10.16920/jeet/2026/v39is4/26124

Cyber Warfare in Modern Conflicts: Implications for Engineering Education

B. Meenakshi Sundaram[1*], Suja Suresh[2], Shailesh G[3], Felcy Judith[4]
[1,4]Department of Computer Applications, [2,3]Department of Management Studies
T. John College (Autonomous), Bangalore.
bmsundaram@gmail.com[1]*, suja@tjohngroup.com[2], shailesh.choudary@gmail.com[3], felcyjudith@gmail.com[4]

***Abstract*— In light of the growing trend toward digitization of critical infrastructure systems and inter-connectedness, cyberspace has emerged as a strategic battleground in modern warfare. State and non-state actors taking part in cyber warfare activities use advanced computational techniques to gain access into and alter data contained in information systems. This paper presents a detailed technical and pedagogical understanding of cyber warfare including attack strategies like DDoS attacks, APTs, zero-day exploits, and ransomware. It also discusses the utilization of Artificial Intelligence (AI) and Machine Learning (ML) technology in cyber warfare attacks and countermeasures against such attacks. Network-centric warfare, cyber physical systems, vulnerabilities in various domains like energy, financial, and telecommunication sectors have also been discussed in the paper. Apart from this, there are certain challenges that have been examined in the current paper including attribution, real-time threat detection, and defense, and the misappropriation of AI by hackers for propaganda purposes. Cybersecurity should be included in engineering education curriculum keeping in mind the modern technological trends.**

***Keywords* — Cyber warfare, cybersecurity, artificial intelligence, machine learning, distributed denial of service (DDoS), advanced persistent threats (APTs).**

I. Introduction

The evolution of digital technologies and interconnection systems has changed the face of security across the globe. The cyber sphere has become an equally vital area as land, air, and water, providing avenues for conducting conflicts, which are much less apparent but devastating all the same. A cyber war is an act of aggression committed against a state's information system and its resources in order to destroy, manipulate, disable, and infiltrate the systems by any digital means available (R. A. Clarke & R. K, 2010).

As the systems become more intertwined and used in key areas like energy distribution, banking, medicine, and telecommunications, more possibilities arise for cyber-attacks. The techniques involved in the current cyber-attacks are highly sophisticated and hard to trace. Distributed denial of service, advanced persistent threats, ransomware, and zero-day attacks are some of the commonly employed forms of cyber-attacks currently (W. Stallings, 2017).

AI and ML are introducing new facets in the realm of cyber warfare (A. Mohamed,, 2023; I. H. Sarker et al, 2023). AI and ML are employed to facilitate automatic attacks, threat detection, and predictive analytics. However, there are many issues that might arise from using AI and ML in cyber warfare, including artificial intelligence and deepfakes (W. Xu et al, 2024).

From an engineering point of view, the knowledge of cyber warfare becomes crucial for creating designs. Engineering should move forward to encompass cybersecurity and other skills within its scope to ensure that future engineers are prepared to deal with emerging challenges (M. A. Ferrag et al, 2024; A. Tripathi, 2024).

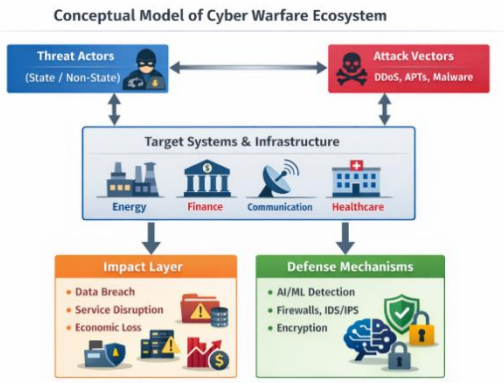

Fig. 1. Conceptual Model of Cyber Warfare Ecosystem

TABLE I
COMMON CYBER ATTACK TYPES AND CHARACTERISTICS

Attack Type	Description	Impact
DDoS	Flooding systems with traffic to disrupt services	Service downtime
Advanced Persistent Threats	Long-term targeted attacks with stealth techniques	Data theft, espionage
Ransomware	Encrypting data and demanding ransom	Financial loss, data inaccessibility
Zero-Day Exploits	Exploiting unknown vulnerabilities	System compromise
AI-driven Attacks	Use of AI for automated and adaptive attacks	Increased attack sophistication

II. LITERATURE ANALYSIS

The area of cyber warfare has seen tremendous progress owing to technological development. For gaining insight into the history of cyber warfare, it is important to have a thorough literature review. This literature review will form a basis for identifying some major findings in the area of cyber-attacks, defenses, and novel techniques. The review would enable one to understand the evolution of traditional security mechanisms into intelligent and adaptive security methods. Various contributions by scholars, including those which can be termed innovative in nature along with recent advancements within the field of artificial intelligence and machine learning, have been taken up for analysis in this paper. Further, the importance of ensuring security for cyber-physical systems has also been discussed in the literature review portion of the research. This way, a common perspective on cyber warfare studies shall be acquired. The technological evolution of cyber warfare studies will also be reviewed in this part of the research. This introduction presents the context for the literature overview that will be provided in the next table.

