OSINT Based Recognized Cyber Picture

Gergo Gyebnar

Abstract—**The Recognized Cyber Picture (RCP) is a critical NATO initiative aimed at enhancing situational awareness in the cyber domain by consolidating intelligence on cyber threats, vulnerabilities, and adversarial tactics. This study explores the feasibility of developing an RCP based on Open-Source Intelligence (OSINT), addressing the absence of publicly available implementations. Leveraging frameworks such as MITRE ATT&CK, methodologies like threat intelligence, weighted scoring model and detection as code concept. The research highlights how OSINT can complement classified data by identifying and prioritizing threats. Through targeted intelligence the study maps adversarial Tactics, Techniques, and Procedures (TTPs) to critical military operations. The findings underscore the importance of a scalable, resource-efficient RCP to counter increasingly sophisticated hybrid warfare threats effectively. The study also suggests onboarding and maintenance methodologies via cutting edge technology called Detection-as- Code.**

Index Terms—**Cybersecurity, Detection-as-Code, MITRE ATT&CK, OSINT, Recognized Cyber Picture, Situational Awareness**

I. INTRODUCTION

Military operations are increasingly characterized using hybrid warfare tactics, where cyberspace plays a crucial role as a battlefield. Hybrid warfare reflects the complexities of contemporary international relations, which have evolved into a polyarchic structure. In this system, state actors often seek to advance their interests not through conventional warfare but via hybrid methods, including cyber capabilities. [1].

The polyarchic nature of today's global order emphasizes the interconnectedness and interdependence of states, which complicates traditional notions of power and conflict. Cyberattacks exemplify this dynamic, offering states the ability to influence, disrupt, or coerce adversaries without engaging in direct military confrontation. Unlike conventional military engagements, cyber operations allow actors to obscure their involvement, leveraging state-supported hacker groups to carry out attacks. These operations often target critical infrastructure, communications, or strategic information, creating significant disruption while maintaining plausible deniability.

Such tactics blur the lines between state and non-state action, and between peace and war. The lack of clear attribution and accountability complicates international responses and raises the stakes for nations to develop robust cyber defense mechanisms. Within this context, NATO's Recognized Cyber Picture (RCP) concept gains heightened importance. As cyberspace becomes a central element of hybrid conflicts, RCP serves as a critical framework for situational awareness and coordination among member states, ensuring collective security in the face of evolving threats.

Faculty of Military Sciences and Officer Training, Ludovika University of Public Service Budapest, Hungary (E-mail: gergo.gyebnar@blackcell.io)

DOI: 10.36244/ICJ.2025.3.3

Threat actors employ increasingly sophisticated techniques, and potential attacks may target both traditional IT systems and complex military assets, including Operational Technology (OT) or Industrial Control Systems (ICS). Additionally, the RCP must be flexible enough to address the unique security and privacy needs of each member state, while still aligning with NATO's overarching cybersecurity strategy.

The RCP leverages various frameworks, such as the MITRE ATT&CK framework, to map and prioritize known threats and adversarial techniques, while also providing a structure for intelligence sharing and coordination. Using a framework approach allows NATO to classify, score, and visualize the risk landscape through methods like heatmaps, which help in setting prioritized defense actions across different operational levels.

Regarding RCPs, which primarily rely on classified data, my work is constrained to open-source intelligence (OSINT), which inherently has limitations. To enhance its effectiveness, OSINT should ideally be supplemented with signals intelligence (SIGINT), human intelligence (HUMINT), and social media intelligence (SOCMINT). Nevertheless, OSINT has demonstrated its effectiveness in this domain.

This paper aims to compile, assess, and illustrate the most used attack techniques targeting military targets in cyberspace. The resulting heatmaps presented here offer a unique visualization, though they require ongoing updates to remain effective. **This paper aims to explore this gap by examining the potential of an OSINT-based RCP and to provide military targets with wit a threat-informed defensive strategy.**

II. THEORETICAL BACKGROUND

In the evolving landscape of modern warfare, hybrid tactics—which blend conventional military strategies with unconventional and asymmetric approaches—have become a predominant mode of operation. Among these tactics, cyberspace has emerged as a critical domain for both offensive and defensive operations. Cyberattacks are increasingly leveraged to disrupt, degrade, and manipulate adversaries' critical infrastructure, command systems, and information networks, often blurring the line between peacetime cyber activities and acts of war.

A. Recognized Cyber Picture (RCP)

The RCP is NATO'sefforts to address the challenges posed by cyberspace as a battlefield. RCP seeks to create a comprehensive and near real-time view of the cyber threat environment. Its primary objective is to enhance situational awareness by consolidating intelligence on cyber activities, vulnerabilities, and adversarial actions that may impact NATO's operational capabilities. Through the RCP, NATO

aims to provide military commanders and decision-makers with actionable insights to enable swift and informed responses to cyber incidents.

