Journal of Posthumanism

2025
Volume: 5, No: 3, pp. 1667–1689
ISSN: 2634-3576 (Print) | ISSN 2634-3584 (Online)
posthumanism.co.uk

DOI: https://doi.org/10.63332/joph.v5i3.965

AI-Enhanced Cyber Threat Detection and Response Advancing National Security in Critical Infrastructure

Mohammad Abdul Goffer[1], Md Salah Uddin[2], Jobanpreet kaur[3], Syed Nazmul Hasan[4], Clinton Ronjon Barikdar[5], Jahid Hassan[6], Niropam Das[7], Partha Chakraborty[8], Rakibul Hasan[9]

Abstract

Rapid digitalization of essential national infrastructure has created new vulnerabilities to cyber threats, leading to major security threats against the nation. The current security measures prove inadequate for keeping pace with developing cyberattacks, so artificial intelligence needs integration for threat detection enhancements and response improvements. The combination of AI-enabled cybersecurity systems gives them the ability to examine huge data collections instantly, monitor irregularities and perform automatic threat response functions to improve national security. Research investigates the system of artificial intelligence to enhance cyber threat response capabilities alongside its specific use for defending crucial infrastructure elements like energy networks as well as financial organizations and government IT infrastructure. Methodology The study combines qualitative approaches with quantitative methods as its research methodology. The analysis includes a structured review of existing frameworks that use AI for cybersecurity purposes with their performance evaluation. The paper evaluates real-world AI deployments across critical infrastructure systems through case studies to reveal successful strategies with encountered problems. The empirical proof of machine learning-based intrusion detection systems is carried out by testing IDS along with real-world dataset assessment to verify AI's threat mitigation effectiveness through the accuracy and precision & recall method. Security experts who perform interviews deliver valuable information about the current use of AI technology in national security applications. The national cybersecurity capabilities gain strength from AI-driven systems because these systems accomplish improved threat detection and swift responses without requiring human involvement. AI deliver its maximum effectiveness only when data privacy issues with adversarial AI attacks and regulatory hurdles, receive proper solutions.

Keywords: *Artificial Intelligence, Cyber Threat Detection, Critical Infrastructure, National Security, Intrusion Detection Systems, Machine Learning, Cybersecurity, Threat Mitigation, AI-Driven Security.*

[1] School of Business, International American University, Los Angeles, CA 90010, USA. Email: mdabdulgoffer1991@gmail.com. ORCID ID: https://orcid.org/0009-0001-1049-947X.
[2] College of Technology & Engineering, Westcliff University, CA 92614, USA. Email: m.uddin.182@westcliff.edu. ORCID ID: https://orcid.org/0009-0001-0741-1393).
[3] College of Technology & Engineering, Westcliff University, CA 92614, USA. Email: j.kaur.244@westcliff.edu. ORCID ID: https://orcid.org/0009-0008-0083-8205.
[4] College of Technology & Engineering, Westcliff University, CA 92614, USA. Email: s.hasan.104@westcliff.edu. ORCID ID: https://orcid.org/0009-0008-0977-595X.
[5] School of Business, International American University, Los Angeles, CA 90010, USA. Email: barikdarclinton@gmail.com. ORCID ID: https://orcid.org/0009-0002-6291-2446.
[6] School of Business, International American University, Los Angeles, CA 90010, USA. Email: engineer.jhassan@gmail.com. ORCID ID: https://orcid.org/0009-0005-0215-3179.
[7] School of Business, International American University, Los Angeles, CA 90010, USA. Email: niropomdas124@gmail.com. ORCID ID: https://orcid.org/0009-0004-6107-7025
[8] School of Business, International American University, Los Angeles, CA 90010, USA. Email: parthachk64@gmail.com. ORCID ID: https://orcid.org/0009-0006-3203-8902
[9] Department of Business Administration, Westcliff University, Irvine, CA 92614, USA. Email: rakibbd2237@gmail.com. ORCID ID: https://orcid.org/0009-0001-7268-390X

Introduction

Overview of cyber threats to national security

National security faces severe cyber threats because these attacks affect governmental processes and economic systems and public security standards. Nation-states and cybercriminals execute diverse malicious actions that combine cyberterrorist attacks and state-based cyberattacks and cybercrime with hacktivist behavior (White, 2016). Nation-state actors take advantage of online system weaknesses to pursue strategic goals, which include intelligence gathering as well as power grid disruption and control of political events. U.S. intelligence published a report that labeled China as an important military power that attacks infrastructure through cyberspace while seeking artificial intelligence dominance against the United States by 2030 (Oruj, 2023). The money-driven cyberattacks make up cybercrime threats, which constitute serious threats to countries' defense systems. Such illicit operations result in financial costs along with disturbances of critical services which deteriorate public confidence.

The overwhelming number of cyberattacks on the country creates sustained pressure on national economic performance while exceeding the limits of cybersecurity defense capabilities (Dinicu, 2014). The contemporary cyber threat environment becomes more complex because various non-state actors, like terror organizations alongside organized crime groups, now utilize cyber capabilities to achieve their objectives (Li and Liu, 2021). The networked characteristics of digital systems generate vulnerability repercussions that spread between different domains, which proves why an adaptable cybersecurity strategy implemented (Patel and Chudasama, 2021). Preventing cyber threats that have multiple dimensions needs synchronized activities between public institutions and business sectors as well as international alliances. Nationwide interests require protection in the digital era because of improved information exchange along with effective defensive systems and active risk management processes (Prasad et al., 2020).

Importance of AI in cyber security

Modern cybersecurity depends heavily on artificial intelligence technology, which detects security threats better, streamlines operational security, and adapts efficiently to new digital risks. Through analyzing extensive data collections, AI-driven systems discover distinct patterns with abnormal activities that traditional security methods cannot achieve (Sarker et al., 2021). The continuous learning ability of machine learning algorithms supported by AI enables the system to discover new attack methods through new data, which helps it modify its defense strategies (Lazić, 2019). AI systems use automation to perform recurring security duties, which include network traffic monitoring and low-level incident response, through which cybersecurity professionals obtain time to address sophisticated security problems (Zhang et al., 2022). AI systems provide extensive benefits from their ability to manage vast digital structures and maintain uniform security supervision over extensive organizations Carlo et al., 2023). AI-powered security tools from Microsoft, alongside others, assist major technology organizations through automated duties, including phishing alert assessment and vulnerability tracking systems, which boost security defenses (Jimmy, 2021). Artificial intelligence integration forms the backbone of modern cybersecurity because it assists in protecting essential digital resources from modern high-level cyber threats (Stamp et al., 2022).

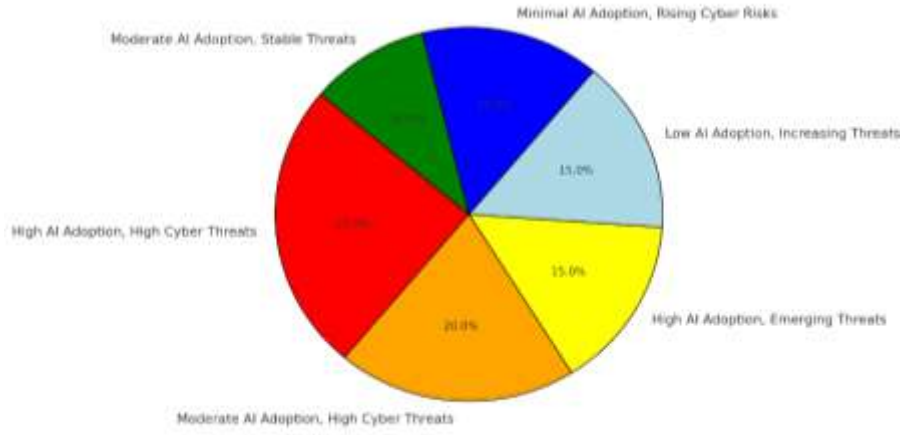


Figure No.01: Cybersecurity threats and AI adoption levels in critical infrastructure

Emergence of Generative AI in cybersecurity

The field of cybersecurity gets transformed through Gen AI, which enables superior threat detection alongside automated incident response and improved security decision-making abilities (Yigit et al., 2024). The system operates differently from conventional AI models since Gen AI applies deep learning techniques to develop new data while mimicking cyberattacks as well as predicting security threats (Dhoni and Kumar, 2023). The primary security application of Gen AI involves security teams employing adversarial AI by generating simulated attacks that assess and enhance their defense structures (Dhoni and Kumar, 2023).

