



EDMONTON UNITED SERVICES INSTITUTE

## PRESIDENT'S ENEWS

APRIL 2023

The information in this newsletter is for informational purposes only. The Edmonton United Services assumes no liability for any inaccurate, delayed or incomplete information, nor for any actions taken in reliance thereon.

**9 April is Vimy Ridge Day**

**30 April is the deadline for filing your income tax.**

### President's Comment

Don't forget on April 1, the Federal Carbon Tax added 14 cents per litre to your fuel tank. I am glad I am living in Edmonton, where regular gas is now averaging \$1.35 per litre. My granddaughter who lives in Vancouver, told me that regular gas is about \$1.90 per litre and diesel is over \$2.00. The ripple effect is still wait to be seen. Don't even think of trying to drown your sorrow in alcohol. Most wines are up 6% and half of what you pay for beer is Federal tax. Meanwhile the Prime Minister's salary goes up \$10400 on April first and all MPs salary go up \$5200. This is not April Fool's joke, it is real. Meanwhile, a large number of soldiers have been told their housing allowance is cut and they can apply for PMQ, which has a waiting list of over 6000. And when one does obtain housing in the base, PMQ rental is comparable to local rental market. If you are posted to Toronto, Ottawa or Vancouver, be prepared to lower significantly your expectations for housing your family. Ironical isn't it? We are commemorating the sacrifices made by our forefathers in wars past, while squeezing the life out of serving soldiers.

Enough whining, the official spring season has arrived but it will be a few more weeks for all the snow to melt. I have enlarged my vegetable garden to deflate any rise in vegetable price. There is nothing comparable to munching on fresh lettuce from your own garden.

The Annual EUSI symposium was a success and the evening mess dinner was even more enjoyable. The Loyal Edmonton Regiment Band played over 30 March Pasts, including the Command March Past to recognize the presence of LGeneral (retired) Paul Wynnyk, our respected former Vice CDS. The National anthem of Ukraine was also performed to show our support for Ukraine and our soldiers deployed in Eastern Europe in support of the fight against Russian aggression.

For those who missed the morning symposium, the theme was on new approach to mitigate damages caused by natural disasters. According to the Chief of the Insurance Bureau of Canada, the payout in 2021 for insurance damages was billion of dollars. Alberta was on top of the list with \$2.1 billion in claims. Reduced property damages will definitely benefit all Canadians with reduced insurance premiums. The Shadow Minister of Defence, Mr. James Bezan, believes that Reservists could play a bigger role in aiding local disaster. He agrees that the changes in the last decade by the military to have less community engagement led to the

reduced community support, especially when recruitment is concerned. This is certainly the case in Edmonton, where the two armouries have seen many community events no longer took place in the armoury. DND policy and local red tapes played a large part why events are no longer happening in the messes.

Thanks to RAUSI, Joe Howards, Angela Craig and Nate Blackmore who provides audio/Visual tech support for the symposium, the entire presentation is available for further review. There is no cost for anyone who wants to refer to the symposium presentation in their research. The link to the video presentations for the symposium is

<https://www.youtube.com/playlist?list=PLduad7W2y-yEVzf66l2dUAAtn3N44plwq>

The EUSI remains an active organization and our web site recently recorded 1000 plus hit.

On March 7, 2023 King Charles was crowned at West Minister Abbey. His Coronation Emblem is as below. Long Life the King.



Forestburg Cenotaph

### **The Soldier by Rupert Brooke**

If I should die, think only this of me:  
That there's some corner of a foreign field  
That is for ever England. There shall be  
In that rich earth a richer dust concealed;  
A dust whom England bore, shaped, made aware,  
Gave once her flowers to love, her ways to roam;  
A body of England's, breathing English air,  
Washed by the rivers, blest by suns of home.  
And think, this heart, all evil shed away,  
A pulse in the eternal mind, no less  
Gives somewhere back the thoughts by England given;  
Her sights and sounds; dreams happy as her day;  
And laughter, learnt of friends; and gentleness,  
In hearts at peace, under an English heaven.



Get trained!



## What's Out There?

### **Type 052C (Luyang-II Class) Missile Destroyer (China)**

Based on the hull design of the Type 052B (Luyang class) multirole destroyer, the Type 052C features an indigenously developed four-array multifunction phased array radar (PAR) similar to the Aegis AN/SPY-1 equipped by the U.S. Arleigh Burke class and Japanese Kongo class DDG. The ship is also armed with the indigenous HQ-9 air defence missile system, which is believed to be comparable to the Russian S-300F/Rif in performance, and the newly developed Yingji-62 (C-602) anti-ship cruise missile (ASCM).