Despite its importance, there is currently not publicly available Open-Source Intelligence (OSINT)-based implementation of the RCP These are confidential. This study seeks to provide initial insights and recommendations that could contribute to the development of such a system.

B. Components of the RCP

An effective RCP encompasses several critical elements. Threat intelligence aggregation to integrate intelligence to RCP to ensures a multifaceted understanding of cyber threats. Realtime monitoring and analysis that requires continuous monitoring of cyber activities provides the means to detect emerging threats, analyze attack patterns, and identify vulnerabilities to be able to create an actionable threat intel. The framework utilization where RCP leverages established frameworks, such as the MITRE ATT&CK framework, to classify, map, and prioritize adversarial techniques. Tools such as heatmaps visualize risks and guide decision-making on defense priorities. It facilitates structured intelligence sharing and operational coordination among NATO members, ensuring alignment with NATO's overarching cybersecurity strategy.

C. Challenges in Implementing the RCP

Developing and maintaining an effective RCP is a complex undertaking due to the dynamic nature of cyber threats and the diversity of NATO's member states. Key challenges include the **s**ophistication of threat actors because adversaries employ advanced techniques to target both traditional IT systems and operational technology (OT) assets used in military environments. They may also change their adversarial infrastructure and develop new TTPs. Interoperability is also a kind of challenge since member states' varied cybersecurity policies, capabilities, and legal frameworks necessitate a flexible yet cohesive approach to intelligence sharing and response coordination. The rapid pace of cyber threat evolution demands continuous updates to the RCP, requiring substantial investment in personnel, technology, and training.

D. Hypothesis

Given the increasing sophistication of hybrid warfare and the integral role of cyberspace as a modern battlefield, the development of an OSINT-based RCP can provide a viable, flexible, and scalable solution for enhancing situational awareness and decision-making capabilities. While the RCP concept has been central to NATO's cybersecurity framework, there is currently no publicly available implementation of an OSINT-based RCP. This gap presents a significant opportunity to explore how OSINT, combined with proven frameworks like the MITRE ATT&CK, can be leveraged to aggregate, analyze, and visualize cyber threats relevant to military operations.

The hypothesis is grounded in prior studies and frameworks utilized in cybersecurity, particularly in the electric sector.

The Pyramid of Pain (D. Bianco, 2013) [2] emphasizes the varying levels of effort adversaries face in cyber operations, which can inform the prioritization of intelligence in an RCP. MITRE ATT&CK Framework (The MITRE Corporation, 2022) [6] is widely recognized as a structured approach to identifying adversarial techniques, offering a foundation for mapping threats in the electric sector, such as examples of cyberattacks on power grids, including Crashoverride [3] and incidents involving APT groups like Sandworm Team [4], demonstrate the utility of structured intelligence-sharing platforms and visualization techniques for proactive threat management.

Techniques from studies like MISP [5] have demonstrated the efficacy of visualizing gaps in cyber defenses and patterns of adversarial behavior. By integrating OSINT into an RCP model, this study aims to demonstrate how OSINT can fill gapsthat arise due to resource constraints or the unavailability of classified data. It seeks to establish methods for visualizing and prioritizing threats using tools like heatmaps and the MITRE ATT&CK Navigator [6].

III. METHODOLOGY

Many cybersecurity assessment frameworks exist, but some focus more on compliance, lack objectivity, or are unmature. In contrast, the MITRE ATT&CK Framework is a widely accepted knowledge base detailing adversary tactics, techniques, and procedures (TTPs). TTPs describe adversarial behaviors, processes, actions, and workflows used to infiltrate target infrastructures. This paper will specifically examine the "Enterprise" domain within MITRE ATT&CK v16, with the Enterprise domain covering 14 tactics, 203 techniques, and 453 sub-techniques. This approach is among the most pragmatic for defending critical infrastructure today. [7]

The results highlight the critical techniques that entities should monitor, alert and respond to effectively. To accomplish this, organizations need visibility into detailed datasets. Without relevant data, effective detection is impossible.

Drawing on historical data and analysis of cyberattacks, this research aggregates actionable methods for detecting adversary Tactics, Techniques, and Procedures (TTPs).

The methodology followed a structured approach to identify and analyze incidents. Initially, incidents of interest were identified through targeted queries, followed by a deeper investigation phase that reduced irrelevant data and focused on relevant materials. Each incident was analyzed to identify specific malware, tools, and techniques used, and to extract patterns and profiles linked to adversary groups.

Using the MITRE ATT&CK framework, specific TTPs were precisely identified and mapped to tactics. MITRE ATT&CK Navigator was then used to visualize threat actor tactics and techniques across various operational domains. This tool allows for creating customized views, scoring, color-coding, and filtering to highlight critical areas for analysis and defense.

