

**THE NAVAL  
MUSEUM OF  
MANITOBA**

**Honorary Patron:**

**The Honourable Anita  
R. Neville, P.C., O.M.**

**BOARD OF  
DIRECTORS**

Chairman & Editor:

J. Dawson

Curator:

C. Rivard

Treasurer:

C. Cassidy

Secretary:

P. Young

Board Members:

A. Sheppard

A. Smith

C. Lemoine

J. Fraser

M. Shortridge

R. Skelton

M. Weir

O. Linton

P. Bingham

P. Smith

R. Leveque

**CONTENTS**

Cover Story

- Camp X

Page 2

- Camp X (Cont'd)

Page 3

- Camp X (Cont'd)

Page 4

- Museum Log
- Naval Museum of  
Manitoba Information

**(See also:** "A Legacy in  
Stone" Brochure - "The  
Prairie Sailor Memorial"

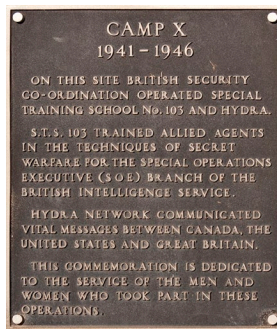
# WHEELHOUSE LOG

Our Mandate: *To Preserve, Honour and Educate.*  
Our Motto: *A Look to the Past with a View to the Future.*

FALL 2025

## Camp X

### The Past Throws Some Light on the Present



#### The Past

It was North America's first spy school – a place where aspiring assassins, saboteurs and signal interceptors learned their trade and skill sets, and how to put them to use against the Nazis. Known to the Canadian, U.S. and British governments by various names at different times, it was a place to learn the fundamentals about the dark arts of espionage and counter-espionage. It was a place to learn the secrets of "The Second Oldest Profession".

Skill sets including how to kill a targeted German; how to bomb trains and factories; how to capture radio airwaves, and mine them for intelligence value. This brings to mind the intense attempts to capture the notorious German "Enigma Machine", one of the major aims assigned to Cdr. Ian Fleming, RN (of *James Bond* fame) who was imbedded in the Dieppe Raid to achieve that very purpose.

Located on the shores of Lake Ontario near Oshawa, *Camp X* was the brainchild of a Canadian – a Winnipegger from Point Douglas, none the less – who was working for British intelligence: William Stephenson, "the man called *Intrepid*", who would later work closely with General "Wild Bill" Donovan in establishing the American OSS, which would later morph into the world

famous CIA.

Pearl Harbor exploded one day after the doors opened at *Camp X*, so it wasn't long before livid American agents flocked north to use the camp, too, because they had nothing like it at the time. Indeed, operatives from around the free world were trained at the camp before being dropped behind enemy lines in Europe to carry out their clandestine sabotage.

When the Nazis were vanquished in 1945, *Camp X* was wound down, partially because the Americans had developed and strengthened their own OSS, which as previously stated, was later to become the CIA, or major counter-intelligence and espionage service for the United States. However, *Camp X* also briefly became home and sanctuary to Igor Gouzenko, the Soviet embassy cipher clerk who defected to Ottawa as the first major Soviet intelligence defector of the new atomic age. Gouzenko disclosed intricate details of how Moscow, our former friend and ally, had become an enemy who had infiltrated security offices all across North America and Europe. Indeed, the management of the "Gouzenko Affair" became *Intrepid's* last case; but just as Gouzenko was about to divulge even more devastating disclosures than those concerning atomic espionage, the case was mysteriously terminated, and *Intrepid's* organization was dissolved. But that's a story for another day.

Today, however, what with the complexities of "cyber warfare" and the advent of an increasingly malignant application of "artificial intelligence" (AI), the world of intelligence gathering, plus the application of espionage and counter-espionage has become quantumly and quantitatively more complex and dangerous, even world-threateningly so.

*Continued on Page 2*

# Camp X: The Past Throws Some Light on the Present (Continued)

*Continued from Page 1*

Alarming, this is something that every citizen must become totally aware, as it will affect all our lives sooner or later, either directly or indirectly.