## **Cyber Intelligence Report**

This cyber-intelligence product is produced by David Swan. Collection of information is in accordance with guidelines provided by clients. It contains 'observations', meaning headlines and links to information published online. It MAY contain comments and analysis. It is copyright ©David Swan 2023. This report MAY be circulated. If this report does not meet your requirements, is in error or if you need additional information and/or analysis, please contact David Swan at [DSC.Ops.Vulcan@gmail.com](mailto:DSC.Ops.Vulcan@gmail.com) Cyberwarfare: Russia vs Ukraine (27) The Expanding CyberWar This report contains selected cyber-security information from 17th to 31 March 2023.

Synopsis 1. Largely ineffective against Ukraine, Russia targets Ukrainian allies doubling the number of attacks. The potential for cyber weapons to get released outside Ukraine is increasing with Russia trading cyber ware to Iran for drones and 'wiper ware' going into wider circulation.

2. Russian 'Courses of Action' for cyber forces, including allies such as 'patriotic', mercenary, and domestic criminal hackers are assessed as: Ongoing: Russian cyber forces, including allied forces, have launched a series of cyber campaigns against both Ukrainian targets and Ukrainian allies. Targeting Includes strategic and general targets as well as vulnerable governments. Analysis suggests Russian cyber attacks are increasing against Ukrainian Allies. Worst Case Scenario: President Putin decides to focus Russia's cyber attacks on one country (such as Canada) or a small group of vulnerable countries. Assessed as UNLIKELY. Best Case Scenario: Russia agrees to cease or is forced to cease offensive cyber operations. Assessed as VERY UNLIKELY. Russia

3. French defence firm Thales said Russia's cyberwar on Ukraine largely failed and Moscow is increasingly targeting Kyiv's European allies. Microsoft said in a threat assessment earlier this month that Russian actors had launched attacks in at least 17 European countries in the first six weeks of this year. Thales observed that Russia was hitting Poland, the Nordic and Baltic countries with an arsenal of cyber weapons aiming to sow divisions and promote anti-war messages. This trend probably started late in 2022. The attacks are mostly carried out by "hactivist" groups aligned with the Kremlin. Thales says that Poland, Latvia and Sweden were among the most affected countries.

4. During the past few weeks, we found few reports of Russian cyber attacks in Ukraine. There are ongoing cyber attacks, however as previously reported<sup>2</sup>, the attacks <sup>1</sup> Source: Barron's Magazine. Russia Ramps Up Cyberattacks On Ukraine Allies: Analysts 1 / 4 2023-03-30 © David Swan Consulting 2022 Cyber-Intelligence Report are increasingly espionage (data collection) oriented, as opposed to highly destructive 'wiper' attacks. These cyber attacks are not usually reported as they are not considered 'significant'. In order to verify the Thales report, and validate the change in targeting, we checked on Russian cyber attacks outside Ukraine, reported during the past two weeks. • India. Cyber-security researchers from CloudSEK reported that a Russian hacker group called 'Phoenix' compromised the Indian Health Ministry website and accessed the data of its Health Management Information System. The hackers accessed the personal information and licensing data of all employees and Chief Physicians of all hospitals in the country.<sup>3</sup> • Netherlands. The 'Play' ransomware group hit the Dutch maritime logistics company 'Royal Dirkzwager', announcing the theft of stolen private and personal confidential data, employee IDs, passports, contracts, etc. on its Tor data leak site.

5 Targets include government organizations, high profile individuals within governments and telecommunications companies.

6 Another tactic is to get targets to download fake anti-virus software.. Blackberrys security team reported 'NOBELIUM', also known as Cozy Bear, The Dukes and APT29, attributed to the Russian Foreign Intelligence Service of the Russian Federation (SVR), had created 'lures' using the Ministry of Foreign Affairs of Poland's recent visit to the U.S. The targets are EU diplomats interested in the diplomatic visit. The campaign attempts to leverage the electronic system for official document exchange in the EU called LegisWrite.

