Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 12:2025
DOI: 10.5281/zenodo.18126209

AI DRIVEN THREAT DETECTION IN PUBLIC SECTOR CYBERSECURITY, INTEGRATING MACHINE LEARNING INTO NATIONAL SECURITY SYSTEMS

MD SAZZAD HOSSAIN
School of Business and Technology, Emporia State University. Email: mhossain@g.emporia.edu, ORCID: 0009-0009-4948-1179

MOHAMMED MAHBUBUR RAHAMAN
Maharishi International University. Email: mrahaman@miu.edu, ORCID: 0009-0001-8317-7949

BIDHAN BISWAS
University of the Cumberlands. Email: bidhanbiswas.cse@gmail.com, ORCID: 0009-0002-0891-5400

Abstract

Public sector institutions are increasingly targeted by advanced persistent threats, ransomware campaigns, supply-chain compromises, and coordinated influence operations that exploit the scale and complexity of national digital services. Conventional signature- and rule-based security controls remain essential but often underperform against novel, stealthy, and fast-evolving attack patterns, particularly where cross-agency visibility and timely threat sharing are limited. This study develops a national-security–oriented perspective on AI-driven threat detection for the public sector, focusing on how machine learning can be operationalized to improve real-time identification, triage, and response across heterogeneous government environments. Drawing on recent advances in AI-enabled threat intelligence, adversarial machine learning, and autonomous cyber defense, the article synthesizes an integrated framework that combines multi-source telemetry ingestion, automated feature engineering, hybrid detection models, and decision-support pipelines aligned with governance constraints. The framework emphasizes: (i) near-real-time threat intelligence fusion and secure inter-agency sharing, (ii) risk-scoring and prioritization for critical infrastructure and mission systems, (iii) resilience against adversarial manipulation and model drift, and (iv) Accountable deployment through human-in-the-loop workflows, auditability, and policy compliance. The analysis highlights implementation considerations for national security systems, including data sovereignty, interoperability across legacy platforms, incident command alignment, and safeguards for civil liberties. The article concludes with design recommendations and a research agenda for deploying scalable, trustworthy, and continuously improving AI-enabled cyber defense capabilities in public sector ecosystems.

Keywords: Artificial Intelligence; Machine Learning; Threat Detection; Public Sector Cybersecurity; National Security Systems; Threat Intelligence Sharing.

1. INTRODUCTION

Public Sector Cybersecurity Threat Landscape

Public sector institutions have become prime targets for sophisticated cyber adversaries due to the scale, sensitivity, and strategic value of government-held data and services. National security systems, critical infrastructure platforms, healthcare networks, financial systems, and e-government services are increasingly exposed to advanced persistent threats (APTs), ransomware-as-a-service campaigns, supply-chain compromises, insider threats, and coordinated cyber-physical attacks.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 12:2025
DOI: 10.5281/zenodo.18126209

Unlike private-sector environments, public sector systems often operate within complex inter-agency ecosystems, legacy infrastructures, and rigid regulatory frameworks, which collectively expand the attack surface and slow defensive adaptation [1], [3], [9].

Recent studies emphasize that cyber threats against government institutions are no longer isolated technical incidents but systemic risks capable of disrupting national stability, economic continuity, and public trust [18], [20], [21]. Threat actors increasingly leverage automation, artificial intelligence, and data-driven reconnaissance to exploit vulnerabilities at scale, overwhelming conventional security operations centers (SOCs) and fragmented threat intelligence mechanisms [4], [24]. As a result, national cybersecurity has shifted from perimeter defense toward resilience-oriented, intelligence-driven, and predictive security models [14], [30].

Limitations of Traditional Rule-Based Security Systems

Traditional cybersecurity defenses in the public sector have historically relied on rule-based systems, static signatures, and predefined access-control policies. While effective against known threats, these approaches are fundamentally reactive and struggle to detect zero-day exploits, polymorphic malware, and stealthy lateral movement within government networks [16], [17].

Signature-based intrusion detection systems and manually curated rulesets require continuous updates and expert intervention, making them ill-suited for high-velocity threat environments and real-time national security operations [10], [15].

Moreover, rule-based systems lack contextual awareness and adaptive learning capabilities, leading to high false-positive rates that overwhelm analysts and delay response actions [7], [11]. In public sector environments where resource constraints, skills shortages, and bureaucratic workflows persist, these inefficiencies translate into prolonged dwell times for attackers and increased systemic risk [5], [26]. Research further demonstrates that static defenses are particularly vulnerable to adversarial evasion techniques, including obfuscation, data poisoning, and mimicry attacks, which exploit deterministic detection logic [8], [23].