Gen AI develops superior threat intelligence capabilities through its ability to scrutinize extensive datasets, which reveal system weaknesses and give immediate security evaluations (Krishnamurthy, 2023). The development of general artificial intelligence gives cybercriminals the ability to create complex phishing attacks and deepfake-based social engineering scams and automated malware because of its advanced capabilities (Teo et al., 2024).Security organizations establish AI-based defense systems that utilize self-learning security mechanisms and AI authentication along with anomaly detection protocols as their countermeasures (Vardhan et al., 2025).The integration of generalized artificial intelligence become essential for defenders of digital systems since cyber threats continue to progress while protecting essential sectors against risks.

Research objectives and scope

The study investigates how Artificial Intelligence with its subtype Generative AI serves cybersecurity functions for protecting national security in addition to critical infrastructure components. The research evaluates the uses of AI in threat detection and incident response alongside risk management through an assessment of its contributions toward securing energy sectors and finance and healthcare alongside government institutions. The study conducts an evaluation of AI's capacity to fight international safety threats such as cyber warfare with terrorism and state-sponsored attacks. AI technology strengthens cybersecurity resilience it creates new vulnerabilities through adversarial AI systems and deepfake threats as well as AI automation of cyber-attacks. The research goal is to analyze AI security system vulnerabilities

to develop safety guidelines that maximize AI security benefits for national cybersecurity. This study branches out across the whole world to examine cybersecurity through multiple American, European Union, Chinese, and other cybernation cases and incorporates cybersecurity threat intelligence alongside international security regulations and ethical considerations regarding AI systems.

Figure NO.02: Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity

Literature Review

AI applications in cybersecurity

The field of cybersecurity receives transformation through artificial intelligence, which enables threat detection enhancement and security operation automation and incident response improvement (Jun et al., 2021). AI-driven cybersecurity systems use machine learning algorithms to scan extensive data, which helps them detect irregular patterns that represent cyber threats (Zhang et al., 2022). AI systems powered by artificial intelligence function as real-time threat detectors to track network traffic while they spot abnormal activities before attacks become full-scale events (Abbas et al., 2019).Artificial intelligence-based endpoint security enhances protection against malware, ransomware, and phishing attacks through its behavior-based threat detection approach (Khan et al., 2024).

AI enables automated incident response by allowing security systems to initiate real-time responses against cyber threats reducing incident damage and human security analyst involvement (Hofstetter et al., 2020). The combination of artificial intelligence powers fraud prevention measures along with identity verification systems to stop unauthorized entry and criminal transactions in online platforms and financial institutions (Sikos, 2018). Security defenses receive expanded protection through the implementation of adversarial AI and AI-driven cyber deception approaches that conduct sophisticated cyber-attack simulations (Kaur et al., 2023). AI supports nations and world operations for cybersecurity protection by helping governments protect their essential infrastructure systems, which include energy grids, communication networks, and financial institutions (Camacho, 2024).The increasing strength of AI in cybersecurity has created new opportunities for cybercriminals who continue using AI to conduct automatic attacks as well as generate deepfake-based social engineering attacks and AI-

made malware while needing sustained advancements in AI-defense strategies (Salem et al., 2024).

Evolution of cyber threats targeting critical infrastructure

The cyber threats focused on critical infrastructure have undergone substantial development, which resulted in more complex activities with greater frequency because of technological progress and the widespread use of digital infrastructure (Aminu et al., 2024).The attack landscape for infrastructure security behaviors transformed to encompass basic malware and ransomware initially it transformed into much more advanced threats because of state-sponsored cyber warfare and AI-driven attacks and zero-day exploit developments (Lehto, 2022). Attacks performed by perpetrators using artificial intelligence combined with machine learning automation systems target industrial control systems as well as supervisory control and data acquisition networks to perform widespread exploits as well as overcome detection systems (Rudner, 2013).

Critical infrastructure facilities, including hospitals, power grids and financial institutions, fall victim to ransomware attacks that force criminals to initiate ransom payments (George et al., 2024). The persistent threat of Advanced Persistent Threats enables nation-state actors to successfully penetrate government along with military networks so they acquire sensitive data while taking control of critical systems (Beretas, 2024). The increasing threat comes from supply chain attacks since adversaries exploit weak third-party vendors to obtain entry into big infrastructure providers, as demonstrated by the SolarWinds attack (Mitsarakis, 2023). The increase of cyber threats caused by AI technology introduced deepfake-based information manipulation with automated phishing schemes and malware that breaks through standard security systems (Choraś et al., 2016). The Internet of Things and 5G technologies have added to the attack surface because cybercriminals now use these new technologies to breach smart grid and connected vehicle and industrial automation systems (Riggs et al., 2023).

National and international security frameworks

Governments across the nation have established regulatory policies and cybersecurity laws and frameworks as protective measures. The U.S. Cybersecurity and Infrastructure Security Agency has launched two critical programs, which are the National Cyber Incident Response Plan and Cybersecurity Framework to assist organizations with their cyber risk management (Ripsman and Paul, 2005). The European Union added the NIS2 Directive to its legislation for enhancing cybersecurity requirements aimed at essential services and digital service companies (Leffler, 1990). Global cooperation regarding cybersecurity occurs through UN, NATO, and ITU organizations, which implement policy standards and information-sharing programs and develop cyber defense procedures (Handley and Zeigler, 2002). International cooperation for handling cybercrimes moves forward through the Budapest Convention on Cybercrime, which the Council of Europe established as a complete global framework to assist countries in teaming up across borders.

The Cybercrime Directorate of INTERPOL gives worldwide law enforcement agencies the power to fight cybercrimes by sharing intelligence data along with conducting united operations (Alagappa, 1998). Current global cybersecurity alliances such as the Global Forum on Cyber Expertise and the Paris Call for Trust and Security in Cyberspace concentrate on combining efforts between government entities and private organizations as well as academic institutions

to create guidelines for responsible cyber operations (McCormack, 2008). Various issues work against creating uniform cybersecurity rules between nations because legal systems differ while countries evolve technologically and remain geopolitically distant (Davies, 2013). National and international security frameworks strengthened because they protect critical infrastructure and help achieve digital world stability and control cyber threats (Scheppele, 2010).

Figure No 03: Key Business Security functions automated

Security Issues in Critical Infrastructure

Energy Sector Attacks

Power grids with oil refineries and nuclear plants, now function as primary cybercriminal targets since state-supported cyberattacks combined with ransomware threats escalate persistent security breaches (Aradau, 2010). Power supply infrastructure dependent on Industrial Control Systems and Supervisory Control and Data Acquisition networks expose systems to major failures that result in general power outages as well as national security concerns and economic disruptions (Ghafir et al., 2018). The Colonial Pipeline attack in 2021 represented one of the most renowned ransomware assaults against the energy sector because it resulted in fuel supply disruptions across the U.S. East Coast, which required Colonial Pipeline to pay $4.4 million in ransom to cybercriminals (Khaustova et al., 2023). Ukraine experienced nationwide power outages when Russian puppet hackers attacked its power grid during 2015 and 2016 through SCADA system weaknesses (Younis and Kifayat, 2013).