To assign priority levels, each layer in the matrix was evaluated and assigned weighted scores based on several

factors. The **Impact Score**, ranging from 1 to 5, measures the severity of a technique, from minor disruptions to life-threatening consequences. The **Evasion Score**, also on a scale of 1 to 5, assesses how effectively a technique can avoid detection mechanisms. The **Complexity Score** reflects the skill level and resources required to execute a given technique, again ranging from 1 to 5. Historical data informed the **Historical Successfulness Score**, which indicates the past effectiveness of a technique, scored on the same scale. Additionally, the **Data Accuracy Score**, a multiplier ranging from 0.5 to 1.5, adjusts the weighting to reflect the reliability of the data. The scores based on the identified threats are shown in *Table1. Scoreboard*

For visualization, a Red-Amber-Green (RAG) scoring model was employed to convey priority levels in an intuitive and easily interpretable format.

IV. Analyzed incidents, threat actors and identified tools or malware

A. Andariel

Andariel is a North Korean state-sponsored cyber threat group active since at least 2009. This group has primarily targeted South Korean government agencies, military entities, and various domestic companies, often employing destructive tactics. Notable operations attributed to Andariel include Operation Black Mine, Operation GoldenAxe, and Campaign Rifle. Andariel is regarded as a subset of the broader Lazarus Group and is linked to North Korea's Reconnaissance General Bureau. [8].

B. APT-C-23

APT-C-23 is a cyber threat group active since at least 2014, primarily targeting entities in the Middle East, including Israeli military assets. Since 2017, APT-C-23 has developed and deployed mobile spyware aimed at both Android and iOS devices, enabling extensive surveillance and data collection capabilities [8].

C. APT1

APT1 is a Chinese cyber threat group attributed to Unit 61398, a division of the 2nd Bureau within the 3rd Department of the People's Liberation Army (PLA) General Staff Department (GSD) [8].

D. APT28

APT28, a cyber threat group linked to Russia's General Staff Main Intelligence Directorate (GRU), specifically the 85th Main Special Service Center (GTsSS), military unit 26165, has been active since at least 2004. This group reportedly targeted the Hillary Clinton campaign, the Democratic National Committee (DNC), and the Democratic Congressional Campaign Committee (DCCC) in 2016 to interfere with the U.S. presidential election. Some of these activities were conducted in coordination with GRU Unit 74455, also known as the Sandworm Team [8].

E. Confucius

Confucius is a cyber espionage group active since at least 2013, primarily targeting military personnel, high-profile individuals, business figures, and government organizations across South Asia. Security researchers have observed similarities between Confucius and the threat group Patchwork, particularly in their use of custom malware code and their choice of targets [8].

F. Gallmaker

Gallmaker is a cyberespionage group active since at least December 2017, primarily targeting organizations in the Middle East. The group has focused its efforts on the defense, military, and government sectors, aiming to infiltrate and gather intelligence from these high-value targets [8].

G. Gamaredon Group

Gamaredon Group is a suspected Russian cyber espionage threat group that has been active since at least 2013, primarily targeting military, NGO, judiciary, law enforcement, and non-profit organizations in Ukraine. The group's name originates from an early campaign where the word "Armageddon" was misspelled as "Gamaredon." In November 2021, the Ukrainian government officially attributed Gamaredon Group to Center 18 of Russia's Federal Security Service (FSB) [8].

H. Ke3chang

Ke3chang is a Chinese threat group active since at least 2010, targeting entities in the oil sector, government, diplomatic, military, and NGOs. Its operations have spanned Central and South America, the Caribbean, Europe, and North America, focusing on intelligence gathering from high-value organizations across these regions [8].

I. Machete

Machete is a suspected Spanish-speaking cyber espionage group active since at least 2010. The group has primarily focused its operations on Latin America, with a particular emphasis on Venezuela, while also targeting entities in the United States, Europe, Russia, and parts of Asia. Machete typically targets high-profile organizations, including government institutions, intelligence agencies, military units, as well as telecommunications and power companies, seeking to gather sensitive information [8].

J. Magic Hound

Magic Hound is an Iranian-sponsored cyber threat group that conducts long-term, resource-intensive cyber espionage operations, likely on behalf of the Islamic Revolutionary Guard Corps (IRGC). Active since at least 2014, the group has targeted government and military personnel, academics, journalists, and organizations such as the World Health Organization (WHO) across Europe, the United States, and the Middle East. Their operations typically involve complex social engineering campaigns aimed at gaining access to sensitive information [8].