TABLE II
LITERATURE OVERVIEW

Ref. No.	Author(s) & Year	Focus Area	Key Contribution	Limitations / Research Gap
[1]	Clarke & Knake (2010)	Cyber Warfare Foundations	Established cyberspace as a fifth domain of warfare; outlined strategic cyber doctrines and national security implications	Lacks modern AI-driven threat context
[2]	Stallings (2017)	Network Security	Provided detailed taxonomy of cyber-attacks and layered defense mechanisms; widely adopted academic reference	Limited coverage of evolving threats like APTs and AI attacks
[3]	Vance (2023)	AI Policy & Cybersecurity	Analysed global AI adoption in cybersecurity; proposed governance models and policy frameworks for cyber defense	Limited technical implementation details
[4]	Mohamed (2023)	AI & ML Security Trends	Comprehensive survey of ML algorithms (SVM, ANN, DL) for intrusion detection and threat classification	Lacks cyber warfare-specific applications
[5]	Sarker et al. (2023)	AI-based Cyber Defense	Proposed intelligent IDS using ML models with improved detection accuracy and adaptive learning capabilities	Performance depends on training datasets
[6]	Xu et al. (2024)	LLMs in Cybersecurity	Introduced use of Large Language Models (LLMs) for automated threat analysis,	Limited deployment and scalability studies

			vulnerability detection, and incident response	
[7]	Ferrag et al. (2024)	Generative AI Security	Identified vulnerabilities in generative AI systems; proposed mitigation strategies against prompt injection and model misuse	Requires real-world validation
[8]	Tripathi (2024)	AI in Cybersecurity	Discussed predictive analytics and AI-driven cyber defense frameworks for proactive threat mitigation	Conceptual; lacks empirical validation
[9]	Kour et al. (2024)	Industry 5.0 Security	Highlighted cybersecurity challenges in Industry 5.0 environments integrating IoT, CPS, and AI systems	Limited focus on cyber warfare scenarios
[10]	ScienceDirect Study (2024)	AI & Geopolitical Risk	Established correlation between cyber warfare and geopolitical tensions; emphasized cyber deterrence strategies	Limited technical experimentation
[11]	Haryanto et al. (2024)	Contextual AI Security	Proposed context-aware AI models for adaptive cybersecurity and real-time anomaly detection	Limited benchmarking with existing systems
[12]	Uddin et al. (2025)	Generative AI in Security	Explored GenAI applications in threat intelligence, automated response, and cyber defense orchestration	Emerging field; lacks standard metrics
[13]	CrowdStrike Report (2025)	AI-driven Attacks	Provided empirical evidence of accelerated attack timelines and AI-powered cyber threats in real-world scenarios	Industry-focused; limited academic validation
[14]	Netwrix Reports (2025)	Cybersecurity Trends	Identified trends in zero-trust architecture, AI-based defense, and cloud security adoption	Lacks experimental validation
[15]	Erukude et al. (2026)	AI-driven Threat Evolution	Proposed new taxonomy of AI-enabled cyber threats including deepfakes, autonomous malware, and adversarial AI	Early-stage research; needs validation

III. Research Gaps and Engineering Education Perspectives

The reviewed literature exhibits great progress towards understanding cyber warfare across multiple domains including advanced attack vector, AI-based threat detection, and critical infrastructure cybersecurity (W. Xu et al, 2024; M. A. Ferrag et al, 2024; A. Tripathi, 2024).

However, some relevant problems in this sphere require further consideration. Firstly, there is no adequate theoretical framework for integrating an AI-based cybersecurity system into practice (R. Kour et al, 2024; Y. Zhang et al, 2024), as the existing literature focuses mainly on theoretical discussion and empirical analysis. Secondly, the cyber warfare model considering the technical, strategic, and geopolitical dimensions requires more consideration. Thirdly, while the use of LLMs and Generative AI in cybersecurity demonstrates positive trends (T. Haryanto et al, 2024; M. Uddin et al, 2025), there is still no point at which validation and practical implementation of this technology should be considered. Fourthly, the issue of cyber-physical systems in different industries requires further examination.