## **Today's Cyber Intelligence: Cyberwarfare and DeepSeek.**

According to David Swan's *Cyber Intelligence Report* of early 2025, the three major cyber conflicts – *Russia vs. Ukraine, Iran vs. Israel*, and *the People's Republic of China (PRC) vs. the U.S. and the West* – are the most likely sources for the creation of next generation malware, and/or a primary source for cyberattacks. This includes government funded hackers (military, intelligence and civilian employees), affiliated hackers (criminals and mercenaries), and volunteer "supporters".

## **Russia vs. Ukraine**

### **1. Russian Activity: Russia Cyber Attacks Estonia**

Estonia has reported that the number of cyberattacks against the country increased 2.5 times in 2024 above the number of attacks in 2023. Even before 2023, "Estonian government and corporate web servers hosting e-services were the primary targets of Russia's DDoS (or main internet infrastructure company) attacks." In 2024, "name servers, which help users access websites, became a key target." Data breaches doubled in 2024. The European Union (EU) is playing catch-up in identifying and sanctioning members of Russia's GRU (Main Intelligence Directorate) involved in the attacks.

### **2. EU Responds to Attacks on Estonia**

On January 28, 2025, "the European Union announced sanctions for three members (Nikolay Korchagin, Vitaly Shevchenko, and Yurly Denisov) of *Unit 29155* of Russia's military intelligence service (GRU) for their involvement in cyberattacks against Estonia in 2020. ... The state-sponsored hackers stole sensitive documents, including business secrets, health records, and other critical information compromising the security of the targeted institutions. ... Russia's GRU Unit 29155 is also responsible for attempted coups, influence operations, and assassination attempts across Europe. Since 2020, the unit has expanded into offensive cyber operations aimed at espionage, reputational harm, and data destruction. ... Additionally, the FBI assesses *Unit 29155* cyber actors rely on non-GRU actors, including known cyber-criminals and enablers to conduct their operations."

### **3. Separate Russian Hacking Team Targets EU Embassies**

Russian government hackers have been tracked as *UAC-0063* have apparently expanded their target sets. Active since 2021, they are known for attacking Ukraine and governments in Central Asia. Cyber security company *BitDefender* has identified the group as "targeting entities such as embassies in

multiple European countries, including Germany, the U.K., the Netherlands, Romania and Georgia." The group uses stolen diplomatic documents, infected with a downloader, to extract information.

### **4. New Russian Hacker Group Targets U.S. Oil and Gas**

On January 31, 2025, computer security company *Cyble* announced they had identified a new pro-Russian hacking group named *Sector 16*, which "hacked into control panels in energy facilities, and tampered with system control settings ... working with another pro-Russian group – *Z-Pentest* – which had been hacking into critical water and energy infrastructure since last year." The groups are continuing "a trend of Russian hacktivists posting videos of their members tampering with critical infrastructure control panels ... *Cyble* speculated that the videos may have been 'more to establish credibility or threaten than to inflict actual damage, although in one case *Z-Pentest* claimed to disrupt a U.S. oil well system.'"

### **5. NoName Hacks Polish Sewage**

On February 3, 2025, Russian Hacker groups *NoName 057(16)* and *Z-Pentest* hacked Polish sewage treatment plants; *Z-Pentest* claimed [this was done by] "...changing all the parameters' of its sewage treatment plants. This allegedly disrupted its operations despite the alarms going off." *NoName 057(16)* also claimed they had launched cyberattacks (probably DDoS attacks) against seventeen web sites belonging to various Polish companies.

### **6. Ukrainian Activity: Russian Telecommunications Targeted**

On January 24, 2025, it was reported that Ukrainian Intelligence hacked a major Russian telecommunications provider, *MegaFon*. According to Ukrainian intelligence sources, "other operators, including *Yota* and *NetByNet*, also experienced disruptions. The attack temporarily cut off Russians from internet resources and services such as *Steam*, *Twitch* and *Discord* – platforms widely used by the Russian military and intelligence services in their operations against Ukraine." Affected users were left without mobile phone service or internet access throughout Friday, January 24th. Ukrainian Intelligence described it as a successful 'carpet attack' (Distributed Denial of Service Attack).