Strategic Relevance of AI and Machine Learning to National Security

Artificial intelligence (AI) and machine learning (ML) have emerged as strategically transformative technologies for national cybersecurity, enabling proactive, adaptive, and intelligence-driven defense mechanisms.

AI-driven threat detection systems leverage large-scale data analytics, behavioral modeling, and predictive learning to identify anomalous patterns that traditional tools fail to recognize [2], [4], [25]. By continuously learning from network telemetry, threat intelligence feeds, and historical incidents, ML models can anticipate emerging attack vectors and support near-real-time decision-making in national security contexts [6], [12], [22].

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 12:2025
DOI: 10.5281/zenodo.18126209

Table 1: Public Sector Cybersecurity Threat Landscape and Limitations of Traditional Defenses

Threat Category	Description in Public Sector Context	Limitations of Rule-Based Security Systems	Implications for National Security	Key References
Advanced Persistent Threats (APTs)	Long-term, stealthy intrusions targeting government networks, defense systems, and critical infrastructure using multi-stage attack campaigns	Signature-based systems fail to detect unknown attack vectors and lateral movement patterns	Prolonged attacker dwell time, intelligence leakage, and systemic national security risks	[1], [3], [9], [18], [24]
Ransomware and Supply-Chain Attacks	Large-scale ransomware campaigns and compromised third-party software affecting public services and inter-agency systems	Static rules cannot adapt to rapidly evolving malware variants and obfuscation techniques	Disruption of essential public services and erosion of public trust	[7], [10], [15], [20], [27]
Insider Threats	Malicious or negligent actions by authorized users within government institutions	Rule-based access controls lack behavioral context and anomaly awareness	Unauthorized data exposure and mission-critical system compromise	[5], [11], [13], [26], [29]
Zero-Day Exploits	Exploitation of previously unknown vulnerabilities in government and critical infrastructure systems	Dependence on known signatures makes detection ineffective until post-disclosure	High-impact breaches before mitigation measures are deployed	[4], [16], [17], [25], [30]
Adversarial and Evasive Attacks	AI-assisted evasion, data poisoning, and mimicry techniques designed to bypass deterministic defenses	Deterministic logic is highly vulnerable to adversarial manipulation	Degradation of detection accuracy and erosion of defensive confidence	[8], [19], [23], [24], [27]

For public sector cybersecurity, AI offers critical advantages in inter-agency threat intelligence sharing, automated risk assessment, and coordinated response orchestration across heterogeneous systems [1], [9], [13]. Studies highlight that AI-enabled cyber defense enhances national resilience by reducing response latency, improving situational awareness, and enabling scalable protection for critical infrastructure and mission-critical services [18], [20], [27]. Furthermore, hybrid AI approaches combining supervised, unsupervised, and deep learning techniques have demonstrated superior performance in detecting advanced threats while maintaining operational flexibility and governance compliance [19], [23], [24].

Research Objectives and Contributions

Despite growing interest in AI-driven cybersecurity, significant gaps remain in the systematic integration of machine learning within public sector and national security systems. Existing research often focuses on isolated technical solutions or enterprise contexts, with limited attention to governance, interoperability, accountability, and policy

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 12:2025
DOI: 10.5281/zenodo.18126209

constraints unique to government environments [21], [28], [30]. Additionally, challenges related to adversarial robustness, data sovereignty, ethical oversight, and human–AI collaboration continue to hinder large-scale deployment in national security infrastructures [8], [17], [19].

In response, this article aims to:

1. **Critically examine** the evolving cybersecurity threat landscape confronting public sector and national security systems [1], [3], [9].
2. **Analyze the limitations** of traditional rule-based defenses and justify the need for AI-driven approaches [10], [16], [26].
3. **Synthesize current research** on machine learning techniques for threat detection, intelligence sharing, and risk assessment in national cybersecurity contexts [2], [4], [14], [25].
4. **Propose an integrated conceptual framework** for AI-driven threat detection tailored to public sector cybersecurity, emphasizing governance, resilience, and operational scalability [6], [20], [30].

By addressing these objectives, the study contributes a structured, policy-aware perspective on deploying machine learning within national security systems, bridging the gap between technical innovation and public sector cybersecurity practice.