Advanced cyber threats have become stronger because attackers employ AI-controlled malware with phishing schemes and zero-day vulnerabilities to penetrate vital infrastructure operations (Buttyán et al., 2010). The rising cybersecurity risks compel energy providers to deploy artificial intelligence systems that use anomaly detection algorithms and real-time threat analysis and automated incident handling capabilities as described in (Lewis, 2019).

The International Energy Agency, along with the U.S. Department of Energy and other

international organizations, has launched cybersecurity resilience frameworks to defend national power grids from cyber attackers (Radvanovsky and McDougall, 2023). Modern energy infrastructure security faces three main obstacles which include defending aged systems, strengthening private-public sector partnerships and enforcing rigorous cybersecurity regulations (Stamp et al., 2003). The energy sector significantly enhance its cyber resilience because it protects the national security system from major disruptions that become more frequent due to digital threats (Abouzakhar, 2013).

Table No.01: summarizing security threats and their impact on ransomware attacks targeting power grids,

Security Threats	**Colonial Pipeline Attack (2021)**	**Ukraine Power Grid Attack (2015 & 2016)**	**Triton Malware Attack (2017)**	**Black Energy Malware Attack (2014)**
Phishing Attack	√	√	×	√
Ransomware Deployment	√	×	×	×
SCADA System Exploitation	×	√	√	×
State-Sponsored Cyberattack	×	√	√	√
Zero-Day Vulnerability Exploit	√	×	√	√
Disruption of Power Grid Operations	×	√	√	√
Data Exfiltration & Espionage	√	×	√	×
Use of AI-Enhanced Malware	×	×	√	×
Insider Threats	×	×	√	×

Financial Sector Breaches

Financial institutions now serve as top choice targets for AI-driven cyber-attacks because criminals use machine learning and deepfake technologies to achieve complex fraud, steal identities, and perform massive financial breaches (Cyriac and Sadath, 2019). Cybercriminals now use AI technology to go around traditional security measures while they create automated phishing attacks that take advantage of banking network weaknesses (Lee et al., 2022). Deepfake fraud represents a grave financial threat because attackers apply synthetic media to create executive impersonations that authorize criminal transactions. A UAE bank lost $35 million to cybercriminals who mimicked a high-ranking official with fake voice deepfakes during an audacity in 2020 (Hemphill and Longstreet, 2016). The combination of AI algorithms by malefactors generates fake news, which they use to control market sentiment and execute rapid

fraudulent stock market trades (Chaturvedi et al., 2022). AI-based botnet attacks currently pose a serious threat to financial institutions because cybercriminals succeed in automating credential stuffing security breaches in addition to carrying out brute-force attacks and evading real-time fraud detection (Weiss and Miller,2015).

Table No.02;AI-driven financial sector breaches and their associated security threats using

Security Threats	**AI-Driven Deepfake Fraud (2020 UAE Case)**	**Stock Market Manipulation**	**AI-Powered Phishing Attacks**	**AI-Driven Botnet Attacks**
Deepfake Voice/Video Impersonation	√	×	×	×
Automated Phishing Campaigns	×	×	√	×
Algorithmic Market Manipulation	×	√	×	×
Real-Time AI-Based Fraud Execution	√	√	√	√
Credential Stuffing & Account Takeover	×	×	√	√
Synthetic Identity Fraud	√	×	√	×
Regulatory & Compliance Challenges	√	√	√	√

Government and Defense Systems Intrusions

Nation-state cyber warfare targets government and defense platforms by enabling enemies to use AI-empowered cyberattacks for attacking vital defense structures and intelligence manipulation, which weakens national security (Mitchell and Banker, 1997). Modern geopolitical conflicts utilize three prominent cyber weapons, which include cyber espionage with data breaches as well as AI-enhanced malware attacks (Dasgupta,1999). The SolarWinds hack from 2020 became a notable example of nation-state cyber warfare because APT groups backed by a state government successfully concealed malware solutions inside IT management software as they penetrated U.S. federal agencies (Foo et al., 2008). Coders successfully penetrated Iranian nuclear centrifuges by means of sophisticated AI-powered cyber warfare in the Stuxnet attack of (Anwar et al., 2017). The realm of cyber warfare has transformed through AI technology because of its capability to create automatic threats while speeding up data theft operations and distributing fake content through deepfake techniques (Terry, 1999).

Governments across the world continue to answer AI threats by implementing AI technology into defensive systems that detect threats and make predictions about cyber intrusion capabilities (Kakareka, 2013).

Table No.03: AI-Powered Cyber Threats to Government and Defense Systems

Cyber Threats	SolarWinds Hack (2020)	Stuxnet Attack (2010)	Chinese Cyber Espionage (2021)	Russian Disinformation Campaigns
AI-Powered Malware	√	√	√	×
Supply Chain Attack	√	×	√	×
Nation-State Espionage	√	√	√	√
Autonomous Cyber Threats	×	√	√	√
Deepfake-Based Disinformation	×	×	√	√
AI-Driven Data Exfiltration	√	×	√	√

Telecommunications and Smart Cities Vulnerabilities

The fast development of telecommunications networks alongside smart cities produced rising interconnectivity threats from Internet of Things (IoT)-based devices that expose critical infrastructure to cybersecurity dangers (Kitchin and Dodge, 2020). 5G networks and linked surveillance systems and smart traffic control networks along with energy grids enabled by IoT represent main attack targets, including botnet-driven DDoS events, AI-enabled malicious code, and continuous-time information breaches (Tahirkheli et al., 2021). Named after the Mirai botnet attack from 2016, the Mirai botnet attack represented one of the notorious IoT-based attacks that used compromised IoT devices to launch massive distributed denial-of-service attacks on main websites and telecom services (Cardoni, A., Borlera et al., 2022). Smart cities face modern-day threats from AI-based cyberattacks, including deepfake-generated voice spoofing for telco fraud and machine learning-generated adversarial difficulties that break through infrastructure security protocols. Cybercriminals with state-sponsored actors, find telecommunications networks and smart cities appealing targets because of non-standard security procedures, outdated IoT firmware, and weak encryption protocols (Al-Turjman et al., 2022).

Table No.04: IoT-Based Cyber Threats in Telecommunications and Smart Cities

Cyber Threats	Mirai Botnet Attack (2016)	Smart City Water Hack (2021)	AI-Driven Telecom Fraud	IoT DDoS on 5G Networks
Botnet-Based DDoS Attack	√	×	×	√
Critical Infrastructure	×	√	×	√

Manipulation				
AI-Powered Malware Injection	×	√	√	√
Deepfake-Based Telecom Fraud	×	×	√	×
Adversarial AI Exploits in IoT	√	√	√	√
Data Exfiltration from Smart Systems	×	√	√	√

