for the change we seek. As we go into Christmas, more than 90% of naval leaders above the rank of MS have participated in the training serial and have become empowered, indeed responsible, to deliver our desired inclusive and diverse institution.

Recall, too, that in the summer we moved to adopt more inclusive and gender-neutral rank designations for our junior ranks. This was another important and far from symbolic incremental step in ensuring that the RCN remains a forward looking, inclusive and diverse organization.

These efforts are about nothing less than ensuring that our Navy strives to keep pace with the society we serve so as to remain exactly the Service that Canadians want to represent them in the world's darkest corners when principles and values matter.

Meanwhile, while culture change is underway as a priority activity, so too is the collective effort to progress realization of our future fleet.

We took delivery of HMCS HARRY DEWOLF, the first-of-class Arctic and Offshore Patrol Ship, at the end of July. This was a momentous occasion for the RCN and our industry partners – our Navy growing for the first time in more than two decades. The excitement continued in October when HARRY sailed under naval command for the first time. With the completion of Basic Ship Sea Readiness Training (BSSRT), what used to be called Sea-Readiness Inspections (SRIs), followed by incremental operationalization and crew proficiency training in the final months of 2020, we are well underway to seeing the ship – a great new capability for the RCN, the CAF and Canada – commissioned and fully operational in 2021.

Amongst other National Shipbuilding Strategy milestones this past year was the ceremonial keel laying of the future HMCS PROTECTEUR, one of Canada's two new Joint Support Ships. The progress in PROTECTEUR's build is now evident to all peering into Vancouver Shipyard as the ship takes shape en route to a 2024 delivery – with sister-ship PRESERVER tracking for delivery two years later.

The Canadian Surface Combatant (CSC) project also continues to be well progressed. Preliminary Design Review (PDR) has been progressed in earnest, undeterred by the pandemic and while exploiting the shipbuilding world's best practices and most amazing innovations – as we've shared via our website and as Irving Shipbuilding Inc, Lockheed Martin and BAE Systems have all shared via various products.

Of course, as our future shapes up through the parallel change efforts of culture change and new fleet realization, what will not change is the central role that families play in our success. We would not be able to achieve any of our successes in this incredibly challenging year – or indeed any year – without the unwavering love and support of our families and loved ones at home who always enable and celebrate naval successes and console in our tragedies. Thank you all for your routine sacrifices – for countless missed events and uncelebrated milestones during your sailor's absence that can never be recovered – for which the RCN/CAF, our great country and our allies are thankful! In recognition of all that you do, dear families, I hope that these Holidays afford you all the opportunity to enjoy a little of the peace on Earth that you've helped maintain through your sacrifice!

And as you try to enjoy your Holidays, Shipmates, I remind you that in this, an already stressful year, you all need be on guard against these stresses becoming exacerbated during the Holiday Season. So I ask you to look out for each other and remember that help, and mental health resources, are available if needed. We need everyone to rest, recuperate, recharge, and be healthy and ready to return to the deck plates recharged for what lies ahead in 2021.

Indeed, 2021 promises much. I am, for example, encouraged, Shipmates, by the recent vaccine roll-out and Operation VECTOR which signal that the pandemic's end is coming. It remains, meanwhile, vital that we continue our active defence against COVID's impact on what we are charged with doing, but there is a light at the end of the tunnel. In any event, the New Year will begin with HALIFAX deploying from Halifax as the Flagship to SNMG1, with CALGARY departing as the latest West Coast Indo-Asia Pacific deployer, and with future deployers progressing a myriad of pre-deployment sailings and activities. Three submarines will also sail in 2021. And, I note with great pride too, that RCN Flag Officers will also once again be honoured with international naval commands: in the Middle East, Cmdre Dan Charlebois will command Combined Task Force 150 beginning in January; and in Northern Europe, Cmdre Brad Peats will command Standing NATO Maritime Group 1 with

HALIFAX his initial Flagship. The provision of leadership concurrently in some key partner/ally naval operational formations is indicative of the professionalism of our Navy and of the high regard in which we are held in the eyes of our partners and allies. And, meanwhile, what excites me most, is the prospect of making significant progress in our culture change efforts with respect to creating an inclusive and diverse organization in which racism, anti-Semitism, misogyny, and discrimination in all of its forms are exposed and combatted whenever found. In short, I look forward to sharing the exciting year ahead with you and watching the greater RCN team continue to prosper together.

I'll conclude now by sharing that it's been my honour to be charged with your leadership in the significant year that has passed! Thank you all – the extended naval family including my shipmates, your loved ones, our incredible civilian workforce, and our industry partners across Canada – for your service, sacrifice and/or support of the RCN/CAF in the past year! This has indeed been a difficult year, but your perseverance, encouragements, and efforts are truly appreciated and delivered our many enviable successes! Bravo Zulu, Shipmates! I'm so proud of you all!

The Command Chief Petty Officer, CPO1 Dave Steeves, and I wish you all the best of health and happiness for the Holiday Season. Enjoy it! You all deserve it!

Stay healthy, safe, and ready, Shipmates. Stay Salty!

Yours Aye, With Wishes of the Season's Best

Vice-Admiral Art McDonald

Commander Royal Canadian Navy