2. LITERATURE REVIEW AND THEORETICAL FOUNDATIONS

a. AI in Threat Intelligence and Detection

Contemporary public sector cyber defense increasingly frames *threat intelligence* as a continuous cycle of collection, fusion, analysis, dissemination, and action where speed, credibility, and interoperability are decisive. Recent scholarship positions AI as an enabler of this intelligence cycle by automating ingestion of heterogeneous signals (logs, endpoint telemetry, network flows, OSINT, and classified feeds), extracting actionable indicators, and prioritizing threats for operational response [1], [4], [9], [24]. In national security settings, the strategic value of AI is frequently tied to its ability to support near-real-time threat sharing across agencies and to reduce latency between detection and coordinated response actions [1], [6], [20].

A key theme in the recent literature is that AI-supported threat intelligence shifts security operations from reactive alert handling toward predictive defense where models forecast likely attacker behaviors and recommend response options based on learned patterns [9], [18], [24]. This direction is further reinforced by work emphasizing autonomous and hybrid AI approaches for identifying APT-like behaviors that are not easily captured by static indicators [23], [24]. National-level cyber defense narratives increasingly emphasize “intelligent threat prediction and response” as a capability layer for strengthening resilience across critical government systems [9], [20].

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 12:2025
DOI: 10.5281/zenodo.18126209

Importantly, the threat intelligence literature also recognizes a reliability challenge: the public sector often depends on cross-organizational intelligence that varies in fidelity and timeliness, creating decision risk during incident response. AI-driven analytics are therefore frequently proposed as mechanisms to normalize and score intelligence quality, reduce noise, and enable actionable prioritization under resource constraints [6], [13], [25]. In this direction, integrated pipelines that combine data analytics with intelligence-sharing protocols are presented as central to modern public sector cybersecurity posture [1], [6], [20].

b. Machine Learning Models in Cybersecurity

The ML cybersecurity literature converges on the view that no single model family is sufficient for modern threat detection; instead, robust detection requires layered methods across supervised learning, unsupervised anomaly detection, deep learning, and hybrid ensembles. Reviews of state-of-the-art techniques highlight the breadth of ML-driven detection across malware analysis, network intrusion detection, phishing detection, and behavioral anomaly identification [4], [17]. Within these categories, ML is primarily justified on two grounds: (i) scalability for high-volume telemetry, and (ii) adaptability to evolving attack patterns beyond fixed signatures [2], [7], [16].

Across recent studies, supervised models are commonly positioned as effective for classification tasks when high-quality labeled data exist (e.g., known malware families, known attack traces), while unsupervised methods are emphasized for uncovering unknown or emerging threats—especially in environments where labels are scarce or unreliable [7], [17]. Deep learning approaches are repeatedly discussed as particularly relevant for complex temporal and multivariate signals (e.g., sequence-based detection from logs or network flows), although operationalization challenges compute cost, explainability, drift are recognized [25], [29].

The literature also emphasizes end-to-end frameworks that combine multiple ML components into operational security workflows. AI-driven frameworks for advanced threat detection and prevention typically incorporate feature extraction, model selection, continuous learning, and response automation often within a SOC-aligned pipeline [2], [7], [11]. In public sector contexts, these frameworks are increasingly tied to “real-time” requirements and decision support, including risk scoring for prioritization and rapid containment [14], [25].

A rapidly growing subarea is *adversarial machine learning*, motivated by the reality that sophisticated adversaries can exploit ML systems through evasion, poisoning, and manipulation of decision boundaries. Work focusing on adversarial ML strategies argues that cybersecurity ML must be designed with threat-model awareness, robustness evaluation, and defensive hardening mechanisms (e.g., adversarial training, anomaly-aware feature sets, and secure ML pipelines) [8], [23]. This concern is especially acute for national security systems, where ML failure modes may translate into severe operational consequences and strategic risk [9], [20].

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 12:2025
DOI: 10.5281/zenodo.18126209

Another prominent stream addresses *AI + big data analytics* in cybersecurity. Here, the core claim is that large-scale analytics when paired with ML can strengthen cybersecurity frameworks by improving situational awareness, enabling correlation across disparate data sources, and accelerating incident response cycles [6], [7], [20]. This is consistent with broader reviews that position AI-driven cybersecurity as a field anchored in security intelligence modeling and data-centric defense practices [17].

c. Public Sector and National Security System Challenges

While enterprise cybersecurity research provides useful detection techniques, public sector environments introduce constraints that materially alter how AI/ML can be deployed. First, public sector infrastructures are frequently heterogeneous and legacy-heavy, with fragmented identity systems, uneven telemetry coverage, and complex procurement and compliance processes.