### **7. Hackers Use Russian Tactics on Russian Defense Industry**

On January 27, 2025, a previously unknown threat actor was reported as cyberattacking Russian entities using "tradecraft associated with the Kremlin-aligned *Gamaredon* hacking group." According to cyber security company *Knownsec 404 Advanced Threat Intelligence* team, "The TTP (Tactics, Techniques, and Procedures) of this organization imitates that of the *Gamaredon* organization which conducts attacks against Ukraine." The attacks appear to target military facilities by

*Continued on Page 3*

# Camp X: The Past Throws Some Light on the Present

## (Continued)

*Continued from Page 2*

using an ‘email document lure’ that, when activated, allows the hacker remote access. *Knownsec* attributes the attack to a threat cluster dubbed *GamaCopy* which shares signatures with another hacking group named *Core Werewolf*.” Analyst’s Comment: This threat cluster consistently targets Russian defence organizations and individuals, including defence industry targets. More importantly, it targets information extraction, which makes it a government sponsored group, not a criminal organization.

### 8. Ukraine Disrupts Russia’s Gazprom Services

On January 29, 2025, cyber specialists from Ukraine’s Military Intelligence Agency (HUR) launched a distributed denial-of-service (DDoS) attack, severely disrupting *Gazprom*’s digital services. (Note: On this anniversary date, back in 1918, Ukrainian cadets and volunteers fought against about 5,000 Bolshevik troops intent on seizing Kyiv. Therefore, it would seem that this date was deliberately chosen.) This DDoS “attack targeted critical online systems, and as a result, customers have been unable to access accounts, process fuel payments, or use other digital services since January 28th.”

### People’s Republic of China

#### 9. PRC Hackers Target South Korean VPN Provider

On January 22, 2025, *ESET*, a cyber security company, warned that a People’s Republic of China (PRC) hacking group nicknamed *PlushDemon* hacked the installer of *Ipany*, a South Korean VPN provider. *ESET* reported “we discovered that the installer was deploying both the legitimate software and the backdoor that we’ve named *SlowStepper*.” Although *PlushDemon* has been around since 2019, and has a track record of cyberespionage in China, Taiwan, South Korea, and the U.S., in publishing its findings in its company blog, *ESET* warned that the compromised website contained no code to circulate the malicious installer to specific users based upon their geographic region or IP address: “Therefore, we believe that anyone using the *Ipany* VPN might have been a valid target.”

#### 10. DeepSeek

Following the U.S. Government announcement of *Action to Enhance AI leadership*, *DeepSeek*, an artificial intelligence (AI) start-up based in the People’s Republic of China, released its latest model called *DeepSeek R1*. *DeepSeek* claimed the model “rivalled technology developed by *ChatGPT*-maker *OpenAI* in its capabilities, while costing far less to create.” The announcement wiped “billions of dollars off the market value of chip giant *Nvidia* – and called into question whether

American firms would dominate the booming artificial intelligence (AI) market, as many assumed they would.” *Microsoft* and *Open AI* quickly announced they would investigate for a potential data breach of their work.

A. What is *DeepSeek* (the chatbot)? In general, one-way chatbots can be thought of as ‘research assistants’. When asked a question, they go to the internet and research the answer. Some chatbots have made-up answers, while others have generated answers that are either incomplete and/or lack context. *DeepSeek* is another chatbot-type research assistant that merely answers questions.

B. Can *DeepSeek* (the chatbot) do what is claimed? Yes...and No. Yes, *DeepSeek* can be asked questions, exactly like other chatbots, but it also appears to have the ability to ask for context to questions, which improves the quality of its results. No, *DeepSeek* is also uniquely a tool created inside the PRC; meaning, don’t ask it questions about ‘China’ or ‘Tiananmen Square’, or anything else that might prove embarrassing to the PRC. Analyst’s Comment: In time, other shortcomings will probably be revealed.