K. Mofang

Mofang is a likely China-based cyber espionage group known for its tactic of imitating a victim's infrastructure to carry out attacks. Active since at least May 2012, Mofang has conducted targeted operations against government entities and critical infrastructure in Myanmar, as well as other sectors and countries, including military, automobile, and weapons industries. The group's activities are primarily focused on intelligence gathering through sophisticated and stealthy cyber intrusions [8].

L. Naikon

Naikon is a state-sponsored cyber espionage group attributed to the Chinese People's Liberation Army's (PLA) Chengdu Military Region Second Technical Reconnaissance Bureau (Military Unit Cover Designator 78020). Active since at least 2010, Naikon has primarily targeted government, military, and civil organizations in Southeast Asia, as well as international entities such as the United Nations Development Programme (UNDP) and the Association of Southeast Asian Nations (ASEAN). While Naikon shares some similarities with APT30, the two groups are not considered identical in their tactics or operations [8].

M. Sandworm Team

Sandworm Team is a destructive cyber threat group attributed to Russia's General Staff Main Intelligence Directorate (GRU), specifically to the Main Center for Special Technologies (GTsST), military unit 74455. Active since at least 2009, Sandworm Team has carried out a series of high-profile cyber operations. In October 2020, the United States indicted six officers from GRU Unit 74455 in connection with several major attacks, including the 2015 and 2016 cyberattacks on Ukrainian electrical companies and government organizations, the global NotPetya attack in 2017, interference with the 2017 French presidential campaign, the 2018 Olympic Destroyer attack on the Winter Olympic Games, an operation against the Organisation for the Prohibition of Chemical Weapons in 2018, and attacks on Georgia in 2018 and 2019. Some of these operations were carried out in collaboration with GRU Unit 26165, also known as APT28 [13].

N. Sidewinder

Sidewinder is a suspected Indian threat actor group active since at least 2012. The group has primarily targeted government, military, and business entities across Asia, with a particular focus on Pakistan, China, Nepal, and Afghanistan. Sidewinder's operations are believed to involve cyber espionage, aimed at gathering sensitive information from these high-value targets [8].

O. The White Company

The White Company is a likely state-sponsored threat actor with advanced cyber capabilities. Between 2017 and 2018, the group conducted an espionage campaign known as Operation Shaheen, primarily targeting government and military organizations in Pakistan. The operation involved sophisticated techniques aimed at gathering intelligence from these high-value sectors [8].

P. Tonto Team

Tonto Team is a suspected Chinese state-sponsored cyber espionage group that has been active since at least 2009. Initially focused on South Korea, Japan, Taiwan, and the United States, the group expanded its operations by 2020 to include other Asian and Eastern European countries. Tonto Team has targeted a wide range of sectors, including government, military, energy, mining, financial, education, healthcare, and technology organizations. Notable operations linked to the group include the Heartbeat Campaign (2009-2012) and Operation Bitter Biscuit (2017), which involved sophisticated cyber espionage tactics [8].

Q. WIRTE

WIRTE is a threat group active since at least August 2018, known for targeting government, diplomatic, financial, military, legal, and technology organizations across the Middle East and Europe. The group is believed to conduct cyber espionage operations, focusing on high-value sectors to gather sensitive information [8].

R. Lotus Blossom

Lotus Blossom is a cyber threat group known for targeting government and military organizations across Southeast Asia. The group's operations focus on intelligence gathering, often aimed at supporting geopolitical interests in the region [9].

S. Turla

Turla is a cyber espionage threat group attributed to Russia's Federal Security Service (FSB). Active since at least 2004, Turla has compromised victims in over 50 countries, targeting a wide range of industries, including government, embassies, military, education, research, and pharmaceutical sectors. The group is known for conducting watering hole and spearphishing campaigns, and for using custom-developed tools and malware, such as Uroburos, to carry out sophisticated intelligence-gathering operations [10].

T. ToddyCat

ToddyCat is a sophisticated threat group active since at least 2020. The group employs custom loaders and malware in multi-stage infection chains, primarily targeting government and military organizations across Europe and Asia. ToddyCat is known for its advanced tactics and persistence in infiltrating high-value targets to conduct cyber espionage operations [11].

U. Agent.btz

Agent.btz is a worm that spreads primarily through removable devices, such as USB drives. It is known for having infected U.S. military networks in 2008, causing significant concerns due to its ability to propagate through unprotected systems and compromise sensitive networks [12].

V. COATHANGER

COATHANGER is a remote access tool (RAT) designed to target FortiGate networking appliances. First identified in 2023, it was used in targeted intrusions against military and government entities in the Netherlands, among other victims. The malware was publicly disclosed in early 2024, with high confidence linking it to a state-sponsored actor from the People's Republic of China. COATHANGER is typically delivered after compromising a FortiGate device, with exploitation of CVE-2022-42475 being associated with its in-the-wild use. The name "COATHANGER" comes from a unique string in the malware that is used to encrypt configuration files: "She took his coat and hung it up." [12].