These conditions complicate standardized data collection and undermine the stability assumptions that many ML pipelines require [18], [20]. Second, national security systems often operate under heightened requirements for confidentiality, data sovereignty, and cross-agency access control conditions that can limit centralized data aggregation and impede model training at scale [1], [21], [30].

Third, the public sector is often characterized by high accountability expectations, including auditability of decisions, civil-liberties safeguards, and strict governance over automated decision-making. These factors intensify the need for explainable outputs, traceable model behavior, and clearly bounded automation (human-in-the-loop controls) [21], [30]. In addition, operational response in public sector settings can involve multi-stakeholder coordination, where detection is only valuable if it can be translated into aligned action under incident command structures making integration into workflows as important as model accuracy [20], [24].

Fourth, sector-specific threat environments matter. For example, healthcare cybersecurity requires multimodal detection and response strategies due to the diversity of clinical systems and sensitive patient data, making real-time AI integration both attractive and difficult [12].

Financial cybersecurity, similarly, emphasizes fraud detection, systemic risk, and regulatory constraints, with research advocating AI-driven fraud analytics as a core capability but acknowledging governance demands and adversarial dynamics [15], [26]. Critical industries and “national infrastructure” contexts where availability and integrity are paramount are repeatedly highlighted as settings where AI-driven detection must be engineered for resilience and continuity, not only classification performance [10], [20].

Finally, cyber-physical system (CPS) environments introduce unique operational risks because threats can translate into physical disruption. Work on AI integration in CPS highlights detection-and-response requirements that span both digital telemetry and operational technology signals, reinforcing the need for hybrid detection architectures and strict safety governance [19], [30].

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 12:2025
DOI: 10.5281/zenodo.18126209

d. Gaps in Integration, Governance, and Real-Time Response

Despite a strong body of work on AI methods for threat detection, the literature identifies persistent gaps that are especially significant for public sector and national security deployments.

Integration gap (technical-to-operational): Many studies present model-level performance without fully specifying deployment pathways: data pipelines, orchestration, incident response integration, and lifecycle management. Framework proposals exist, but practical issues interoperability across agencies, legacy systems, and secure intelligence sharing remain insufficiently operationalized in many contributions [2], [6], [20], [28]. In particular, intelligence-sharing studies point to the need for secure, standardized, and policy-aligned exchange mechanisms that can support real-time national coordination [1], [24].

Governance gap (accountability and oversight): National security applications demand governance mechanisms for decision authority, auditability, and policy compliance. However, much of the ML cybersecurity literature remains solution-centric rather than governance-centric, leaving unresolved questions about responsible automation, oversight models, and risk ownership when AI-driven systems influence high-stakes decisions [21], [30]. This issue becomes more acute under adversarial ML conditions, where attackers may intentionally manipulate models and thereby undermine trust in automated outputs [8], [23].

Real-time response gap (from detection to action): Real-time threat detection is frequently claimed but less frequently achieved end-to-end, especially in environments with constrained telemetry, fragmented data access, and limited automation authority. Work focusing on real-time crisis response and infrastructure protection argues for AI-driven analytics as a national resilience capability, but highlights that response latency, workflow friction, and cross-agency coordination are persistent bottlenecks [20]. Similarly, risk assessment studies emphasize that predictive models must connect to mitigation actions and governance controls to deliver operational value at national scale [5], [14], [25].

Trustworthiness gap (robustness, drift, and validation): Reviews emphasize model drift, changing attacker tactics, data imbalance, and adversarial pressure as core reasons why ML systems degrade over time if not continuously validated and updated [4], [17]. This motivates ongoing research toward autonomous or hybrid AI approaches that can sustain detection efficacy while maintaining accountability, particularly for APT detection [23]. Additionally, the blockchain–AI synergy literature frames decentralization and integrity controls as potential enablers for trusted intelligence sharing and tamper-resistant logging, but practical governance and interoperability considerations remain open [27].

Synthesis (positioning of this study): Taken together, the literature supports the argument that public sector AI-driven threat detection must be treated as a *socio-technical system* comprising models, data pipelines, governance controls, and operational

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 12:2025
DOI: 10.5281/zenodo.18126209

response protocols—rather than as a standalone classifier. This study therefore builds on AI threat intelligence and ML detection research [1], [2], [4], [7], [24], strengthens alignment with national resilience and infrastructure protection perspectives [9], [20], and explicitly elevates integration and governance considerations emphasized in national security frameworks and data-driven eGovernment infrastructures [21], [30].