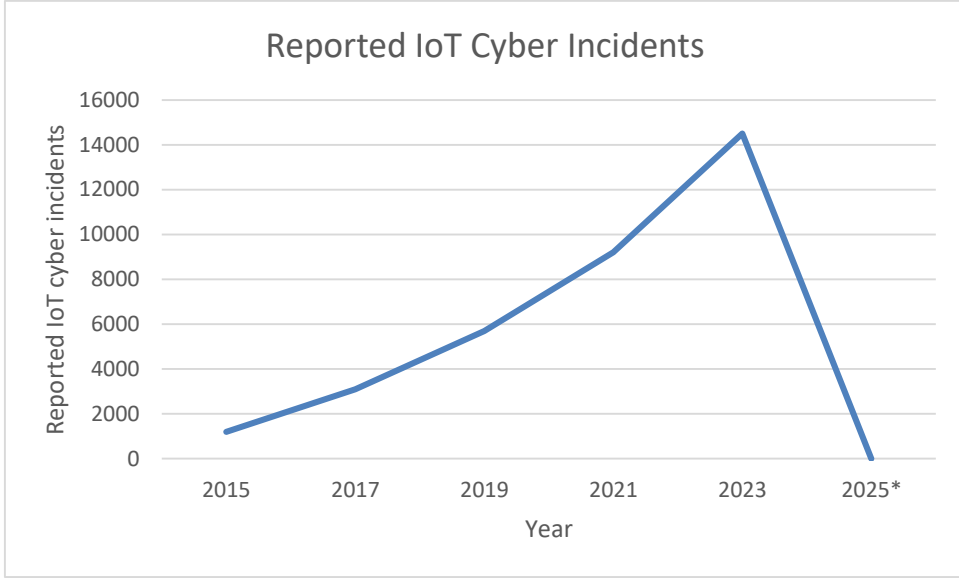


Figure No.04: Increase in IoT-Based Cyber Threats (2015–2025 Projection)

International Cybersecurity Threats

Nation-State Cyber Attacks

National cyberattacks have become an urgent threat to worldwide safety because governments use cyber warfare methods alongside sanctioned hacking techniques and artificial intelligence in spy operations against rival infrastructures (Lundbohm, 2017). Geopolitical tensions between Russia and Ukraine, along with Chinese cyber espionage, serve as evidence that cyber operations threaten the stability of national security and economic foundations and military defense networks (Mansfield-Devine, 2020). Cyberattacks functioned in conjunction with typical military operations throughout the Russia-Ukraine conflict.

A malware attack called NotPetya (2017) resulted from Russian-backed hackers targeting Ukrainian government systems, banks, and media organizations, which produced billions of dollars' worth of financial damage (Wentz et al., 2011). The cyber espionage activities

performed by China target intellectual property theft as well as surveillance efforts and infiltration of vital infrastructure. The Chinese-based APT41 organization employs AI-assisted techniques to execute cyberattacks against international healthcare defenses and financial institutions and defense facilities (Wentz et al., 2011).

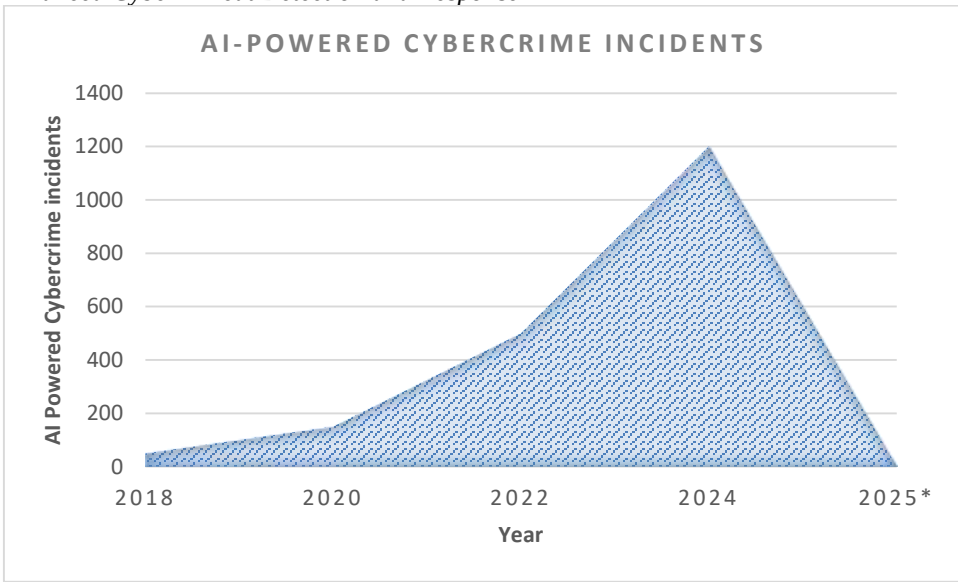
Table No.05: Nation-State Cyber Attacks and Their Impact

Nation-State Cyber Attack	**Targeted Country**	**Tactics Used**	**Impact**
NotPetya Malware (2017)	Ukraine	Data-wiping malware, ransomware disguise	$10 billion in global damages
SolarWinds Hack (2020)	USA, Europe	Supply chain attack, espionage	18,000 compromised organizations
Microsoft Exchange Hack (2021)	Global (China-linked)	Zero-day vulnerabilities, espionage	Data breaches in 60,000+ companies
Hermetic Wiper (2022)	Ukraine	Destructive malware, infrastructure sabotage	Disruption of financial institutions
APT41 Espionage (Ongoing)	USA, Europe, Asia	AI-enhanced cyber intrusions	Stolen defense and business secrets

AI-Driven Cybercrime

Table No.06 Case Study: AI in Phishing and Deepfake Scams

Cybercrime Type	**Example Case**	**AI Technique Used**	**Impact**
Deepfake CEO Fraud	UK-based energy firm scam (2019)	AI voice cloning	$243,000 stolen
AI Phishing Attack	Office 365 phishing campaign (2022)	ML-generated emails	30,000+ accounts compromised
Deepfake Video Scam	Fake Elon Musk cryptocurrency ad (2023)	GAN-based video synthesis	Millions lost in fraud



Cyber Terrorism Disrupting financial markets, targeting critical systems

The existing threat to national and international security stems from cyber terrorism because it attacks financial markets as well as critical infrastructure and essential government systems. By using sophisticated AI techniques, cyber terrorists interrupt stock exchanges, banking systems, and power grids, which results in economic troubles and mass public panic (Lewis, 2002). AI-based cyberattacks function to manipulate financial transactions as well as crash stock markets while disabling vital digital networks (Nish et al., 2022). Cyber-attacks against power grids along with transportation systems create widespread disruptions that result in extensive power outages and compromised essential services for millions of people (Johnson, 2015). AI-enhanced malware with ransomware, continues to threaten defense networks and government agencies, so security personnel are at risk (Wilson, 2003).

Table No.07: Cyber Terrorism Threats and AI Techniques

Threat Type	**Target**	**AI Techniques Used**	**Potential Impact**
Financial Market Disruptions	Stock exchanges, banks	Algorithmic market manipulation, AI-powered fraud	Economic instability, stock crashes
Critical Infrastructure Attacks	Power grids, water systems	AI-driven ransomware, IoT-based cyberattacks	Blackouts, water contamination
Government Network Intrusions	Defense agencies, databases	AI-enhanced malware, deepfake identity fraud	Data breaches, espionage
Transportation System Disruptions	Airlines, railways	AI-manipulated traffic control systems	Travel delays, accidents

Disinformation Campaigns	Public opinion, elections	Deepfake videos, AI-generated fake news	Political unrest, misinformation

Supply Chain Attacks

Supply chain attacks now represent a significant cybersecurity threat, which allows hackers to penetrate vital systems through weak points in third-party vendors and software providers with their operations networks (Ohm et al., 2020). Cybercriminals and nation-state organizations use AI techniques to hunt down supply chain vulnerabilities, which they use to execute malicious code, steal sensitive information, or conduct service disruption (Heinbockel et al., 2017). The SolarWinds attack in 2020 served as a notable incident that started when hackers exploited a widely used software update to gain access to various organizations consisting of government agencies and Fortune 500 companies (Martínez and Durán, 2021).AI-driven malware works alongside automated reconnaissance tools to carry out large-scale attacks that produce minimal signs of danger (Wang, 2021). Mathematical processes taught by machine learning enable hackers to anticipate supply chain action patterns, which lead to precise disruption attempts, for example, through AI-based vendor phishing assaults (Reed et al., 2014).