W. DOGCALL

DOGCALL is a backdoor malware used by the APT37 threat group, primarily targeting South Korean government and military organizations. First observed in 2017, DOGCALL is typically deployed via an exploit in Hangul Word Processor (HWP) documents, enabling the attackers to maintain persistent access to compromised systems for cyber espionage activities [12].

X. Gootloader

Gootloader is a JavaScript-based infection framework active since at least 2020, primarily used as a delivery method for various malicious payloads, including the Gootkit banking trojan, Cobalt Strike, REvil ransomware, and others. Operating on an "Initial Access as a Service" model, Gootloader leverages SEO poisoning techniques to gain access to a wide range of entities across multiple sectors globally, including financial, military, automotive, pharmaceutical, and energy industries. This approach allows attackers to compromise organizations through malicious websites that appear in search engine results [12].

Y. Ninja

Ninja is a C++-developed malware used by the ToddyCat threat group to penetrate networks and remotely control compromised systems since at least 2020. It is believed to be part of a post-exploitation toolkit exclusively used by ToddyCat, enabling multiple operators to work simultaneously on the same machine. Ninjas have been deployed in attacks against government and military entities in Europe and Asia and have been observed in specific infection chains deployed by another group, Samurai [12].

Z. ShimRat

ShimRat is a malware used by the suspected China-based threat group Mofang in cyber campaigns targeting various sectors, including government, military, critical infrastructure, automobile, and weapons development. The malware's name, "ShimRat," comes from its extensive use of Windows Application Shimming techniques to maintain persistence on compromised systems. ShimRat is part of a broader espionage effort aimed at gathering sensitive information from high-value targets across multiple countries [12].

AA. ShimRatReporter

ShimRatReporter is a tool used by the suspected Chinese threat group Mofang to automate the initial discovery phase of cyber intrusions. The information gathered during this discovery is used to customize follow-up payloads, such as ShimRat, and to set up deceptive infrastructure that mimics the adversary's targets. ShimRatReporter has been deployed in campaigns targeting multiple countries and sectors, including government, military, critical infrastructure, automobile, and weapons development, facilitating sophisticated espionage operations [13].

BB. USBferry

USBferry is an information-stealing malware used by the threat group Tropic Trooper in targeted attacks against air-gapped military environments in Taiwan and the Philippines. While USBferry shares an overlapping codebase with another malware, YAHOYAH, it includes several distinct features that differentiate it from its counterpart. USBferry is primarily used to steal sensitive information from compromised systems, with a particular focus on military targets in highly secure, isolated networks [13].

CC. C0011

C0011 was a suspected cyber espionage campaign conducted by the threat group Transparent Tribe, which primarily targeted students at universities and colleges in India. This campaign marked a significant shift from Transparent Tribe's usual focus on Indian government, military, and think tank personnel. Security researchers noted that the C0011 campaign appeared to be ongoing as of July 2022, with the group using new tactics to compromise student networks and potentially gather intelligence [13].

DD. Operation Ghost

Operation Ghost was a cyber espionage campaign conducted by APT29, also known as the "Cozy Bear" group, beginning in 2013. The operation targeted ministries of foreign affairs in Europe as well as the Washington, D.C. embassy of a European Union country. During this campaign, APT29 employed new families of malware and utilized sophisticated techniques such as web services, steganography, and unique command-and-control (C2) infrastructure for each victim.[13].

V. SCOREBOARD

TABLE I.
SCOREBOARD

Layer	Score					
	Impact	*Evasion*	*Complexity*	*Successfulness*	*Accuracy*	*SUM*
Andariel	2	2	2	2	1	8
APT-C-23	2	3	3	3	1	11
APT 1	4	4	4	4	1	16
APT 28	4	5	5	4	1	18
Confucius	4	4	3	4	1	15
Gallmaker	3	3	3	2	1	11
Gamaredon Group	3	4	4	3	1	14
Ke3chang	4	3	4	3	1	14
Lotus Blossom	2	3	2	3	1.2	12
Machete	3	3	2	3	1	11
Magic Hound	3	4	4	4	1	15
Mofang	2	3	2	3	1	10
Naikon	4	3	3	3	1	13
Sandworm Team	5	5	5	4	1.2	22.8
Sidewinder	3	3	3	3	1	12
The White Company	3	4	2	4	1	12
ToddyCat	4	4	3	4	1.3	19.5
Tonto Team	4	4	3	3	1	14
Turla	4	5	5	5	1.4	26.6
WIRTE	3	3	2	3	1	11
Agent.btz	2	2	2	2	1	8
COATHANGER	3	2	3	4	1	12
DOGCALL	3	2	2	3	1	10
ShimRat	3	2	4	4	1	13
ShimRatReporter	3	2	3	3	1	11
USBferry	3	5	3	4	1	10
C0011	3	4	2	4	1	14
Operation Ghost	3	4	2	4	1	13