3. AI-DRIVEN THREAT DETECTION ARCHITECTURE FOR PUBLIC SECTOR SYSTEMS

a. Conceptual System Architecture

An AI-driven threat detection capability for public sector cybersecurity must be engineered as an end-to-end socio-technical architecture that aligns machine learning components with national security mission needs, inter-agency workflows, and governance constraints. The literature converges on a layered approach in which data acquisition, analytics, detection, and response orchestration are tightly coupled, enabling rapid translation of signals into actionable decisions [2], [4], [7].

In national security settings, the architecture must also explicitly support trusted intelligence sharing and cross-domain situational awareness, as threat information often resides across multiple agencies and critical infrastructure operators [1], [9], [20].

Figure-level conceptualization (to be included later as a diagram) can be expressed as six functional layers:

1. **Telemetry and Intelligence Sources Layer** (endpoints, networks, cloud, OT/CPS, identity, threat feeds)
2. **Secure Data Ingestion and Normalization Layer** (streaming + batch, standardization, enrichment)
3. **Feature Engineering and Representation Layer** (behavioral, temporal, graph-based, multi-modal)
4. **Detection and Analytics Layer** (hybrid ML models: supervised, unsupervised, deep learning, ensembles)
5. **Decision Support and Response Orchestration Layer** (risk scoring, playbooks, human-in-the-loop)
6. **Governance, Assurance, and Continuous Improvement Layer** (auditing, drift monitoring, adversarial defense)

This architecture reflects broad findings that AI-driven cybersecurity requires both intelligence modeling and operational integration rather than isolated model deployment [17].

It also aligns with research emphasizing predictive threat intelligence and response for national security outcomes, where the objective is resilience and mission continuity rather than purely technical detection rates [9], [18], [20].

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 12:2025
DOI: 10.5281/zenodo.18126209

b. Data Ingestion, Feature Extraction, and Model Training

Data Ingestion and Normalization

Public sector cyber defense requires multi-source ingestion because threats manifest across endpoints, networks, applications, identity systems, and (increasingly) cyber-physical environments. AI-driven approaches typically rely on high-volume telemetry streams—such as authentication logs, process and file activities, DNS queries, network flows, and cloud audit trails—augmented by external threat intelligence feeds and incident reports [4], [6], [7]. For critical infrastructure and national security systems, ingestion must also accommodate OT/CPS signals (e.g., industrial control logs, sensor states), which expands both the data variety and the safety implications of detection errors [19], [30].

The literature supports adopting a *secure data lakehouse or federated analytics layer* as the canonical security data substrate. Big data analytics is frequently positioned as foundational to scaling AI-driven threat detection by enabling correlation and enrichment across disparate sources in near real time [6], [20]. However, public sector constraints (classified domains, legal restrictions, data sovereignty) often limit centralized data consolidation, motivating controlled federation and tiered access models [1], [21].

Feature Extraction and Representation

Feature engineering for public sector systems should prioritize behavioral and contextual representations that generalize beyond known signatures. Research on holistic AI/ML cybersecurity integration emphasizes that feature pipelines must fuse host, network, and identity signals to reduce blind spots and support robust detection [7]. Core feature families include:

- **Behavioral features:** process lineage, privilege escalation indicators, unusual access sequences [4], [17]
- **Temporal features:** event timing irregularities, burst patterns, session anomalies [25], [29]
- **Relational/graph features:** user–device–resource interaction graphs capturing lateral movement and coordinated activity [30]
- **Intelligence enrichment features:** reputation scores, IOC mappings, TTP alignments, and confidence-weighted threat feed signals [1], [24]

In adversarial settings, feature design must incorporate robustness principles, as deterministic or brittle features can be intentionally manipulated. Adversarial ML studies underscore that attackers can evade models by perturbing inputs or poisoning training data; therefore, feature pipelines should include tamper-resistance, redundancy, and anomaly-aware validation checks [8], [23].

Model Training and Continuous Learning

Model training in public sector environments must address label scarcity, concept drift, and operational heterogeneity. As a result, hybrid detection stacks are increasingly

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 12:2025
DOI: 10.5281/zenodo.18126209

recommended: supervised classification for known threats, unsupervised anomaly detection for novel behaviors, and deep learning for complex patterns in large telemetry streams [4], [17], [25]. Recent frameworks for advanced threat detection and prevention highlight the effectiveness of combining models and continuously retraining using newly observed incidents and feedback from analysts [2], [11].