Current Applications of AI in Cybersecurity and the Emergence of Gen AI

AI for Threat Intelligence and Prediction

AI disrupts threat intelligence prediction through predictive analytics coupled with machine learning models and offensive simulations that detect and stop cyber threats at their source. A substantial number of real-time security data streams are analyzed by AI-driven threat intelligence platforms which potential cyberattacks become detectable by the identification of patterns and anomalies (Rodriguez and Costa, 2024). The combination of historical threat data with AI models through predictive analytics allows organizations to identify imminent attack paths enabling proactive security improvements (Alevizos and Dekker, 2024). System defenses become more secure through attack simulations enabled by AI, which permits cybersecurity teams to run vulnerability tests using virtual cyber threats to optimize their incident response procedures (Dingankar, et al., 2024). The AI-based MITRE ATT&CK simulations function to discover enterprise network vulnerabilities that minimize the time it takes to detect intrusions (Sarker, 2024).

AI-Powered Security Operations Centers

The implementation of AI controls Security Operations Centers to automate how dangers are found and how organizations respond to and prevent security breaches in contemporary environments (Khayat et al., 2025). The traditional Security Operations Centers depend on human operators for their functions, which results in delayed cybersecurity threat management. Security Operation Centers powered by AI use machine learning algorithms with natural language processing and real-time threat intelligence to create automated security workflows that improve operational efficiency (Yadav and Roseth, 2025). AI-powered security operation centers use their machines to process vast datasets and find abnormal patterns while driving threat assessment outcomes better than single-human analysis (Khalid and Purdie, 2024). AI-enhanced SOAR platforms utilize AI automatic incident response functionalities, which shorten attack duration and strengthen overall security resilience (Shaheen Afridi, 2024).

Generative AI in Cybersecurity

Gen AI uses its power to drive changes in cybersecurity that benefit security defenses and attack system development. Gen AI-based automation helps cybersecurity operate more swiftly by speeding up threat identification and package updating systems supported by immediate security report generation (Gupta et al., 2023). The ability of genially ill-intentioned individuals to use Gen AI leads to the creation of AI-generated phishing attacks in addition to deepfake fraud and adaptive malware, which threatens traditional security technologies (Mavikumbure et al., 2024). AI performs in cybersecurity requires complete knowledge of its pros and cons, as this knowledge serves to establish effective security AI governance systems (Capodieci et al., 2024).

How AI is Being Leveraged in Critical Infrastructure

Smart Grids & AI-Driven Energy Security

AI technology operates on smart grids to discover abnormal activities through continuous prevention of cyberattacks and delivery of secure energy systems. Modern energy infrastructure becomes more exposed to cyber threat vulnerabilities which include ransomware attacks on power grids. AI predictive maintenance technologies allow organizations to detect equipment failure risks in advance so they take preventive security measures. The analysis of grid data through real-time machine learning algorithms functions to detect strange patterns that would signify cyber intrusions. The security of electric grids gets improved through automated responses to threats that detect potential attacks before they become major incidents to maintain an uninterrupted power supply.

AI for Financial Sector Fraud Detection

AI-powered cyber threats continuously rise in number to target the financial sector through fraudulent transactions and disruptive money laundering practices and identity theft methods. The transaction anomaly detection combined with the dangerous procedure flagging capabilities of AI systems makes financial cybersecurity stronger by blocking unlawful system entry. The self-evolving nature of platform learning models ensures advanced fraud pattern detection, thus improving their detection capabilities. Identity verification attains stronger strength through biometric authentication capabilities implemented by AI to reduce risks caused by unauthorized entries. The safe operation of digital finance relies on real-time risk scoring technology, which AI provides to financial organizations for creating protected online financial environments.

AI in Government & Defense

Government infrastructure implementing cybersecurity Defense systems prove to be high-value targets because of being hit by cyber warfare conducted by nation-states and state-backed espionage programs. The protection of the nation depends significantly on AI since this technology allows immediate threat detection and executes automated cyber safety procedures. AI-enhanced security operation centers investigate security risks by using big data processing to power up their cyber defense systems. Deep learning models provide effective identification of cyberattacks during modern times because foreign adversaries have dedicated efforts to create these threats. The implementation of artificial intelligence systems for encryption secures critical points of classified information by developing robust protection against cyber attackers.

AI for Secure IoT & Smart Cities

The fast growth of IoT devices in smart cities generates essential cybersecurity challenges that lead to large-scale cyberattacks along with data breaches. The security of IoT systems becomes stronger due to AI systems that monitor network traffic for unusual activities while stopping unauthorized commands directed at core operating systems. Predictive AI systems help organizations find weak points in smart city infrastructure, which allows them to prevent potential threats. The standalone operation of autonomous threat mitigation systems powered by artificial intelligence detects threats automatically and sends cyber protection that prevents smart cities from operational failure. Artificial intelligence will remain indispensable for IoT technology expansion as it protects network connections to maintain urban safety.

Guidelines to Mitigate AI Risks to Critical Infrastructure

Regulatory Frameworks for AI Cybersecurity

The standards guarantee that AI security solutions fulfill robust security protocols, which decrease the vulnerability of national infrastructure to cyberattacks. Organizations with governments, continue to enact compliance with these standards because it improves the ability of AI systems to protect against cyber threats.

AI Ethics and Bias Mitigation in Cybersecurity

AI cybersecurity platforms need to function without prejudice to achieve fair and reliable threat identification operations. The reduction of biases in machine learning algorithms through ethical frameworks aims to stop misidentified attacks either as false threats or legitimate events. Artificial intelligence security solutions that contain biases produce cyber threats and security warnings that go unnoticed by users. Systems use multiple information sources together with AI models to detect bias while performing regular inspections on threat surveillance systems controlled by AI systems. Ethical AI systems sustain computer defenses together with clear visibility of operations and fair practices in their operation.

Adversarial AI Defenses

The term adversarial AI describes attacks performed by cyber thieves who reprogram AI system models to breach security protocols. AI-based cybersecurity solutions require adversary training procedures to safeguard against cyber threats by letting AI models experience simulated attacks for defense development.AI defenders use reinforcement learning with GANs to develop defensive measures against attacks performed by AI systems. Modern organizations gain increased hazard mitigation capability against complex infrastructure attacks through the deployment of AI vs. AI security measures.

Zero Trust Security Models in AI-Based Systems

Under the Zero Trust Security Model every entity positioned inside or outside the network lacks default entitlements to trust and therefore requires complete verification in security processes. Security of AI-driven infrastructure depends heavily on this approach because it puts in place strong access measures and continuous authentication protocols along with real-time operation tracking capabilities. AI-based cybersecurity solutions with Zero Trust principles analyze user behavior to identify anomalies which leads to automatic restriction of critical system access for unauthorized entities. Organizations which implement Zero Trust models decrease substantially

the probability of cyber threats taxing AI vulnerabilities in critical infrastructure systems.

Countering Chemical, Biological, Radiological and Nuclear Threats with AI

AI for CBRN Threat Detection & Early Warning Systems

The identification of CBRN threats improves through AI-based detection systems that operate on live data analysis of environmental, biological, and radiological information. Typically, hazardous materials identified through the analysis of sensor data conducted by machine learning programs. Artificial intelligence-based early warning systems provide active warning signals to security agencies, which enables security agencies and emergency responders to generate preemptive responses before hazardous CBRN situations intensify. Artificial intelligence systems with satellite data, drone monitors, and IoT sensors achieve quick threat evaluation and enhance response velocities while raising overall awareness regarding situations.

