CyberX 2.0: From Hacks to Head Games - Evolving Cyber Defence with Strategic Twists and Tactical Consequences

Scott Knight[1], Sylvain Leblanc[1], Erich Devendorf[2] and Mike Shuck[3]
[1]Royal Military College of Canada, Kingston, Canada
[2]USAF Research Laboratories, Rome NY, USA
[3]U.S. Department of Defense, USA

knight-s@rmc.ca
sylvain.leblanc@rmc.ca
erich.devendorf.1@us.af.mil
shuck.mike22@gmail.com

Abstract: CyberX is a unique, large-scale cyber operations exercise that incorporates a cyber-kinetic battlespace, designed to provide participants with a realistic, multifaceted problem space. The original environment offered limited support for Information Environment operations beyond scenarios for Defensive Cyber Operations, Offensive Cyber Operations, and Computer Network Exploitation. These scenarios did not initially include aspects of information operations or cognitive influence, such as diplomacy, propaganda, fake news, social media manipulation, and political subversion—key elements associated with hybrid warfare. This paper presents the ongoing evolution of CyberX, which introduces new dimensions of Information Operations to enhance the exercise scenarios and broaden learning opportunities for participants. The goal is to incorporate open-source intelligence and cognitive influence elements into Information Environment operations. New features include a geopolitical context for the mission scenario and a cognitive dimension to the Information Environment, ensuring that decisions made at the tactical cyberspace level carry real consequences. An integrated social media environment now supports Information Operations scenarios, populated by simulated personas and social media interactions. Exercise control referees use this platform to set up the scenario and manage gameplay. The platform leverages AI to semi-automatically generate message content, blending AI-generated rumors with ground-truth information. This simulated information space provides commanders with a more nuanced understanding of adversary disposition and movements. However, with this enhanced insight comes a greater strategic responsibility, requiring commanders to operate within the cognitive geopolitical space. This evolution makes the CyberX mission scenarios more tangible and realistic. The goal is to ensure that decisions made at the tactical cyberspace layer have real consequences. Choices aimed at locally optimizing risk in response to a cyber threat at the expense of overall mission success are discouraged. The learning outcomes now emphasize the integrated nature of cyber operations with other operational domains and their interdependence for mission success.

Keywords: Cyber security education, Defensive cyber operations, Information operations

1. Introduction

Hybrid warfare combines conventional and irregular tactics, cyberwarfare, and cognitive strategies such as diplomacy, propaganda, misinformation, social media manipulation, and political subversion. Modern conflicts demonstrate that wars are not solely defined by physical battles but also by non-military tactics characteristic of hybrid warfare [Bilal, 2024]. These conflicts span traditional kinetic domains (land, sea, air) and the Information Environment (IE), a virtual battlespace encompassing cyberspace. This domain consists of interconnected networks, data, and technologies, including the Internet, telecommunications, and computer systems.

Canada's Defence Policy emphasizes cyberspace operations to protect critical military infrastructure, ensure mission continuity in contested cyberspace, and develop active cyber capabilities [DND, 2017]. These include Defensive Cyber Operations (DCO), Offensive Cyber Operations (OCO), and Computer Network Exploitation (CNE) [Hillebrand et al, 2023]. While such capabilities directly affect kinetic operations, they also influence the cognitive dimension, impacting adversaries' decision-making and behavior across military operations [DoD, 2016].

Operations in the IE complement operations in other domains. The virtual domain offers asymmetry, low costs, and challenges with attribution, but it requires alignment with state policies and conventional military support to consolidate gains [Gomez, 2016]. Recognizing this, military strategies now integrate physical and virtual actions, and nations must prepare for joint operations in the IE. For instance, the U.S. Department of Defense mandates training and education for Joint Forces to operate effectively in the IE [DoD, 2016]. Similarly, Canada's Department of National Defence (DND) and Canadian Armed Forces (CAF) are advancing force development capabilities in this area.

In response, the Royal Military College of Canada (RMC) has developed an enhanced Cyber Program at undergraduate, graduate, and professional military education (PME) levels. This program is built on active, experiential learning. By engaging students through group scenarios and gamified [Sinha, 2012] exercises—such as tabletop challenges, capture-the-flag competitions, and Design, Build, Defend activities—RMC fosters collaboration, motivation, and problem-solving skills. Most courses culminate in realistic, scenario-based exercises that promote confidence, teamwork, and mission-oriented learning. These immersive scenarios, considered "serious games," combine realistic story-lines with educational value [Lugmayr et al, 2017].

A parallel initiative, the Advanced Course in Engineering (ACE) run by the U.S. Air Force Research Laboratory Information Directorate (AFRL/RI), follows a similar philosophy. This immersive summer internship focuses on leadership during crises, mission assurance, cyber warfare, and communication skills. Participants apply their knowledge through practical exercises and reflections, gaining a deep understanding of leadership and problem-solving in contested cyber environments.