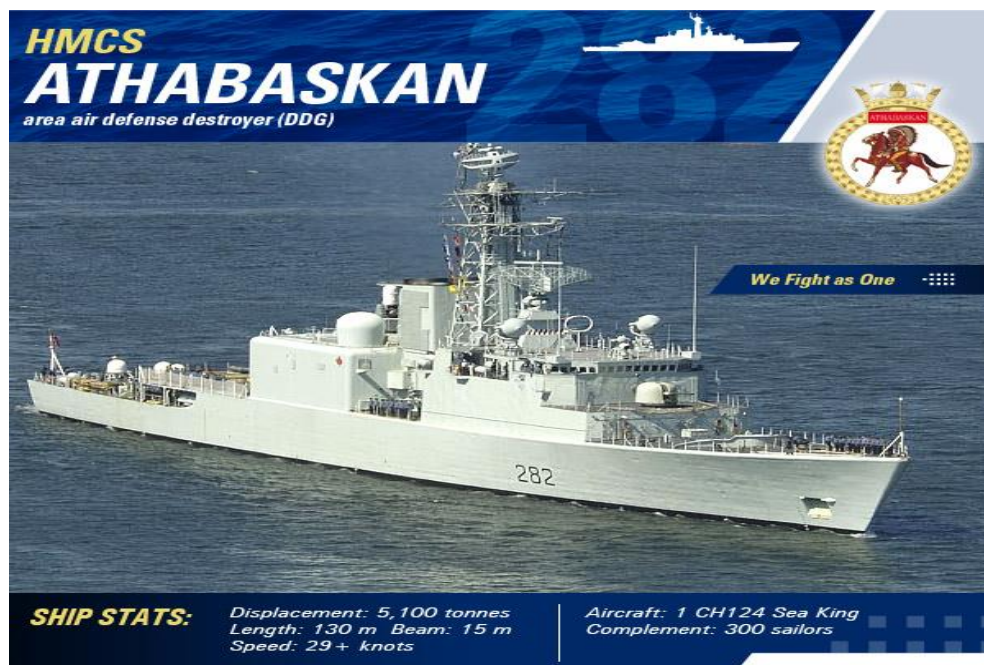
7. The French National Assembly web site was targeted and briefly shutdown by the Russian hacker group 'NoName' ransomware gang hit Dutch shipping firm Royal Dirkzwager. Hackers use fake antivirus scans to install malware. Typically, data is stolen, and web site users are inconvenienced for a few hours. NoName claim they attack entities with pro Ukraine stances. • Slovakia. Following Slovakia sending the first of its Mig-29 fighters to Ukraine, hackers from Anonymous RU sent a warning that Slovakia should not support Ukraine. This was followed by DDoS attacks on the websites of the National Council, the National Bank and the Ministry of Defence. The web sites were disabled for a number of hours. U.S. ProofPoint Software is tracking a Russian group, TA473, that is targeting elected US officials supporting Ukraine. The group is exploiting unpatched Zimbra servers to hack email accounts. The campaign, which also targets officials of European nations, uses malicious JavaScript that's customized for individual webmail portals belonging to various NATO-aligned organizations. The intention is to steal targets' usernames, passwords, and other sensitive login credentials. actions that would increase groups capabilities. The 'Wall Street Journal' has reported that Russia is supplying Iran with cyber weapons in exchange for drones. Iran's focus to date has been on internet censorship tools. Citizen Lab, a University of Toronto-based research center says Russia's PROTEI Ltd tools are part of a developing mobile-phone system that would "enable state authorities to directly monitor, intercept, redirect, degrade or deny all Iranians' mobile communications, including those who are presently challenging the regime." As Russian debt to Iran increases, there is the potential for Iran to demand top tier hacking tools and techniques. Iran has the ability to 'tool up' very quickly if they recognize the opportunity. 7. A critical battlefield capability for Ukrainian forces is the portable Starlink internet. Defense One is reporting that using the Starlink



service has become a double-edged sword. Ukrainian soldiers are reporting a variety of ways in which the Russians can locate, jam, and degrade the devices, which were never intended for battlefield use. The Russians “will find you,” the soldier said. “You need to do it fast, then get out of there.” Jamming began two to three months ago, and that its intensity varied from place to place. “In one place everything’s fine, and in another—it doesn’t work.” The end result is a MacGyver-esque arms race, as Ukraine rushes to innovate and Russia moves to overcome these innovations.



## Canadian Gear



Canadian Uniforms

## Alexander Tsang CD

Major (retired)

President

Edmonton United Services Institute

[Alexanderhtsang@hotmail.com](mailto:Alexanderhtsang@hotmail.com)



**IT IS TOO LATE TO SHARPEN SWORDS, WHEN THE DRUMS OF WAR ARE BEATING**