VI. HEATMAP

The analysis of military RCP has revealed a set of emerging Tactics, Techniques, and Procedures (TTPs) that adversaries increasingly leverage to compromise systems, evade detection, and maintain persistence. These TTPs span a wide range of tactics, from phishing and infrastructure acquisition to advanced scripting and exploitation techniques. Each TTP is accompanied by distinctive indicators that enable detection and mitigation, offering a roadmap a prioritized action plan for strengthening defenses against evolving cyber threats. The following breakdown highlights the most critical and actionable TTPs identified. The heatmap is shown below.

A. *Emerging Threat TTP Analysis Based on Military RCP heatmap*

1) T1566.001 – Phishing: Spearphishing Attachment: This TTP remains a cornerstone for adversarial initial access strategies. Key indicators include suspicious execution of HH.EXE, Microsoft OneNote spawning unexpected child processes, and file creations in Outlook Temp Folders. Additionally, activity involving Office macros generating files and ISO file operations in temporary directories signals potential spearphishing campaigns. Monitoring these patterns can disrupt early-stage compromises effectively.

2) T1566.002 - Phishing: Spearphishing Link: Like T1566.001, this method emphasizes adversaries leveraging links to execute payloads. Indicators overlap with suspicious HH.EXE executions but extend to HTML Help child processes, highlighting the necessity of scrutinizing link-based attachments and their follow-on behaviors.

3) T1583.001 - Acquire Infrastructure: Domains: This TTP is characterized by adversaries setting up malicious infrastructure. Observations primarily derive from Cyber Threat Intelligence (CTI) operations, as detection is complex without additional telemetry or proactive monitoring of domain registration trends.

4) T1588.002 - Obtain Capabilities: Tool: Adversaries demonstrate increasing sophistication using renamed tools, such as Sysinternals DebugView and RegistrySet utilities. These tactics allow malicious activities to blend with legitimate processes, demanding nuanced detection strategies to differentiate genuine tool usage from adversarial actions.

5) T1189 - Drive-by Compromise: Drive-by compromises often exploit user interactions with vulnerable web services. DNS rebinding attacks stand out as the primary indicator, requiring proactive monitoring of web server behaviors and DNS activity.

6) T1047 - Windows Management Instrumentation (WMI): Adversaries increasingly leverage WMI for lateral movement and persistence. Anomalies include WMIC executions, encoded scripts within WMI consumers, and unquoted service paths for reconnaissance, which warrant close inspection of WMI-related command-line activity and associated processes.

7) T1204.001/002 - User Execution (Malicious Link or File): These tactics involve the execution of malicious files or links delivered through spearphishing or drive-by techniques. Indicators include VBA DLL loading, creation of binaries or files through Office applications, and abnormal activity from user directories or temporary locations. Detecting these patterns is crucial for mitigating user-targeted exploits.

8) T1053.005 - Scheduled Task/Job: Scheduled Task: Adversaries exploit scheduled tasks for persistence or payload execution. Abnormal task creation, modification, or disabling is a key indicator, particularly when tasks are linked to PowerShell-encoded payloads or registry-based persistence attempts.

9) T1106 - Native API: Monitoring adversaries' exploitation of WinAPI calls via PowerShell or command-line interfaces is vital. This includes observing deviations in expected script behavior or unusual API access attempts.

10) T1203 - Exploitation for Client Execution: This TTP highlights client-side vulnerabilities exploited via malicious documents or scripts. Detection focuses on sub-process activities and network connections initiated by Excel or similar applications, signaling potential exploitation.

11) T1059.003 - Command and Scripting Interpreter: Windows Command Shell: Adversaries use the Windows command shell for malicious execution. Notable patterns include path traversal anomalies and commands embedding suspicious URLs, often targeting AppData or temporary directories.

12) T1059.005 - Command and Scripting Interpreter: Visual Basic: Indicators focus on WScript or CScript droppers and unexpected parent processes for Csc.exe, emphasizing the importance of monitoring Visual Basic-based execution paths.

13) T1059.001 - Command and Scripting Interpreter: PowerShell: PowerShell remains a favored tool for adversaries due to its flexibility and obfuscation capabilities. Detection includes encoded commands, reverse shell activity, and obfuscated script patterns designed to evade traditional defenses.

14) T1505.003 - Server Software Component: Web Shell: Web shells are deployed to maintain persistent access. Suspicious ASPX file drops, SQL server anomalies, and webshell reconnaissance activities highlight the need for vigilant monitoring of server and database operations.