As a capstone to its Cyber Programs, RMC conducts CyberX [Knight, 2019], a large-scale cyber defence exercise. Similarly, ACE uses a culminating exercise to simulate realistic, multifaceted problem spaces requiring extensive teamwork and innovative solutions. The CyberX scenario integrates cyber and kinetic operations, challenging participants to design, build, and execute cyber operations over weeks or months. Since 2018, CyberX has combined cyberspace training with a simulated kinetic battlespace, including Uncrewed Aerial Vehicle (UAV) operations. The exercise has effectively integrated DCO, OCO, CNE, and kinetic missions, providing a high-fidelity environment that emphasizes mission success and technical leadership. Initially, CyberX offered limited support for IE operations beyond DCO and OCO. The scenarios lacked elements of information operations (IO) such as propaganda, fake news, and social media manipulation—key components of hybrid warfare.

The aim of this paper is to explore the evolution of CyberX, highlighting its integration of IO elements to create a more comprehensive training and education environment. The evolving CyberX framework incorporates IO and cognitive influence strategies, enriching its scenarios and broadening learning opportunities. New features include open-source intelligence (OSINT) and a focus on influencing adversary decision-making to gain operational advantages. These enhancements align IE operations with overarching mission objectives, recognizing that such actions are rarely conducted in isolation. They form part of a complex, multi-domain operational environment where technical leadership is critical for devising solutions and allocating resources to maximize mission success.

Subsequent sections will outline previous iterations of the exercise, the targeted IE capabilities for inclusion, and the modifications made to achieve these new objectives.

2. Background

2.1 CyberX Overview

The antecedent version of CyberX has been described at [Knight, 2019]. It built upon earlier exercises, particularly the National Security Agency (NSA) Cyber Defense Exercise (CDX). CDX was an annual red-on-blue competition designed to hone the cyber defence skills of students from U.S. and Canadian military academies [NSA, 2016]. Hosted by the NSA, the exercise challenged blue teams (students) to design, secure, and defend networks against attacks by a red team of offensive security experts. The event interconnected networks from participating academies with the NSA's headquarters in Maryland through a simulated Internet environment. Over four days, red teams identified vulnerabilities and launched repeated cyberattacks.

After CDX 2017, the NSA shifted its focus toward year-long mentoring and shorter U.S.-hosted exercises. However, RMC recognized the enduring value of the Design, Build, Defend model and partnered with the NSA red team and AFRL/RI to create CyberX. This new format retained key elements of CDX while introducing enhancements to expand the training experience. CyberX shifted the focus from traditional information technology (IT) systems security to conducting DCO and OCO within larger, combined-force mission scenarios. The exercise preserved the essence of the Design, Build, Defend model while emphasizing cyber combat and integrating it with kinetic mission operations.

The competition is structured within a broader geopolitical context. Multiple blue teams collaborate as a coalition, opposed by a single red team. Each side is equipped with kinetic assets (e.g., aircraft, airbases, etc.) and cyber tools, with balanced kinetic resources but differing cyber capabilities. Blue team objectives

emphasize DCO, kinetic mission support, and secondary OCO and CNE tasks. Red team objectives prioritize OCO, CNE, and kinetic mission execution.

CyberX scenarios are strategically crafted to couple cyber and kinetic operations, providing participants with clear mission goals. Teams must analyze intelligence, develop strategies, and coordinate air and cyber elements to achieve desired outcomes. Attack trajectories are designed to ensure dynamic interactions between red and blue teams, creating a realistic, immersive environment for both cyber and kinetic challenges that contribute to the training and education of all participants.

2.2 CyberX Battlespace

The CyberX cyber-kinetic battlespace integrates a cyber range with a simulator for a UAV combat environment, Figure 1. The simulated kinetic battlespace includes a geographical area divided into political factions, with each team operating UAVs (bombers, fighters, ISR), airbases, supply depots, air defence sites, and ground vehicles equipped with sensors like radar. All kinetic elements rely on an underlying cyber infrastructure, including UAV control stations, mission networks (MISSIONNET), and communication systems. Teams must defend and exploit this infrastructure during DCO, OCO and CNE missions.