Machine Learning in CBRN Risk Assessment

Through machine learning technology, risk assessments become more effective because the system reviews historical patterns combined with predictive methods to detect CBRN incidents. The combination of AI systems identifies several threat risk variables with an emphasis on geopolitical temperatures along with industrial operations and environmental modifications, which generate precise intelligence alerts. Through AI-driven simulations, organizations gain the ability to run different attack simulations, which enables them to create specific countermeasures specifically targeted against these attacks. The conducted risk assessments help government agencies and defense organizations with first responder groups, improve their ability to plan for and minimize the effects of CBRN events.

AI-Enabled Predictive Models for Emergency Response

The emergency response plans become optimally effective through the use of AI predictive models, which generate simulated CBRN attack simulations while evaluating different response protocols. Emergency organizations achieve enhanced preparedness through AI-based simulations that test the effectiveness of their decontamination procedures and their evacuation designs as well as their containment measures. The deployment of autonomous drones coupled with AI-powered robotic systems permits reconnaissance duties and contaminated area hazard assessment, which reduces conditions that endanger emergency personnel. Emergency response authorities achieve better coordination, resource management, and real-time decision excellence through AI implementations in their emergency frameworks during CBRN disasters.

Methodology

The author adopts a defined method to explore how AI implements cybersecurity measures for sustaining critical assets while fighting upcoming cyber dangers. A combination of case studies with cybersecurity datasets expert interviews was used by the study to achieve a thorough research analysis. The evaluation of AI-based security systems uses established performance metrics through testing and training of their AI models.

Data Collection

Multiple data sources are used for collected for the study through real-world applications of AI cybersecurity that demonstrate best practices as well as publicly available cybersecurity information sets connected with expert specialist interviews. True-case examples of AI delivery

in national defense with financial sectors and critical infrastructure safeguarding generate hands-on findings.

AI Model Training and Testing

The project use supervised and unsupervised machine learning algorithms, which include neural networks with decision trees and anomaly detection models for implementation. The training step of AI models requires labeled cybersecurity threat data as input, but the testing process measures the capability of AI to classify cyber threats. The analysis includes testing of AI security solutions through methods developed by adversarial AI.

Results & Discussion

Effectiveness of AI-Enhanced Cybersecurity

AI technologies used for cybersecurity operations demonstrate high effectiveness when they detect new cyber threats as well as respond to security threats in real time. The conventional security systems use pre-established rules and signatures, which fail to stop emerging threats because of their set nature. The application of AI uses learning models to detect suspicious patterns that indicate harmful operations. Security Operations Centers using artificial intelligence automation allow rapid threat discovery along with decreased mistakes from human operators. Artificial intelligence systems that use predictive analytic capabilities help organizations stay prepared for security attacks because they predict when such incidents happen. Cybersecurity systems that use AI require ongoing model updating with training campaigns to defend against newly developed and complex digital threats.

Challenges (Adversarial AI, Data Privacy, Regulation)

Multiple obstacles block the general acceptance of AI technology for cybersecurity improvements, although it improves security measures. Security professionals fear adversarial AI because cyber attackers utilize data poisoning as well as evasion attacks and adversarial perturbations to bypass cyber defenses. Security systems that implement AI need significant datasets, which lead to user privacy violations and significant damage to data security. Security organizations follow data privacy rules for their cybersecurity systems to gain benefits from AI technology. These frameworks encounter regulatory obstacles since there are no worldwide standards established for their implementation. Organizations need to follow GDPR, NIST, and ISO/IEC 27001 standards which create barriers for regional implementation standards. The successful implementation of AI cybersecurity depends on appropriate resolutions for the existing concerns in order to keep these systems under responsible control.

Comparative Analysis of AI-Based Solutions

Virtual information security tools use different AI frameworks, which determine their overall performance levels. Decision trees along with support vector machines function under machine learning frameworks as security tools because their ability to detect anomalous patterns and recognize patterns stands exceptional. Security systems equipped with training data of substantial size demonstrate poor ability to detect new types of potential risks. Security systems powered by deep learning frameworks deliver their top results through the identification of complex cyber dangers using convolutional and recurrent neural networks. Computational processing requires high demand because deep learning models need substantial resources for operation. AI technology combined with rule-based security systems creates a solution that

unites AI advantages with human specialist expertise due to their connected implementation. Modern threat detection capability grows stronger when hybrid systems are combined while simultaneously cutting down incorrect alarm frequency. The deployment of AI-driven cybersecurity solutions optimized to fulfill three objectives: security performance and operational efficiency as well as ethical framework adherence for organizational requirements.

Conclusion & Recommendations

National security protection has made artificial intelligence indispensable due to its capabilities for protecting critical infrastructure from contemporary cyberattacks. The implementation of AI technologies in cybersecurity functions helps professionals to discover threats better and deploy automated response systems to raise their preparedness against sophisticated cyberattacks. Expanding AI utilization across the nation for national security needs demands the solution of AI system adversaries as well as data protection rules that address current regulations. The section utilizes predictions about cybersecurity with proposed policies that advocate worldwide interstate efforts for fighting global cyber threats.

Future of AI in National Security

The security outlook regarding AI worldwide becomes more promising since deep learning and machine learning technology working together with generative AI strengthens cybersecurity protection systems. Security solutions powered by AI technology need continuous advancement to produce sufficient real-time prevention of anticipated threats through automated security management. The linkage between AI systems and quantum computing, along with blockchain systems, builds up national cybersecurity capabilities. The expansion of AI capabilities results in more serious cybersecurity threats because improper AI usage increases its danger levels. State security benefits from ethical AI usage and responsible AI deployment for national security matters because it offers public trust as experts work to reduce unintended consequences.

Policy Recommendations

The laws Payers achieve two goals by encouraging AI innovation and guarding citizens from cybersecurity risks. Multiple government agencies should establish security protocols that use NIST best practices along with GDPR standards and ISO/IEC 27001 requirements to maintain appropriate best practice standards. The funding allocation for AI development research include ethical considerations for AI as well as systems that promote open accountability procedures. Security policies establish employee training programs that demonstrate to experts how they can respond to contemporary security threats through AI systems. The public sector, along with government departments create adaptive policies using AI to address novel cyber dangers as well as futuristic cybersecurity solutions.

Need for International Collaboration

Electronic dangers traverse international frontiers, which forces nations to establish combined efforts under intergovernmental cybersecurity programs. International cybersecurity accords, along with standardized AI protection measures, should be implemented through nationwide collective efforts that include exchanging security information. International entities such as INTERPOL plus the United Nations actively support worldwide security cooperation for the field of cybersecurity. Standardized rules for AI cybersecurity management enable the protection of ethical and legal standards throughout different regional laws. Nations working through

international partnerships enhance their collective cybersecurity capabilities for defending critical infrastructure against novel security threats while stopping AI-powered cyberattacks.

Ethics approval statement

Ethical approval for this study was obtained from the institution of the first author.

Submission declaration and verification

The authors declare that the manuscript is original, has not been published elsewhere and is not currently being considered for publication by another journal. All named authors have read and approved for submitting to International Journal of Information Management.

Credit authorship contribution statement

Writing, original draft, review & editing, Supervision, Project administration, Methodology, Investigation, Conceptualization. Validation, Funding acquisition, Formal analysis, Data curation,

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

White, J. (2016). Cyber Threats and Cyber Security: National Security Issues, Policy and Strategies. Global Security Studies, 7(4).

Oruj, Z. (2023). Cyber Security: contemporary cyber threats and National Strategies. Distance Education in Ukraine: Innovative, Normative-Legal, Pedagogical Aspects, (2), 100-116.

Dinicu, A. (2014). Cyber threats to national security. Specific features and actors involved. Scientific Bulletin-Nicolae Balcescu Land Forces Academy, 19(2), 109.

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports, 7, 8176-8186.

Patel, K., & Chudasama, D. (2021). National security threats in cyberspace. National Journal of Cyber Security Law, 4(1), 12-20.

