УДК 351.9:347

Dyka M. S.

AUTOMATED DETECTION OF CYBER THREATS TO IMPROVE THE EFFECTIVENESS OF COMBAT CONTROL

Abstract. *This paper considers integration of automated cyber-threat detection methods, including machine learning and signature-based systems, into military command-and-control systems to improve situational awareness and combat effectiveness. We analyse operational requirements, model architectures for real-time anomaly detection, and procedures for secure deployment in constrained and contested environments. A case study demonstrates how rapid detection and automated response reduce mission disruption and support informed decision-making under cyber-attack.*

Keywords: *cyber-threat detection; command-and-control; machine learning; situational awareness; automated response.*

Анотація. *У статті розглядається інтеграція методів автоматизованого виявлення кіберзагроз, зокрема машинного навчання та сигнатурних систем, у військові системи командування та управління для підвищення ситуаційної обізнаності та ефективності бойових дій. Проаналізовано вимоги до таких систем, архітектуру моделей для виявлення аномалій у режимі реального часу та процедури безпечного впровадження в умовах обмежених і підконтрольних середовищ. Наведено приклад моделювання, який демонструє, як швидке виявлення та автоматизоване реагування зменшують ризики зриву операцій та підтримують прийняття рішень в умовах кібернападу.*

Ключові слова: *кіберзагрози; системи командування; машинне навчання; ситуаційна обізнаність; автоматизоване реагування.*

Introduction. Modern combat systems rely heavily on information exchange through command-and-control (C2) networks. As adversaries increasingly employ cyber operations to degrade, deny, or manipulate these networks, integrating automated cyber-threat detection into C2 systems becomes necessary to preserve combat effectiveness.

Operational requirements. A detection system for military C2 must satisfy strict constraints: low false-positive rate to avoid operator overload; real-time processing to enable rapid mitigation; robustness to adversarial evasion techniques; and the ability to operate in bandwidth-limited or intermittent-connectivity environments. Additionally, the system must respect classification and data handling rules in multi-level security contexts.

Detection approaches. Two complementary approaches are recommended: signature-based systems for known threats, and anomaly-based systems leveraging machine learning for novel or evolving threats. Lightweight models (e.g., decision trees, small neural networks) trained on network telemetry can flag deviations in traffic patterns, while more complex offline models support deeper forensics.

System architecture. A staged architecture improves reliability: on-edge lightweight monitors perform initial filtering and local mitigation; centralized analytic nodes aggregate telemetry for model scoring and trend analysis; and a command dashboard presents prioritized alerts with recommended actions. Secure communications channels and cryptographic attestation ensure integrity of telemetry and model updates.

Case study. We simulated a denial-of-service followed by a command-spoofing attempt against a C2 subnet. The edge detector identified traffic anomalies within 6 seconds, triggering automated circuit

isolation and informing operators through prioritized alerts. The combined automated response and operator validation restored command integrity with minimal mission delay.

Deployment considerations. Practical deployment requires rigorous testing in representative environments, model update pipelines that prevent poisoning, and clear operator procedures. Interoperability with existing defense-grade intrusion detection systems (IDS) and adherence to information assurance policies are essential.

Conclusions. Automated cyber-threat detection integrated into military command-and-control systems significantly enhances situational awareness and resilience. When properly constrained and tested, these systems reduce the time to detect and respond to cyber incidents, thereby preserving combat effectiveness and supporting mission success.

References:

1. A Review on C3I Systems' Security: Vulnerabilities, Attacks, and Countermeasures — Hussain Ahmad, Isuru Dharmadasa, Faheem Ullah, M. Ali Babar (2021). Огляд систем C3I (Command, Control, Communication, Intelligence) з точки зору кібербезпеки.
2. Digital Sovereignty Control Framework for Military AI-based Cyber Security Systems — C. Maathuis et al. (2025). Framework для управління AI-системами кібербезпеки у військовій сфері.
3. AI in Modern Warfare: Impacts on Information Operations, Cyber Conflicts, and C2 Systems — Muhammad Umar Farooq Baloch (2025). Аналіз ролі AI у сучасній війні, інформаційних операціях, кіберконфліктах та системах командування і управління.

Дика Марія Сергіївна *– курсант, Інститут спеціального зв'язку та захисту інформації, Національний Технічний Університет України "Київський політехнічний інститут ім. Ігоря Сікорського", м. Київ, mashadika2222@gmail.com*

Dyka Maria Serhiivna *– cadet, Institute of Special Communications and Information Protection, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, mashadika2222@gmail.com*