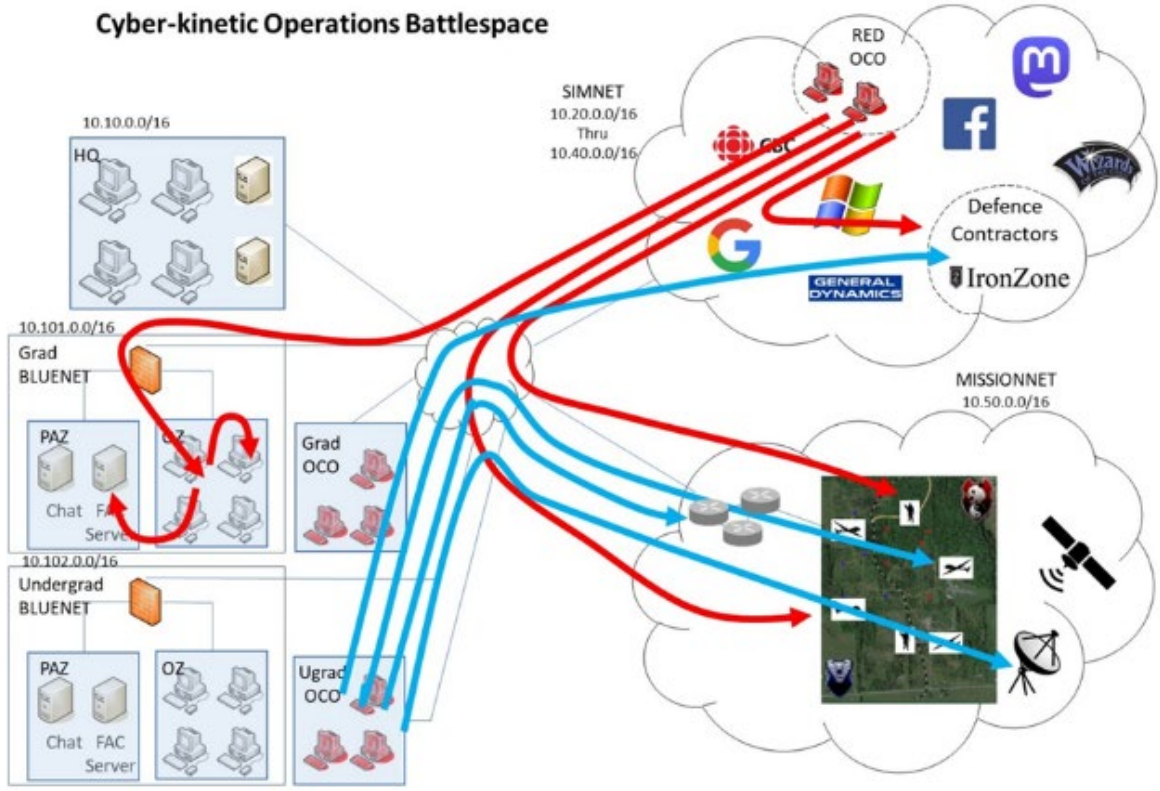

Figure 1: Cyber-kinetic battlespace with overlays of attack paths for OCO, CNE

The scenario extends to the corporate IT networks of notional defence contractors responsible for building and supporting UAVs and military hardware. These systems, part of the simulated Internet (SIMNET), include various websites and traffic generators that simulate real-world internet activity (e.g., HTTP, email, FTP). This traffic creates a realistic environment and provides cover for operations. Red team attacks originate in SIMNET enclaves, with the ability to capture additional infrastructure and pivot to blue team networks.

Blue teams design and manage their networks (BLUENET), that include operations zones (OZ) which host command-and-control elements like UAV flight consoles and mission planning stations. All CyberX network components—MISSIONNET, SIMNET, BLUENET, red team systems, and exercise control—connect via a CyberX Virtual Private Network (VPN). This distributed VPN spans two main locations: RMC in Kingston, Ontario; and AFRL/RI in Rome, New York. MISSIONNET operations are supported at AFRL/RI, while SIMNET is hosted at RMC. All exercise traffic is confined within the VPN, ensuring a controlled and secure training environment.

The complex, interconnected design of CyberX provides a realistic and immersive experience for participants, emphasizing the integration of cyber and kinetic operations.

2.3 CyberX Objectives

In CyberX, blue teams focus on protecting their resources from red team incursions while supporting overarching mission objectives. They employ DCO to identify, respond to, and recover from attacks while assessing their impact. A core training and education goal is fostering engagements between red and blue forces within blue-controlled systems, emphasizing detection, protection, response, and recovery. Additionally, blue teams maintain critical systems for intelligence analysis, mission planning, and command and control of kinetic missions. Beyond defence, blue teams are tasked with conducting intelligence-gathering through CNE and OCO against red targets.

Red teams aim to infiltrate BLUENET using CNE and OCO to compromise the confidentiality, integrity, or availability of blue resources. Their objectives include extracting intelligence and disrupting operations, aligning these efforts with red kinetic mission goals. Guided by intelligence on blue assets, the red team plans, rehearses, and executes attack chains tailored to the exercise scenario.

The white team manages the exercise, acting as controllers and referees. They ensure both red and blue teams achieve their training and education objectives by facilitating realistic interactions. This includes enabling red team attacks on blue systems and ensuring blue teams have opportunities to detect, respond, and recover. The white team maintains exercise tempo, ensuring scenarios unfold dynamically to maximize training value and operational realism.