C. Did *DeepSeek* (the company) get cyberattacked? Yes...and No. Analyst’s Comment: It is assessed as highly likely that some pro-American/anti-PRC hackers have hit the company with DDoS attacks. Indeed, the PRC and *DeepSeek* are certain the company has been attacked. That said, it is highly unlikely that the company foresaw the onslaught of new account registration that followed the announcement of its existence. This onslaught would have produced a similar effect to a DDoS attack by overwhelming the company’s servers. The other problem was that *DeepSeek* did not secure its database infrastructure: “That means conversations with the online *DeepSeek* chatbot, and more data besides, were accessible from the public internet with no password required.” Competitors who want to know how *DeepSeek* achieved its results could access the exposed database and download a ‘wide range of information’. So, did *DeepSeek* get hacked? Mostly NO.

#### 11. Analysts’ Final Comment

It should not come as a surprise to anyone that a country that works as hard at stealing intellectual property as the PRC should be able to rapidly produce a competing product, and quite possibly beat the U.S. at its own game. Isn’t it ironic that the U.S. Senate has confirmed *Tulsi Gabbard* as its next *Intelligence Czar* (Director of National Intelligence)? Should Canada and the rest of its other *Five Eyes* allies be worried, including ‘truly patriotic Americans’ themselves? You can bet your last shrinking Canadian dollar they should! Where are the likes of *Intrepid* and *James Bond* when you truly need them?

**Editor’s Note:** “This cyber-intelligence product was originally (and primarily) produced by David Swan. It is copyright @ *David Swan Consulting* 2025. This report is *TLP: CLEAR*, and may be shared freely.”

# Museum Log

Some of what has happened at the Naval Museum of Manitoba in the past six months

The volunteers of the Naval Museum of Manitoba have been very busy since our last newsletter. They further updated the Helmsman display, discussed in the previous newsletter, adding an engine room telegraph to the display.



The First World War Medal display has also been updated so that all medals have a descriptive card. And, a newly donated Memorial Cross for OS William Stanley, RNCVR was added to the display.



Two new ship's bells were added to the Museum collection over the past six months. The bell for C.F.A.V. Riverton, a Norton Class Tugboat, and the bell for H.M.C.S. LaSalle, a River Class Frigate, were added to our collection and now reside in the Museum.



Cards with details and statistics of each of the model airplanes, in the Naval Aircraft display, were added to make the display for accessible.



A new display has been added to the Museum. It contains a Prairie Sailor statuette, a hand-painted miniature Kisbee ring for HMCS Armentieres, a handmade dagger hand-engraved with HMCS Summerside, and a handmade brass ashtray.



The medals for WRCNS who served aboard HMCS Chippawa were consolidated in the WRCNS display. Medals for SLt Agnes W. Wilkie (Nursing Sister), LCdr Edith J. Williams, CD, CPO1 Shirley Brown, CD, CPO2 Patricia Murphy, CD, and CPO2 Irene Carter, BEM, are now on display in the Museum.



Finally, the Medal display for those who have served aboard HMCS Chippawa and received medals of note was updated. Medals for Cdr William Atkinson, DSC, CD, Capt(N) Conan Frayer, OBE, Capt(N) Gordon Fahrni, DSC, CD, MD, AB Daniel Stone, DSM, Con/L/Sig Walter Walberg, BEM and CPO1 Leslie Williams, MMM, CD are now on display in the Museum.

Ready Aye Ready,  
NMM Volunteers.



**The Naval Museum of Manitoba located at**  
HMCS Chippawa 1 Navy Way Winnipeg

When is the Museum open?

Wednesday 9:00 am to 3:00 pm  
**School or Group Tours available on request.**  
Contact: Claude Rivard  
Phone (204) 9437745 Ext: 3294  
Contact can also be made through the web site  
<https://naval-museum.mb.ca/>

Was a member of your family in the Royal Canadian Navy during WWII ?

All Donations made to the Naval Museum, whether they are naval artifacts or financial donations, will receive a tax receipt for charitable purposes.

For More information call:  
Claude Rivard, Curator  
Phone: 204-943-7745 Ext: 3294