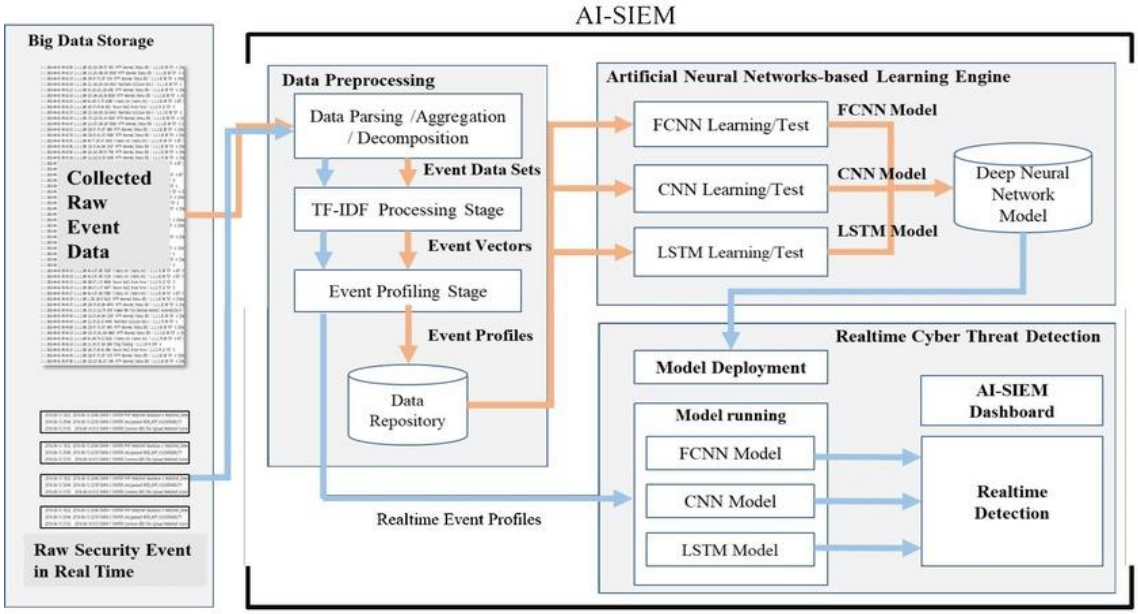

Figure 1: AI-Driven Threat Detection Architecture for Public Sector Cybersecurity

To align with national security priorities, training pipelines should embed **risk assessment outputs** that support prioritization of mission-critical assets and threats. Risk-oriented modeling is repeatedly highlighted as essential for defense and critical infrastructure projects, where the consequence of failure varies widely across system components [5], [14], [25]. In practical terms, this means models should generate calibrated risk scores and confidence measures rather than binary alerts, enabling structured escalation, triage, and resource allocation [14], [20].

4. MACHINE LEARNING TECHNIQUES FOR NATIONAL SECURITY CYBER DEFENSE

i. Supervised, Unsupervised, and Deep Learning Approaches

Machine learning techniques applied to national security cyber defense are typically categorized into supervised learning, unsupervised learning, and deep learning approaches, each addressing distinct detection and operational requirements. The literature consistently emphasizes that **no single technique is sufficient in isolation**, particularly in public sector environments characterized by evolving threats, heterogeneous systems, and limited labeled data [4], [17], [29]. Consequently, hybrid and layered ML strategies are increasingly advocated for national security contexts [2], [9], [20].

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 12:2025
DOI: 10.5281/zenodo.18126209

Supervised learning models such as decision trees, random forests, support vector machines, and gradient-boosting classifiers are widely used for classifying known attack patterns, malware families, and fraud behaviors when high-quality labeled datasets are available [7], [11], [15]. In national security systems, supervised models are particularly valuable for high-confidence detection of recurring threats and policy-defined risk categories, including known APT indicators and regulated compliance violations [1], [25]. However, their reliance on historical labels constrains effectiveness against novel threats and rapidly evolving attack tactics, a limitation repeatedly noted in public sector cybersecurity studies [16], [26].