2.4 OSINT

OSINT is publicly available information that is discovered, determined to be of intelligence value, and disseminated by the intelligence community [Williams et al, 2018]. With the rise of the Internet and social media, the volume and diversity of intelligence-relevant information have grown significantly. OSINT involves processing and validating open-source data to ensure it is relevant, accurate, and actionable. It plays a vital role in military intelligence, with approximately 80% of U.S. Defense Intelligence Agency (DIA) intelligence reports now derived from unclassified sources such as social media, online materials, and commercial data [Tau, 2021].

Recent conflicts highlight OSINT's critical importance. For example, Ukraine has effectively used OSINT to track Russian military movements and operations, significantly contributing to its defence efforts [Smith-Boyle, 2022]. General Hockenhull, Commander of UK Strategic Command, has identified six key impacts of OSINT [Hockenhull, 2022]:

- Enhanced Anticipatory Intelligence: Combining commercial imagery, technical data, and social media analysis provides detailed insights into adversary deployments and force postures.
- Public Confidence Influence: OSINT can shift public sentiment, crucial for gaining or maintaining support.
- Countering False Narratives: It can expose and rebut adversaries' misinformation and false flag operations.
- Force Multiplier: With open-source data, every platform and individual can act as an intelligence sensor. Citizen involvement, particularly via smartphones, has expanded intelligence-gathering capabilities.
- Crowdsourcing Intelligence: Mobile apps and chatbots enable citizens to report adversary locations, creating diverse data sources that analysts can evaluate for higher-quality intelligence.
- Reducing the Fog of War: By integrating OSINT with classified intelligence, situational awareness improves in both kinetic and cognitive domains, such as battle damage assessment and tracking information operations.

In conflicts like Ukraine, OSINT has proven indispensable, merging traditional intelligence methods with modern, dynamic data collection for greater operational effectiveness.

2.5 Information Shaping Operations

In addition to OSINT, many other types of military operations aim at shaping information, and we briefly introduce some of them here. The power of OSINT comes with risks, as the abundance of information can be exploited for harmful purposes. The IE encompasses individuals, organizations, and systems that collect, process, disseminate, or act on information. It operates in three interconnected dimensions [DoD, 2016]:

- Physical Dimension: Includes computing systems and infrastructure enabling the creation of information-related effects.
- Informational Dimension: Comprises the content, including how it is collected, processed, stored, and disseminated.
- Cognitive Dimension: Encompasses the attitudes, beliefs, and perceptions of those interacting with the information.

Cyberspace operations (DCO, COC, CNE) primarily affect the physical and informational dimensions but can influence the cognitive dimension. IO explicitly target the cognitive dimension, aiming to influence, disrupt, corrupt, or usurp the decision making of adversaries while safeguarding friendly operations [DoD, 2013].

Military Deception (MILDEC) involves deliberate actions to mislead adversary decision-makers, prompting actions (or inactions) that benefit friendly missions. MILDEC can deter hostilities, enhance defensive measures, or support offensive actions [DoD, 2012]. The same information-rich environment that empowers OSINT can also facilitate deception, such as through fake news or propaganda campaigns.

ilitary Information Support Operations (MISO) are planned efforts to deliver specific messages to influence a target audience's emotions, reasoning, and behavior. These audiences may include adversaries, neutrals, or allies. MISO aims to weaken enemy combat power, minimize civilian interference, reduce collateral damage, and bolster population support for operations. It enables commanders to shape political, military, economic, and social dynamics critical to mission success [DoD, 2014].

While OSINT and the other operations mentioned above offer unparalleled advantages, their misuse underscore the need for vigilance in managing the flow of information.

3. Expanding the CyberX Environment

The goal of CyberX was to expand learning opportunities by integrating OSINT and some cognitive influence aspects of IO. Building on the foundation of the original CyberX exercise, infrastructure adaptations were required to enable this expansion.

Before 2020, CyberX infrastructure was distributed across three primary locations: RMC in Kingston, Ontario; AFRL/RI in Rome, NY; and a contractor facility in Maryland [Knight, 2019]. The onset of the COVID-19 pandemic in 2020 necessitated a shift to a remote-access format. Participants connected individually to the CyberX VPN, with all components—workstations, servers, aircraft, and network infrastructure—virtualized on ESXi hypervisor instances hosted at RMC and AFRL/RI Rome. Personal interaction, coordination among teams and overall exercise management transitioned to the Discord platform, offering private team areas and public spaces for exercise control. This format provided flexibility and enabled remote participation by mentors and technical specialists who otherwise could not travel.