Regarding engineering education (CrowdStrike, 2025; Netwrix Corporation, 2025; O. Erukude et al, 2026), the most essential gap can be identified as the lack of cyber warfare courses in the curriculum of engineering students. The current educational programs are focused primarily on cybersecurity and do not provide enough information regarding the practical implications of cyber warfare, threat intelligence, and AI-based cybersecurity systems. Moreover, there is no proper platform where the knowledge and skills of students in these areas can be practiced.

Based on the above-mentioned factors, this paper identifies the need to address the following shortcomings:

- Over-reliance of the existing curriculum on issues related to cyber warfare, artificial intelligence, and protection of critical infrastructures;
- Use of simulation environment as a learning platform;
- Integration of cybersecurity with data science and system engineering in the same module.

Creation of an efficient cybersecurity framework that can scale up, therefore bridging the gap between research and application within engineering education is vital.

IV. Proposed Cyber Warfare Education Framework

The increasing complexity of cyber threats and the integration of Artificial Intelligence (AI) in cyber warfare necessitate a structured and application-oriented educational framework. This section proposes a comprehensive Cyber Warfare Education Framework designed to bridge the gap between theoretical knowledge and practical implementation in engineering education.

The framework adopts an **interdisciplinary approach**, integrating cybersecurity, artificial intelligence, network engineering, and critical infrastructure protection. It emphasizes **hands-on learning, simulation-based training, and real-world case analysis** to equip students with the necessary skills to address modern cyber threats.

1. Framework Architecture

The above-mentioned structure can be divided into four main layers:

1. Layer of Basics

Deals with basic fundamentals in terms of cybersecurity, networking, and cryptography.

2. Technical Layer

Considers technical attacks like DDoS, APTs, ransomware, and zero-day exploits.

3. Intelligence Layer

Incorporates intelligence in terms of AI/ML-based threats, threat prediction, and automation tools.

4. Practical Layer

Offers practical exposure through cyber ranges and case studies.

Fig. 2. Proposed Cyber Warfare Education Framework

2. Curriculum Integration Model

The framework can be integrated into engineering programs through modular course design:

TABLE III
MODULAR COURSE DESIGN

Module	Title	Key Topics	Learning Outcome
Module 1	Fundamentals of Cybersecurity	CIA Triad, Network Basics	Understand security principles
Module 2	Cyber Threats & Attacks	DDoS, Malware, APTs	Analyse cyber-attack methods
Module 3	AI in Cybersecurity	ML models, anomaly detection	Apply AI for threat detection
Module 4	Cyber Warfare & Infrastructure	CPS, critical systems	Evaluate infrastructure risks
Module 5	Simulation & Case Studies	Cyber labs, real attacks	Develop practical skills

3. Practical Implementation Strategy

In order for effective learning to take place, the model includes:

- Simulation-Based Learning: Utilization of cyber ranges and virtual labs to simulate cyber attacks in the real world
- Tool-Based Training: Direct interaction with tools such as Wireshark, Kali Linux, Metasploit, and AI-powered security applications
- Case Study Methodology: Examination of cyber attacks that have occurred in reality to comprehend attack methodologies and defenses against them
- Project-Based Learning: Creation of cybersecurity techniques using AI

4.4 Assessment and Outcome Mapping

The framework supports **Outcome-Based Education (OBE)** by aligning learning outcomes with assessment methods:

TABLE IV
OBE METHODS

Assessment Method	Skills Evaluated
Assignments	Conceptual understanding
Lab Experiments	Practical skills
Case Studies	Analytical ability
Projects	Problem-solving & innovation
Exams	Technical knowledge

4. Key Contributions of the Framework

- Bridges the gap between **theoretical cybersecurity knowledge and practical application**
- Integrates **AI/ML with cyber warfare concepts**
- Supports **interdisciplinary and outcome-based education**
- Prepares students for **real-world cyber defense and security challenges**