Unsupervised learning approaches, including clustering, density-based methods, and statistical anomaly detection, address this limitation by identifying deviations from baseline behavior without requiring labeled data. Such methods are frequently positioned as essential for detecting zero-day exploits, insider threats, and stealthy lateral movement in government networks [7], [17]. In public sector systems where labeling is often incomplete due to data sensitivity or classification unsupervised models provide an adaptive mechanism for surfacing suspicious activity that would otherwise evade deterministic controls [5], [18].

ii. Real-Time Analytics and Predictive Threat Modeling

Real-time analytics is a defining requirement for national security cyber defense, where delayed detection can translate into strategic harm. AI-driven cybersecurity research increasingly frames ML models not only as detectors but as *predictive instruments* capable of anticipating threat evolution and supporting proactive defense [9], [18], [24]. Predictive threat modeling leverages historical incidents, behavioral patterns, and threat intelligence to forecast likely attack vectors, targets, and escalation paths [1], [25].

Table 2: Comparative Analysis of Machine Learning Techniques for National Security Cyber Defense

ML Technique	Primary Role	Key Advantage	Main Limitation	Representative References
Supervised Learning	Detection of known threats	High precision for labeled attacks	Poor performance on unknown threats	[7], [11], [15], [25]
Unsupervised Learning	Anomaly and insider threat detection	No labeled data required	Higher false positives	[5], [17], [18], [23]
Deep Learning	Real-time and complex pattern detection	Handles large-scale, high-dimensional data	Limited explainability	[4], [25], [29], [30]
Hybrid / Ensemble Models	Comprehensive threat detection	Balances accuracy and adaptability	Higher integration complexity	[2], [9], [14], [20]
ML-Based Risk Assessment	Decision support and prioritization	Aligns alerts with mission impact	Depends on contextual data quality	[5], [14], [20], [26]

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 12:2025
DOI: 10.5281/zenodo.18126209

Machine learning enables real-time analytics by processing continuous data streams and updating detection outputs dynamically as new evidence emerges. Studies focusing on AI-driven threat intelligence emphasize that streaming ML pipelines significantly reduce response latency and improve cross-agency coordination by enabling early warning and preemptive mitigation [1], [6], [20]. In this context, ML models act as force multipliers for constrained public sector security teams, automating triage and prioritization in environments characterized by alert overload [7], [11].

iii. Risk Assessment and Decision-Support Mechanisms

Beyond detection, national security cyber defense requires ML systems to support **risk-based decision-making**. Risk assessment models translate technical signals into prioritized insights aligned with mission impact, asset criticality, and threat severity [5], [14]. The literature consistently emphasizes that national security stakeholders require *actionable intelligence*, not raw alerts, particularly in crisis or multi-incident scenarios [20]. AI-driven risk assessment frameworks typically integrate ML detection outputs with contextual data such as system importance, interdependencies, and threat confidence to generate composite risk scores [14], [25]. These scores support decision-support mechanisms within SOCs and national incident command structures, enabling structured escalation, resource allocation, and coordinated response [2], [7]. In defense and critical infrastructure projects, such ML-enabled risk prediction has been shown to improve mitigation planning and reduce operational uncertainty [5], [14].

5. DISCUSSION

The findings synthesized across the preceding sections reinforce a central argument in the contemporary cybersecurity literature: **AI-driven threat detection is no longer an optional enhancement for public sector cybersecurity but a strategic necessity for national security systems**. The discussion below interprets these findings through operational, policy, and strategic lenses, emphasizing implications specific to government and national security contexts rather than generic enterprise deployments.

i. Operational Implications for Public Sector Cyber Defense

From an operational standpoint, the literature consistently demonstrates that AI and machine learning materially improve the **speed, scale, and adaptability** of threat detection in public sector environments [1], [4], [9]. Unlike traditional rule-based systems, ML-enabled detection can process high-volume telemetry in near real time, reducing alert fatigue and shortening the window between intrusion and response [7], [11], [20]. This capability is particularly consequential for national security systems, where delayed detection may lead to intelligence compromise, service disruption, or cascading failures across critical infrastructure [18], [24].

However, the discussion also highlights that **operational value depends less on model accuracy alone and more on workflow integration**. Studies emphasize that ML outputs must be embedded within SOC processes, incident command structures, and inter-agency coordination mechanisms to translate detection into effective action [2], [20].

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 12:2025
DOI: 10.5281/zenodo.18126209

Without such integration, even high-performing models risk becoming isolated analytical tools with limited real-world impact. This reinforces the need for AI-driven systems that prioritize actionable risk scoring and decision support rather than raw alert generation [14], [25].

ii. Strategic Value for National Security and Resilience

At the strategic level, AI-driven cybersecurity contributes to **national resilience** by enabling predictive defense and collective situational awareness. Predictive threat modeling and intelligence fusion allow security leaders to anticipate adversary behavior, allocate resources proactively, and coordinate defense across agencies and sectors [1], [9], [18]. The literature frames this capability as a shift from perimeter-centric defense toward intelligence-centric security, where learning systems continuously adapt to evolving threats [17], [20].