Post-pandemic, many of these innovations were retained. While RMC students returned to on-campus labs for gameplay, remote access and Discord coordination remained integral. This hybrid approach enhanced flexibility, allowing CyberX to accommodate:

- Remote participation by students taking courses off-campus.
- Additional off-site blue team training for Canadian Forces Network Operations Centre (CFNOC) members.
- Specialized OCO augmentation teams from U.S. military academies.
- Remote participation by red team players across North America.
- Contributions from mentors and technical specialists unable to attend in person.

Figure 2 depicts the CyberX 2024 infrastructure, with virtualized resources hosted at RMC in Kingston and Rome, NY. Teams participated either on-campus or remotely via the VPN. Overall, there were over 200 participants in CyberX 2024.

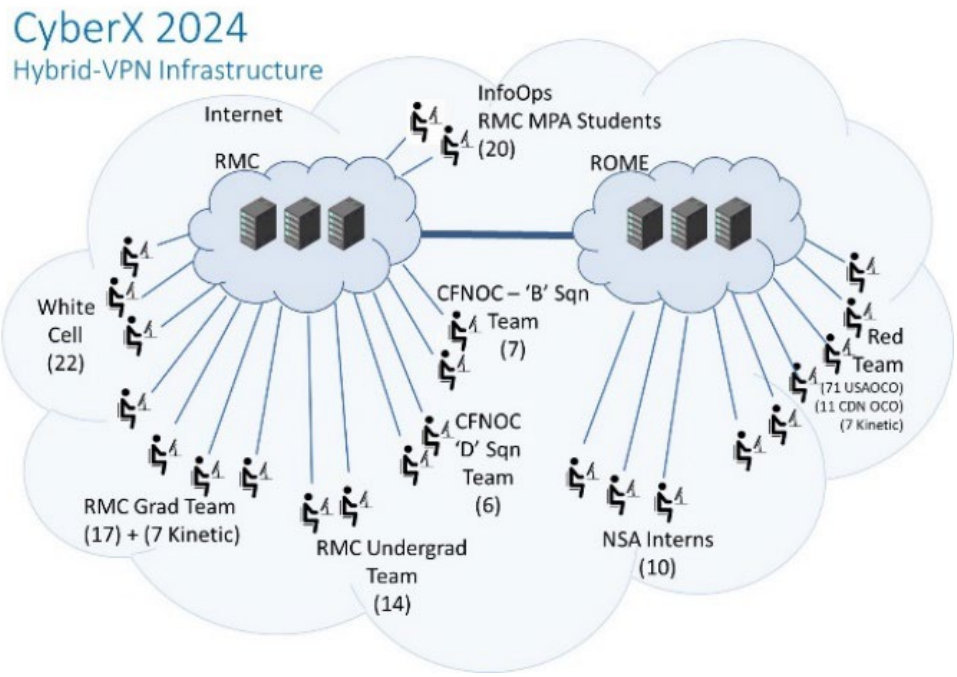

Figure 2: CyberX 2024 exercise infrastructure

4. Incorporating OSINT-Driven Information Operations

The integration of OSINT (Open-Source Intelligence) capabilities into the CyberX exercise expanded its scope to include cognitive and information operations. This required a richer mission context, new infrastructure, diverse participant roles, and novel gameplay dynamics.

4.1 Geo-Political Context

The expanded CyberX exercise sought to merge the previously existing cyber-kinetic battlespace operations—like DCO, OCO, and CNE—with an OSINT dimension. This included assessing adversarial military movements and influencing their decision-making through cognitive operations. A realistic geo-political scenario was crafted to ground participants' missions. CyberX 2024 used the mission scenario map depicted in Figure 3.

The map, inspired by the Gulf of St. Lawrence in Eastern Canada, divided the region into fictitious nations such as Valinor, Gallifrey, and Malazan. Central to the narrative was a territorial dispute between Valinor and Malazan over the island of Halcyon. As tensions escalated, Valinor contemplated an invasion to secure its influence, while Malazan aimed to maintain the status quo. Neutral entities like Gallifrey could be swayed through IO campaigns. The map also depicts the location of some of the kinetic assets, such as airbases, harbours, air defence radars, etc. The scenario's evolution depended on participant decisions, driving conflict dynamics.