Prasad, R., Rohokale, V., Prasad, R., & Rohokale, V. (2020). Cyber threats and attack overview. Cyber Security: The Lifeline of Information and Communication Technology, 15-31.

Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. SN Computer Science, 2(3), 173.

LAZIĆ, L. (2019, January). Benefit from Ai in cybersecurity. In Proc. 11th Int. Conf. Bus. Inf. Secur.(BISEC) (pp. 103-119).

Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., ... & Choo, K. K. R. (2022). Artificial intelligence in cyber security: research advances, challenges, and opportunities. Artificial Intelligence Review, 1-25.

Carlo, A., Mantı, N. P., WAM, B. A. S., Casamassima, F., Boschetti, N., Breda, P., & Rahloff, T. (2023). The importance of cybersecurity frameworks to regulate emergent AI technologies for space applications. Journal of Space Safety Engineering, 10(4), 474-482.

Jimmy, F. (2021). Emerging threats: The latest cybersecurity risks and the role of artificial intelligence in enhancing cybersecurity defenses. Valley International Journal Digital Library, 1, 564-74.

Stamp, M., Visaggio, C. A., Mercaldo, F., & Di Troia, F. (Eds.). (2022). Artificial Intelligence for Cybersecurity. Springer.

Yigit, Y., Buchanan, W. J., Tehrani, M. G., & Maglaras, L. (2024). Review of generative ai methods in

cybersecurity. arXiv preprint arXiv:2403.08701.
Dhoni, P., & Kumar, R. (2023). Synergizing generative ai and cybersecurity: Roles of generative ai entities, companies, agencies, and government in enhancing cybersecurity. Authorea Preprints.
Krishnamurthy, O. (2023). Enhancing Cyber Security Enhancement Through Generative AI. International Journal of Universal Science and Engineering, 9(1), 35-50.
Teo, Z. L., Ning, C. Q. W., Wong, J. L. Y., & Ting, D. (2024). Cybersecurity in the generative artificial intelligence era. Asia-Pacific Journal of Ophthalmology, 100091.
Vardhan, H., AN, K. S., & Sangers, B. (2025). Future Trends and Trials in Cybersecurity and Generative AI. In Reshaping Cybersecurity With Generative AI Techniques (pp. 465-490). IGI Global.
Jun, Y., Craig, A., Shafik, W., & Sharif, L. (2021). Artificial intelligence application in cybersecurity and cyber defense. Wireless communications and mobile computing, 2021(1), 3329581.
Zhang, Z., Al Hamadi, H., Damiani, E., Yeun, C. Y., & Taher, F. (2022). Explainable artificial intelligence applications in cyber security: State-of-the-art in research. IEEe Access, 10, 93104-93139.
Abbas, N. N., Ahmed, T., Shah, S. H. U., Omar, M., & Park, H. W. (2019). Investigating the applications of artificial intelligence in cyber security. Scient metrics, 121, 1189-1211.
Khan, M. I., Arif, A., & Khan, A. R. A. (2024). The Most Recent Advances and Uses of AI in Cybersecurity. BULLET: Jurnal Multidisiplin Ilmu, 3(4), 566-578.
Hofstetter, M., Riedl, R., Gees, T., Koumpis, A., & Schaberreiter, T. (2020, September). Applications of AI in cybersecurity. In 2020 Second International Conference on Transdisciplinary AI (TransAI) (pp. 138-141). IEEE.
Sikos, L. F. (Ed.). (2018). AI in Cybersecurity (Vol. 151). Springer.
Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion, 97, 101804.
Camacho, N. G. (2024). The role of AI in cybersecurity: Addressing threats in the digital age. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023, 3(1), 143-154.
Salem, A. H., Azzam, S. M., Emam, O. E., & Abohany, A. A. (2024). Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. Journal of Big Data, 11(1), 105.
AMINU, M., AKINSANYA, A., OYEDOKUN, O., & TOSIN, O. (2024). A Review of Advanced Cyber Threat Detection Techniques in Critical Infrastructure: Evolution, Current State, and Future Directions.
Lehto, M. (2022). Cyber-attacks against critical infrastructure. In Cyber security: Critical infrastructure protection (pp. 3-42). Cham: Springer International Publishing.
Rudner, M. (2013). Cyber-threats to critical national infrastructure: An intelligence challenge. International Journal of Intelligence and Counter Intelligence, 26(3), 453-481.
George, A. S., Baskar, T., & Srikaanth, P. B. (2024). Cyber threats to critical infrastructure: assessing vulnerabilities across key sectors. Partners Universal International Innovation Journal, 2(1), 51-75.
Beretas, C. P. (2024). The Most Important Types of Cyber Attacks that France is Expected to Face in the Future and the Cyber Security Measures it Must Implement to Protect Critical Infrastructure, Telecommunication Networks and Personal Data. Universal Library of Engineering Technology, 1(1).
Mitsarakis, K. (2023). Contemporary Cyber Threats to Critical Infrastructures: Management and Countermeasures. Choraś, M., Kozik, R., Flizikowski, A., Hołubowicz, W., & Renk, R. (2016). Cyber threats impacting critical infrastructures. Managing the complexity of critical infrastructures: A modelling and simulation approach, 139-161.
Riggs, H., Tufail, S., Parvez, I., Tariq, M., Khan, M. A., Amir, A., ... & Sarwat, A. I. (2023). Impact, vulnerabilities, and mitigation strategies for cyber-secure critical infrastructure. Sensors, 23(8), 4060.
Leffler, M. P. (1990). National security. The Journal of American History, 77(1), 143-152.
Handley, J. M., & Zeigler, A. H. (2002). A conceptual framework for National Security. American

Diplomacy, 8(4).
Alagappa, M. (1998). Regional Arrangements, the UN, and International Security: A Framework for Analysis. In Beyond UN Subcontracting: Task-Sharing with Regional Security Arrangements and Service-Providing NGOs (pp. 3-29). London: Palgrave Macmillan UK.
McCormack, T. (2008). Power and agency in the human security framework. Cambridge Review of International Affairs, 21(1), 113-128.
Davies, S. E. (2013). National security and pandemics. UN chronicle, 50(2), 20-24.
Scheppele, K. L. (2010). The international standardization of national security law. J. Nat'l Sec. L. & Pol'y, 4, 437.
Aradau, C. (2010). Security that matters: Critical infrastructure and objects of protection. Security dialogue, 41(5), 491-514.
Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S., ... & Baker, T. (2018). Security threats to critical infrastructure: the human factor. The Journal of Supercomputing, 74, 4986-5002.
KHAUSTOVA, V., TIRLEA, M. R., DANDARA, L., TRUSHKINA, N., & BIRCA, I. (2023). DEVELOPMENT OF CRITICAL INFRASTRUCTURE FROM THE POINT OF VIEW OF INFORMATION SECURITY. Strategic Universe Journal/Univers Strategic, (1).
Younis, Y. A., & Kifayat, K. (2013). Secure cloud computing for critical infrastructure: A survey. Liverpool John Moores University, United Kingdom, Tech. Rep, 599-610.
Buttyán, L., Gessner, D., Hessler, A., & Langendoerfer, P. (2010). Application of wireless sensor networks in critical infrastructure protection: challenges and design options [Security and Privacy in Emerging Wireless Networks]. IEEE Wireless Communications, 17(5), 44-49.
Lewis, T. G. (2019). Critical infrastructure protection in homeland security: defending a networked nation. John Wiley & Sons.
Radvanovsky, R., & McDougall, A. (2023). Critical infrastructure: homeland security and emergency preparedness. press.
Stamp, J., Dillinger, J., Young, W., & DePoy, J. (2003). Common vulnerabilities in critical infrastructure control systems. SAND2003-1772C. Sandia National Laboratories.
Abouzakhar, N. (2013). Critical infrastructure cybersecurity: A review of recent threats and violations.
Cyriac, N. T., & Sadath, L. (2019, November). Is Cyber security enough-A study on big data security Breaches in financial institutions. In 2019 4th International Conference on Information Systems and Computer Networks (ISCON) (pp. 380-385). IEEE.
Lee, J., de Guzman, M. C., Wang, J., Gupta, M., & Rao, H. R. (2022). Investigating perceptions about risk of data breaches in financial institutions: A routine activity-approach. Computers & Security, 121, 102832.
Hemphill, T. A., & Longstreet, P. (2016). Financial data breaches in the US retail economy: Restoring confidence in information technology security standards. Technology in Society, 44, 30-38.
Chaturvedi, M., Sharma, S., & Ahmed, G. (2022). Risks of Data Breaches and Mitigating Controls in Financial Sector. In Intelligent Computing Techniques for Smart Energy Systems: Proceedings of ICTSES 2021 (pp. 709-721). Singapore: Springer Nature Singapore.
Weiss, N. E., & Miller, R. S. (2015, February). The target and other financial data breaches: Frequently asked questions. In Congressional Research Service, Prepared for Members and Committees of Congress February (Vol. 4, p. 2015).
Mitchell, S. D., & Banker, E. A. (1997). Private intrusion response. Harv. JL & Tech., 11, 699.
Dasgupta, D. (1999, October). Immunity-based intrusion detection system: A general framework. In Proc. of the 22nd NISSC (Vol. 1, pp. 147-160).
Foo, B., Glause, M. W., Howard, G. M., Wu, Y. S., Bagchi, S., & Spafford, E. H. (2008). Intrusion response