15) T1547.001 - Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder: Registry and startup folder abuse enable adversaries to maintain persistence. Indicators include modifications to user shell folders, registry run key entries, and PowerShell-based startup shortcuts.

16) T1027 - Obfuscated Files or Information: Adversaries commonly obfuscate payloads to avoid detection. This includes Base64 encoding, renamed executables, and misuse of utilities like Certutil to download and encode files.

17) T1036.005 - Masquerading: Match Legitimate Name or Location: Masquerading involves using legitimate-looking names or locations for malicious files or processes. Indicators include system process names in unusual locations and misused execution paths.

18) T1070.004 - Indicator Removal: File Deletion: File deletion patterns associated with malicious activity include Prefetch file deletion and combinations of ping/del commands, suggesting attempts to erase evidence post-operation.

19) T1140 - Deobfuscate/Decode Files or Information: Decoding tools such as Certutil and MSHTA are leveraged for obfuscation reversal. These activities often precede more overt malicious execution.

20) T1003.001 - OS Credential Dumping: LSASS Memory: Credential dumping from LSASS memory is a persistent threat, with indicators such as Dump64.exe execution and memory extraction via Comsvcs.DLL.

21) T1056.001 - Input Capture: Keylogging: PowerShell-based keylogging tactics target sensitive input data. Monitoring unusual scripting behaviors can aid in early detection *[17].*

VII. DETECTION AS CODE

The Detection as Code (DaC) fundamentally transforms the processes on the defensive side. It offers numerous advantages over traditional, outdated rule-management methods, the most important of which are detailed in the following subsections. DaC is a transformative approach that enables automated, version-controlled detection rules tailored specifically for Military RCP**.** The primary goal is to facilitate quick adaptation to new threats and seamless integration with security tooling. This approach leverages version control (e.g., using Git) to manage detection rules and configurations, allowing teams to track changes and collaborate on detection development.

Automated processes accelerate the creation, testing, and deployment of rules, enabling faster responses to new threats. Equipping defense systems in a timely manner to counter new attacks is essential and can be the difference between a thwarted and a successful attack. Storing rules in a code-like format significantly enhances their clarity, interoperability, and ease of management. Rule sets stored in this manner represent a substantial advancement over the traditional, now outdated solutions used by defenders. F

Version control also simplifies teamwork and enables tracking of changes. Detection rules have designated owners who are responsible for creating and monitoring the lifecycle of the rules. Any fine-tuning or modifications made are automatically logged, making them fully traceable and auditable. Different versions resulting from specific client requirements or unique environmental characteristics can be managed more easily in a structured and organized manner. The use of version control systems opens new possibilities for collaboration, allowing detection rules to reflect the combined expertise.

A key advantage of code-like rule sets is that they can be annotated with MITRE ATT&CK mappings, enabling the creation of an automatically updated matrix that clearly reflects the current state of defense.

The built-in and extensible features of IDEs (such as syntax highlighting and code completion), multi-level automated testing and validation, and mandatory, traceable peer reviews integrated into the process minimize risks arising from human error. [14].

By adopting automation principles, detection rules are automatically deployed to environments, ensuring consistency and repeatability across all devices and systems. Continuous Integration and Continuous Deployment (CI/CD) pipelines further enhance this by automating the testing, validation, and deployment of detection rules, ensuring that updates are made swiftly in response to new attack techniques and vulnerabilities. This approach, when combined with continuous asset discovery, vulnerability management, MITRE ATT&CK mapping creates a comprehensive and adaptive security framework.

VIII. DISCUSSION AND CONCLUSION

Compared to earlier findings, the current study provides advancements in conceptualizing an Open-Source Intelligence (OSINT)-based Recognized Cyber Picture (RCP). By contrast, this study leverages an OSINT-centric approach, highlighting its potential to address situational awareness gaps without reliance on classified data. The absence of an OSINT-based implementation of RCP at the time underscores the novelty of this research [15]. The results indicate that OSINT can indeed serve as a foundation for developing an RCP. The dynamic nature of hybrid warfare necessitates adaptive and proactive measures. OSINT provides a viable alternative to traditional intelligence by aggregating publicly available information, which is often overlooked in classified frameworks. This enhances the feasibility and operational value of OSINT in supporting threat mapping and situational awareness. Tools such as heatmaps and detection coverage analysis and Detection-as-code are borrowed from other sectors like the electric, prove effective in identifying and addressing gaps in cyber defense.

These methods enable actionable insights. For networks to become more resilient against cyberattacks, especially in critical sectors, it is essential to keep these repositories up to date with Detection as code concept. Utilizing frameworks like MITRE ATT&CK, integrating advanced detection technologies, continuously managing risks, and updating threat intelligence systems are key to strengthening defense capabilities.