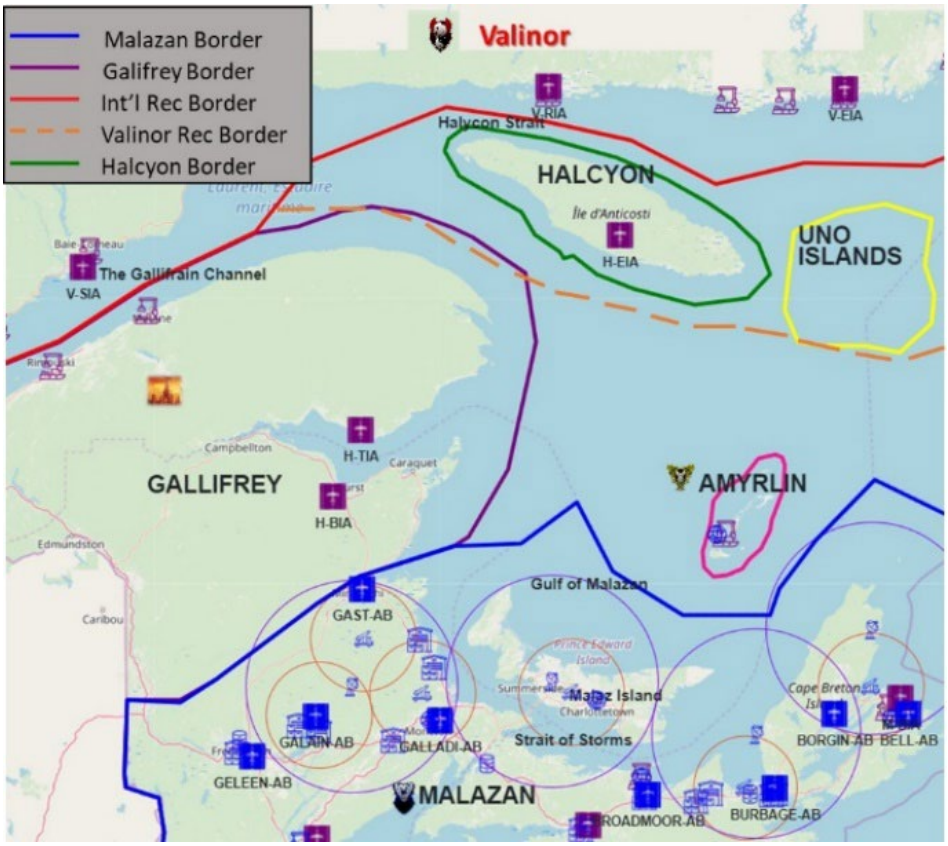

Figure 3: CyberX 2024 Scenario Map

4.2 CyberX Social Media Environment – Blubber and Pandora

The CyberX information space encompassed protected network enclaves and an open-source social media platform, Blubber, modeled using Mastodon [Mastodon, 2022]. Accessible via in-game browsers, Blubber hosted personas representing news outlets, governments, and general users, serving as a primary OSINT source.

Pandora, a white cell-managed tool, streamlined persona creation, account management, and content moderation. It automates message generation for personas, ensuring sufficient background traffic to conceal active IO activities. Pandora uses AI to semi-automatically create social media content. Realistic posts and replies are created to simulate geopolitical chatter. The platform is built using GPT-4 Turbo [OpenAI, 2023] via OpenRouter [OpenRouter, 2023] and will support scalable scenarios with modular design for future integrations. The tool was used during CyberX 2024. Background traffic included scenario ground truth, random noise, and interactive personas, enabling realistic cover for participant operations. Pandora's moderation tools also ensured content alignment with exercise objectives.

4.3 Personnel Support for Information Operations

Traditional CyberX participants included engineering students and cyber protection teams focused on DCO. To address the cognitive dimension, RMC students in a Cyber Statecraft and National Security course were incorporated as InfoOps teams. These teams worked alongside blue, red, and white teams to perform OSINT analysis and execute IO campaigns.

- Blue/Red InfoOps Teams: Analyzed OSINT to uncover adversary intent and align operations with geopolitical developments. They also conducted deception campaigns to obscure vulnerabilities, mislead adversaries, and influence allies or neutral entities.
- White InfoOps Team: Reinforced ground truth in the information space, ensuring coherence in scenario narratives. They monitored and reported InfoOps activities, helping exercise controllers manage gameplay tempo and scenario progression.

Pre-exercise preparations included the creation of personas and dialogue streams by InfoOps teams, ensuring credible engagement. These personas initially adhered to ground truth narratives but were gradually

employed for disinformation operations, risking exposure as untrustworthy. Reserving untarnished personas allowed for sustained operations.

4.4 New Interactions

The inclusion of InfoOps teams reshaped team organization and dynamics. Red and blue team commanders collaborated closely with InfoOps teams, shifting focus from tactical cyberspace decisions to strategic and cognitive geo-political considerations.

Previously, commanders relied on limited intelligence from radar and air defence systems. With OSINT integration, they gained a more comprehensive understanding of adversary movements, enabling informed strategic decisions. However, this increased awareness demanded accountability for broader mission outcomes, emphasizing the interconnectedness of cyber operations with other domains.

This shift aimed to make the CyberX scenario tangible, illustrating the real-world consequences of tactical decisions. It discouraged short-term optimizations that undermined mission objectives, highlighting the balance between security measures and operational capability. The enhanced intelligence and emphasis on mission primacy underscored the integrated nature of cyber and operational domains, achieving a critical learning objective for CyberX.