V. Mapping of Skills vs. Curriculum Components

TABLE V
MAPPING OF SKILLS

Skill Category	Specific Skills	Curriculum Component	Learning Method	Assessment Method
Fundamental Skills	Networking basics, Cryptography, Security principles	Foundation Layer (Module 1)	Lectures, Tutorials	Written Exams, Assignments
Technical Skills	Understanding DDoS, APTs, Malware, Zero-day exploits	Core Technical Layer (Module 2)	Case Studies, Demonstrations	Quizzes, Case Analysis
Analytical Skills	Threat analysis, Vulnerability assessment, Risk evaluation	Module 2 & 4	Problem-based Learning	Analytical Reports
AI/ML Skills	Machine learning models, anomaly detection, predictive analysis	Advanced Intelligence Layer (Module 3)	Lab Experiments, Simulations	Lab Evaluation, Mini Projects
Tool-Based Skills	Wireshark, Kali Linux, Metasploit, AI security tools	Modules 2, 3 & 5	Hands-on Labs	Practical Exams
System Design Skills	Secure system design, architecture planning, CPS security	Module 4	Design Projects	Project Evaluation

Problem-Solving Skills	Incident response, attack mitigation strategies	Module 4 & 5	Simulation Exercises	Scenario-based Tests
Research Skills	Literature analysis, report writing, innovation	All Modules	Research Assignments	Paper/Report Submission
Collaboration Skills	Teamwork, interdisciplinary integration	Project Work (Module 5)	Group Projects	Peer Evaluation
Ethical & Professional Skills	Cyber ethics, legal compliance, data privacy	Integrated across modules	Discussions, Seminars	Viva, Presentations

CONCLUSIONS

The importance of cyber warfare has become more pronounced due to the fast pace of digitization and the growing complexities associated with cybersecurity threats. In this regard, this paper offered a thorough discussion on cyber warfare including its potential attack vectors, Artificial Intelligence and Machine Learning capabilities, and weaknesses in critical infrastructures. Literature review demonstrated that cybersecurity has evolved from defensive strategies to intelligent cybersecurity using artificial intelligence and machine learning but there are still important shortcomings in implementation and teaching.

This paper suggested a Cyber Warfare Education Framework, which includes learning about foundational knowledge, technical concepts, and simulation training through actual cases of cyber attacks. Furthermore, this paper discussed the importance of interdisciplinary learning, tools training, and outcomes-focused education when preparing engineers for future cyber warfare.

In summary, the gap between advancing cyber threats and cyber education needs to be bridged to ensure cybersecurity in the digital age.

REFERENCES

R. A. Clarke and R. K. Knake, Cyber War: The Next Threat to National Security and What to Do About It. New York, NY, USA: HarperCollins, 2010.

W. Stallings, Network Security Essentials: Applications and Standards, 6th ed. Pearson, 2017.

A. Vance, “Artificial intelligence in cybersecurity: A survey of national research investment and policy implementation,” Journal of Cyber Policy, vol. 8, no. 2, pp. 145–162, 2023.

A. Mohamed, “Artificial intelligence and machine learning for cybersecurity: A comprehensive review,” Cogent Engineering, vol. 10, no. 1, pp. 1–15, 2023.

I. H. Sarker et al., “Machine learning-based cybersecurity intrusion detection: A survey,” Information Systems, vol. 117, p. 102215, 2023.

W. Xu et al., “Large language models for cybersecurity: Opportunities and challenges,” arXiv preprint arXiv:2405.04760, 2024.

M. A. Ferrag et al., “Security and privacy challenges in generative AI systems,” arXiv preprint arXiv:2405.12750, 2024.

A. Tripathi, “AI and cybersecurity in 2024: Navigating new threats and opportunities,” International Journal of Information Security Science, vol. 13, no. 1, pp. 25–38, 2024.

R. Kour et al., “Cybersecurity challenges in Industry 5.0: A comprehensive review,” Frontiers in Computer Science, vol. 6, p. 1434436, 2024.

Y. Zhang et al., “Artificial intelligence and cyber warfare: Emerging trends and geopolitical implications,” Computers & Security, vol. 135, p. 103338, 2024.

T. Haryanto et al., “Context-aware artificial intelligence for adaptive cybersecurity systems,” arXiv preprint arXiv:2409.13524, 2024.

M. Uddin et al., “Generative AI in cybersecurity: Opportunities and challenges,” Artificial Intelligence Review, 2025, doi: 10.1007/s10462-025-11219-5.

CrowdStrike, Global Threat Report 2025. CrowdStrike Inc., 2025.

Netwrix Corporation, Cybersecurity Trends Report 2025. Netwrix, 2025.

O. Erukude et al., “AI-driven cyber threats: A new taxonomy and future directions,” arXiv preprint arXiv:2601.03304, 2026.