1) Limitations

While this paper presents avenues for the development of an Open-Source Intelligence (OSINT)-based Recognized Cyber Picture (RCP), several limitations must be acknowledged. One of the most significant limitations is the absence of classified data in this research. While OSINT provides valuable insights, classified intelligence often contains critical details about advanced persistent threats (APTs), attack methods, and vulnerabilities. Without access to this information, the RCP may lack the depth and precision required for high-stakes military applications. The retrospective nature of OSINT poses another challenge. Threat intelligence derived from publicly available sources may lag the rapidly evolving cyber threat landscape. Adversaries frequently update their tactics, techniques, and procedures (TTPs), rendering historical data potentially outdated or less effective for real-time decision-making, thereby introducing latency. Another significant concern is

data quality, which I have addressed through the implementation of a data accuracy multiplier within my methodology. The current RCP methodology lacks a mechanism for incorporating detailed vulnerability information. Effective cyber situational awareness depends not only on understanding adversarial behavior but also on identifying and addressing vulnerabilities within critical infrastructure and systems. This gap could lead to blind spots in the RCP, undermining its utility in proactive defense strategies. Developing an OSINT-based RCP requires substantial technical expertise and resources. Many NATO member states may face challenges in implementing and maintaining the necessary infrastructure, further exacerbating disparities in cybersecurity capabilities across the alliance.

REFERENCES

[1] M. Boda, "Hybrid War: Theory and Ethics", AARMS – Academic and Applied Research in Military and Public Management Science. Budapest, vol. 23, no. 1., pp. 5–17, 2024, DOI: 10.32565/aarms.2024.1.1.

[2] D. Bianco, "The Pyramid of Pain", Mar. 1, 2013. [Online]. Available: https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

[3] R. M. Lee, "Crashoverride – Analysis of the Threat to Electric Grid Operation", Dragos Inc., Hanover, MD, USA, Jun. 13, 2017. [Online]. Available: https://www.dragos.com/wp-content/uploads/CrashOverride-01.pdf

[4] The MITRE Corporation, (Sep. 22, 2022) Sandworm Team. [Online]. Available: https://attack.mitre.org/groups/G0034/

[5] MISP project, (2022, October 5) MISP Threat Sharing. [Online]. Available: https://www.misp-project.org/

[6] The MITRE Corporation, (Sep. 19, 2022) ATT&CK Matrix for Enterprise. [Online]. Available: https://attack.mitre.org/

[7] J. L. Kurtz, L. E. Damianos, R. Kozierok, and L. Hirschman, "The MITRE Map Navigation Experiment", MITRE Corporation, Bedford, MA, USA, Jun. 1., 1999. [Online]. Available: https://dl.acm.org/doi/pdf/10.1145/323216.323365

[8] The MITRE Corporation, (2024) Groups. [Online]. Available: https://attack.mitre.org/groups/

[9] R. Falcone, J. Grunzweig, J. Miller-Osborn, and R. Olson, "Operation Lotus Blossom", Palo Alto Networks, Santa Clara, CA, USA, 2015. [Online]. Available: https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/research/unit42-operation-lotus-blossom

[10] Unit 42, "Threat Group Assessment: Turla (aka Pensive Ursa)", Palo Alto Networks, Santa Clara, CA, USA, Sep. 15, 2023. [Online]. Available: https://unit42.paloaltonetworks.com/turla-pensive-ursa-threat-assessment/

[11] G. Dedola, D. Caldarella, A. Fedotov, and A. Gunkin, "ToddyCat: Keep calm and check logs", Kaspersky Lab, Moscow, Russia, Oct. 12, 2023. [Online]. Available: https://securelist.com/toddycat-keep-calm-and-check-logs/110696/

[12] The MITRE Corporation, (2024) Software. [Online]. Available: https://attack.mitre.org/software/

[13] The MITRE Corporation, (2024) Campaigns. [Online]. Available: https://attack.mitre.org/campaigns/

[14] M. Roddie, G. J, Katz, and J. Deyalsingh, Practical Threat Detection Engineering: A hands-on guide to planning, developing, and validating detection capabilities. Birmingham, UK: Packt Publishing Ltd, 2023.

[15] Kumar, Shekhar, Ummineni, Srikar Lyu, Ran Mondal, Sourav, Muthe, Laxman, Advanced Open-Source Intelligence (OSINT) Platform to Combat Misinformation on Social Media. [Online]. Available: https://vtechworks.lib.vt.edu/items/fbd991c7-a005-4562-8670-053d686b5c68

Gergő Gyebnár is the CEO of Black Cell. With over 15 years of experience in IT security, he brings valuable expertise to the role. As CEO, Gergő is responsible for leading the expansion of Black Cell's OT Security and Detection Engineering services worldwide. He is committed to delivering high-quality services and staying ahead of the curve in terms of technological advancements in the field of IT security.