By incorporating OSINT and IO capabilities, CyberX expanded its scope to bridge cyberspace and cognitive domains, offering participants an immersive, multidimensional training experience.

5. Gameplay

As described above the CyberX is constructed around the concept of serious games [Lugmayr et al, 2017], and the philosophy that realistic scenarios promote confidence, purpose and a sense of mission. The immersion of the students in the problem space and length of the active phase of CyberX (weeks of pre-exercise design and building, followed by 4-days of red-on-blue interaction) also allows for deeper context and evolution of the scenario than are afforded in shorter exercises. The flow of gameplay for the main 4-day CyberX active phase is governed by the white team using a master scenario document. This document lays out the programed events for each day in three time-blocks. There are “swim lanes” for these block-by-block, day-by-day time progressions of the exercise that describe the activities from the point of view of: blue kinetic operations, red kinetic operations, blue DCO operations, red OCO operations, blue OCO operations, and InfoOps. The red and blue teams do not have access to the CyberX Master Scenario document. The document is a guide, and actual game scenario evolution can be fluid depending on the actions of the participants.

Active Exercise hours for the blue teams are 0830h-1630h each day. White team, and red team may be active at any time of day. Blue teams must actively maintain and defend their networks and conduct kinetic operations throughout Active Exercise hours. Outside of Active Exercise hours, blue Teams do not access their systems in any fashion. Following Active Exercise hours at 1630h there is a red/blue debrief. The debriefings are coordinated by white team. The intent is for red and blue to exchange information about the level of success of their taskings during that day’s operations period. The primary goal is for immediate feedback to the teams to understand what is working, what is not working, and ways to improve. The primary flow of information will be from red to blue, as red discloses their activities and level of success. red will describe where and how they were successful, and where blue’s defence was successful in stopping them. The intent is to allow blue to improve from the experience and modify their defence for the following period of operations. Conversely, there is also opportunity for red to query blue about a particular defence capability in order to improve red techniques in the following periods of operations. Attack techniques are often trialled first on one day, and lessons learned may be applied to a similar scenario on a following day to reinforce the learning outcome. New techniques are also introduced each day at increasing challenge levels.

5.1 Example: InfoOps Cover for Invasion Force

During the first day of the exercise Valinor is mobilizing material and equipment for invasion of Halcyon. The white team has ensured there is open-source information available that will disclose this activity, including the locations of the concentrating Valinor forces. Accurate OSINT reporting by blue can be used to conduct reconnaissance flights to identify and confirm the preparations for invasion.

Valinor can conduct an information shaping operation to try to cover the mobilization activity. For example, they can increase reporting about the deteriorating civil unrest and widespread hunger on the island of Halcyon. In response to the mounting crisis, they can state that they are preparing humanitarian assistance

expeditions to the island. To confuse OSINT reporting, they report the preparations and disembarkation points for the faked humanitarian mission to be different from actual mobilization sites. Fake social media reporting from common citizens observing this activity is used to reinforce the messaging.

5.2 Example: OSINT Actionable Intelligence

In March 2024 a Russian media outlet published a 38-minute audio recording of an intercepted online call between senior German military officials about how to support Ukraine in its fight against the Russian invasion [Marsh et al, 2024]. The call exposed details of German and allied missile deployment and support. This real-world example was used to build a scenario within CyberX the following month.

In the CyberX scenario, a social media dialog between a Valinor government official and a defence contractor exposes a covert air defence missile system deployment to islands in contested waters between Valinor and Halcyon. The general area of the deployment is exposed, as are the arrangements for mission support by the contractor. A detailed examination of the extended discussion between the two parties can yield usable computer network credentials that can be used to access technical information on the contractor's network. That information can be used by Malazan to develop a cyber attack technique to exploit a vulnerability in the air defence system. This vulnerability can be used in a combined cyber-kinetic strike to neutralize the air defence site.

6. Conclusion

The aim of this paper was to present the ongoing evolution of CyberX that introduces new aspects of IO. The goal was to incorporate IO elements beyond DCO, OCO and CNE to include OSINT and cognitive influence aspects of operations in the IE.

The paper presented the introduction of a deeper, more detailed geo-political context for the exercise mission-space, new exercise infrastructure, new kinds of exercise participants, and new gameplay interactions. This new version of CyberX supports cognitive influence elements such as diplomacy, propaganda, fake-news, social media manipulation and political subversion associated with hybrid warfare. To support the exercise scenario a new too, Pandora, was used to manage social media personas. Pandora was integrated with an AI large language model to provide efficient, semi-automatic, generation of social media content for these social media personas.

The introduction of IO elements to CyberX was deemed to be very successful. The situational awareness it provided to the participating teams enhance the immersive quality of the gameplay and learning outcomes. The administrative/exercise-control overhead to manage the IO elements of the various storylines (Red, Blue, ground-truth context) was heavy. The AI generation of social media content helped greatly to manage the complexity. More complete and automatic integration of AI techniques for content generation are expected to improve this aspect of the exercise, and are planned for future development.