systems: a survey. Information assurance: dependability and security in networked systems, 377-412.
Anwar, S., Mohamad Zain, J., Zolkipli, M. F., Inayat, Z., Khan, S., Anthony, B., & Chang, V. (2017). From intrusion detection to an intrusion response system: fundamentals, requirements, and future directions. algorithms, 10(2), 39.
Terry, J. P. (1999). Responding to Attacks on Critical Computer Infrastructure: What Targets-What Rules of Engagement. Naval L. Rev., 46, 170.
Kakareka, A. (2013). Detecting system intrusions. In Computer and Information Security Handbook (pp. 47-62). Morgan Kaufmann.
Kitchin, R., & Dodge, M. (2020). The (in) security of smart cities: Vulnerabilities, risks, mitigation, and prevention. In Smart cities and innovative Urban technologies (pp. 47-65). Routledge.
Tahirkheli, A. I., Shiraz, M., Hayat, B., Idrees, M., Sajid, A., Ullah, R., ... & Kim, K. I. (2021). A survey on modern cloud computing security over smart city networks: Threats, vulnerabilities, consequences, countermeasures, and challenges. Electronics, 10(15), 1811.
Cardoni, A., Borlera, S. L., Malandrino, F., & Cimellaro, G. P. (2022). Seismic vulnerability and resilience assessment of urban telecommunication networks. Sustainable Cities and Society, 77, 103540.
Al-Turjman, F., Zahmatkesh, H., & Shahroze, R. (2022). An overview of security and privacy in smart cities' IoT communications. Transactions on Emerging Telecommunications Technologies, 33(3), e3677.
Lundbohm, E. (2017). Understanding nation-state attacks. Network Security, 2017(10), 5-8.
Mansfield-Devine, S. (2020). Nation-state attacks: the escalating menace. Network Security, 2020(12), 12-17.
Wentz, L., Starr, S. H., & Kramer, F. (2011). 20. Nation-state Cyber Strategies: Examples from China and Russia. In Cyberpower and national security (pp. 465-488). University of Nebraska Press.
Lewis, J. A. (2002). Assessing the risks of cyber terrorism, cyber war and other cyber threats (p. 12). Washington, DC: Center for Strategic & International Studies.
Nish, A., Naumann, S., & Muir, J. (2022). Enduring cyber threats and emerging challenges to the financial sector. Carnegie Endowment for International Peace.
Johnson, K. N. (2015). Cyber risks: Emerging risk management concerns for financial institutions. Ga. L. Rev., 50, 131.
Wilson, C. (2003). Computer attack and cyber terrorism: Vulnerabilities and policy issues for congress. Focus on Terrorism, 9(1), 1-42.
Ohm, M., Plate, H., Sykosch, A., & Meier, M. (2020). Backstabber's knife collection: A review of open-source software supply chain attacks. In Detection of Intrusions and Malware, and Vulnerability Assessment: 17th International Conference, DIMVA 2020, Lisbon, Portugal, June 24–26, 2020, Proceedings 17 (pp. 23-43). Springer International Publishing.
Heinbockel, W. J., Laderman, E. R., & Serrao, G. J. (2017). Supply chain attacks and resiliency mitigations. The MITRE Corporation, 1-30.
Martínez, J., & Durán, J. M. (2021). Software supply chain attacks, a threat to global cybersecurity: SolarWinds' case study. International Journal of Safety and Security Engineering, 11(5), 537-545.
Wang, X. (2021, November). On the feasibility of detecting software supply chain attacks. In MILCOM 2021-2021 IEEE Military Communications Conference (MILCOM) (pp. 458-463). IEEE.
Reed, M., Miller, J. F., & Popick, P. (2014). Supply chain attack patterns: Framework and Catalog. Office of the Deputy Assistant Secretary of Defense for Systems Engineering, 2.
Rodriguez, P., & Costa, I. (2024). Artificial Intelligence and Machine Learning for Predictive Threat Intelligence in Government Networks. Advances in Computer Sciences, 7(1), 1-10.
Alevizos, L., & Dekker, M. (2024). Towards an AI-enhanced cyber threat intelligence processing pipeline.

Electronics, 13(11), 2021.
Dingankar, S., Shankar, B. M., Kalnawat, A., Sani, A., Dongre, Y. V., & Nagargoje, V. J. (2024, June). Enhancing Cyber Threat Intelligence with AI and ML: An Ensembled Approach. In International Conference on Frontiers of Intelligent Computing: Theory and Applications (pp. 517-526). Singapore: Springer Nature Singapore.
Sarker, I. H. (2024). AI-driven cybersecurity and threat intelligence: cyber automation, intelligent decision-making and explainability. Springer Nature.
Khayat, M., Barka, E., Serhani, M. A., Sallabi, F., Shuaib, K., & Khater, H. M. (2025). Empowering Security Operation Center with Artificial Intelligence and Machine Learning–A Systematic Literature Review. IEEE Access.
Yadav, K. L., & Roseth, T. (2025). AI-Powered Cyber Security: Enhancing SOC Operations with Machine Learning and Blockchain.
Khalid, I., & Purdie, M. S. (2024). AI-Powered SOC Operations: Revolutionizing Cyber Security Incident Response and Management.
Shaheen Afridi, A. A. (2024). AI and Machine Learning-Driven SOC Operations: Transforming Cyber Security Efficiency.
Gupta, M., Akiri, C., Aryal, K., Parker, E., & Praharaj, L. (2023). From chatgpt to threatgpt: Impact of generative ai in cybersecurity and privacy. IEEE Access, 11, 80218-80245.
Mavikumbure, H. S., Cobilean, V., Wickramasinghe, C. S., Drake, D., & Manic, M. (2024, July). Generative AI in cyber security of cyber physical systems: Benefits and threats. In 2024 16th International Conference on Human System Interaction (HSI) (pp. 1-8). IEEE.
Capodieci, N., Sanchez-Adames, C., Harris, J., & Tatar, U. (2024, May). The impact of generative AI and LLMs on the cybersecurity profession. In 2024 Systems and Information Engineering Design Symposium (SIEDS) (pp. 448-453). IEEE.