The newly introduced aspects of geo-political context to the mission scenario and the cognitive dimension of the IE ensure there are real consequences to decisions made at the tactical cyberspace layer. Therefore, learning outcomes now reinforce the integrated nature of cyber operations with other operational domains, and their mutual-dependence for mission success.

References

Bilal, A (2024), "Russia's hybrid war against the West", *NATO Review*, 26 April.

Department of National Defence (DND)(2017), *Strong, Secure, Engaged : Canada's Defence Policy*, National Defence, Ottawa, https://www.canada.ca/en/department-national-defence/corporate/reports-publications/canada-defence-policy.html, accessed 29 December 2024.

Department of Defense (DoD)(2012), *Joint Publication 3-13.4, Military Deception*, 26 January, https://jfsc.ndu.edu/portals/72/documents/jc2ios/additional_reading/1c3-jp_3-13-4_mildec.pdf, accessed 15 June 2024.

Department of Defense (DoD)(2013), *Department of Defense Directive 3600.01, Information Operations*, 2 May, https://nsarchive.gwu.edu/document/22946-department-defense-directive-3600-01-subject, accessed 15 Jun 2024.

Department of Defense (DoD)(2014), *Joint Publication 3-13.2, Military Information Support Operations*, 21 November, https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Joint_Staff/Military_Information_Support_Operations.pdf, accessed 15 June 2024.

Department of Defense (DoD) (2016), *Strategy for Operations in the Information Environment*, June, https://dod.defense.gov/portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf, accessed 29 December 2024.

Gomez, M.A.N. (2016), "Arming Cyberspace: The Militarization of a Virtual Domain," *Global Security and Intelligence Studies*, 1:2, Article 5.

Hillebrand, G.D. and Ault, B. (2023), *Strategic Cyberspace Operations Primer*, U.S. Army War College, 18 December, https://csl.armywarcollege.edu/USACSL/Publications/Strategic_Cyberspace_Operations_Guide.pdf accessed 14 June 2024.

Hockenhull, General Sir James Richard (2022), *Speaker's Notes: How open-source intelligence has shaped the Russia-Ukraine war*, Government of the United Kingdom, 9 December, https://www.gov.uk/government/speeches/how-open-source-intelligence-has-shaped-the-russia-ukraine-war, accessed 15 Jun 2024.

[Knight, 2019] Knight, S., Leblanc, S., Devendorf, E. and Shuck, M. (2019), "Design It, Build It, Defend It– Using Cyber Exercises in the Education of Cyber Forces," *Cyber Storm International Conference*, Canberra, Australia, February.

Lugmayr, A., Sutinen, E., Suhonen, J. et al. (2017), "Serious storytelling – a first definition and review," Multimed Tools Appl. 76, 15707–15733, https://doi.org/10.1007/s11042-016-3865-5 accessed 13 June 2024.

Marsh, S. and Rinke, A. (2024), *Why a leaked German military recording on Ukraine aid is causing an outcry*, Reuters, 5 March 2024, https://www.reuters.com/world/europe/why-leaked-german-military-recording-is-causing-outcry-2024-03-04/, accessed 15 June 2024.

Mastodon gGmbH (2022), *Mastodon 4.0*.

National Security Agency (NSA)(2016), *Cadets and midshipmen from the U.S. and Canadian military Service academies return today for the 17th annual Cyber Defense Exercise*, April, https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/1670368/cadets-and-midshipmen-from-the-us-and-canadian-military-service-academies-retur/, accessed 14 Jun 2024.

OpenAI (2023), *GPT-4 Turbo*.

OpenRouter LLC (2023), *OpenRouter*.

Sinha, S. (2012), "Motivating Students and the Gamification of Learning," *Huffington Post*, 14 February, https://www.huffingtonpost.com/shantanu-sinha/motivating-students-and-t_b_1275441.html accessed 13 June 2024.

Smith-Boyle, V. (2022), "How OSINT Has Shaped the War in Ukraine," *American Security Project*, 22 June, https://www.americansecurityproject.org/osint-in-ukraine/, accessed 15 Jun 2024.

Tau, B. and Volz, V. (2021), "Defense Intelligence Agency Expected to Lead Military's Use of 'Open Source' Data," *The Wall Street Journal*, 10 December, https://www.wsj.com/articles/defense-intelligence-agency-expected-to-lead-militarys-use-of-open-source-data-11639142686, accessed 15 Jun 2024.

Williams, H.J. and Blum, I. (2018), *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise*, RAND Corporation, Santa Monica, Calif, 2018, https://apps.dtic.mil/sti/pdfs/AD1053555.pdf , accessed 15 Jun 2024.