This strategic value is amplified in critical infrastructure and cyber-physical systems, where disruptions can have physical, economic, and societal consequences [19], [30]. AI-driven analytics, when aligned with risk assessment frameworks, enable prioritization of assets based on mission criticality and potential impact, supporting more informed national security decision-making [5], [14]. The discussion thus positions machine learning not merely as a detection tool but as an enabler of **strategic cyber governance** at the national level [21].

iii. Governance, Accountability, and Ethical Considerations

Despite its advantages, the literature is unequivocal that **AI deployment in public sector cybersecurity introduces significant governance and ethical challenges**. Automated threat detection intersects with privacy, civil liberties, and accountability concerns, particularly when surveillance-scale data and autonomous analytics are involved [21], [30]. As a result, studies emphasize the importance of human-in-the-loop models, explainability, and auditable decision processes to preserve legitimacy and public trust [19], [21].

Governance challenges are further compounded by adversarial machine learning risks. Research highlights that sophisticated attackers can intentionally manipulate ML systems through evasion or data poisoning, undermining detection reliability and decision confidence [8], [23]. This necessitates treating ML pipelines themselves as protected assets, subject to continuous validation, red teaming, and lifecycle governance [4], [17]. In national security contexts, failure to address these issues may erode institutional trust in AI-driven defenses, limiting their adoption despite technical promise [9], [20].

iv. Interoperability and Cross-Agency Coordination

A recurring theme across the literature is the **interoperability gap** in public sector cybersecurity. National security ecosystems are inherently multi-organizational, involving defense agencies, civilian institutions, healthcare systems, financial regulators, and critical infrastructure operators. AI-driven threat detection can only deliver systemic benefits if intelligence is shared securely and acted upon collectively [1], [20], [24].

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 12:2025
DOI: 10.5281/zenodo.18126209

The discussion suggests that standardized data models, shared taxonomies, and policy-driven intelligence exchange mechanisms are as important as ML algorithms themselves [6], [28]. Emerging approaches, including decentralized trust mechanisms and secure provenance tracking, show promise but remain constrained by governance and integration challenges in government environments [27]. Consequently, interoperability should be treated as a first-order design requirement rather than a post-deployment consideration [21], [30].

6. CONCLUSION

This article examined AI-driven threat detection in public sector cybersecurity with a focus on integrating machine learning into national security systems. Across the reviewed literature, a consistent conclusion emerges: traditional rule-based and signature-driven defenses remain useful for known threats but are structurally limited in detecting novel, stealthy, and fast-evolving attack behaviors that increasingly characterize public sector threat environments [16], [17]. In contrast, AI and machine learning enable adaptive detection, continuous intelligence fusion, and near-real-time analytics that can materially improve situational awareness and response readiness in national security contexts [1], [4], [9], [20]. The analysis further shows that effective national security cyber defense requires **layered ML techniques** rather than a single-method approach. Supervised models support high-confidence detection of known threats, unsupervised methods provide coverage for unknown and anomalous behaviors, and deep learning offers advantages for complex and large-scale telemetry analysis when deployed with appropriate governance controls [4], [7], [25], [29]. However, the decisive factor for success is not model selection alone but the extent to which ML outputs are integrated into operational workflows, inter-agency threat intelligence sharing, and risk-based decision support mechanisms [14], [20], [24]. The article also highlighted that public sector deployment introduces non-negotiable governance requirements. Accountability, auditability, interoperability, and civil-liberties safeguards must be designed into AI-driven threat detection architectures to preserve legitimacy and ensure reliable operational use [21], [30]. In addition, adversarial machine learning risks require explicit hardening of the ML lifecycle, including robust feature design, continuous validation, and protection against evasion and poisoning tactics [8], [23].

References

1) Miah, M. N. I., Uddin, M. J., & Ahmed, M. W. (2025). AI-Driven Threat Intelligence: Evaluating Machine Learning for Real-Time Cyber Threat Sharing Among US National Security Agencies. *Journal of Computer Science and Technology Studies*, *7*(8), 300-313. https://doi.org/10.32996/jcsts.2025.7.8.34

2) Malik, A., Arshid, K., Noonari, N., & Munir, R. (2025). Artificial Intelligence-Driven Cybersecurity Framework Using Machine Learning for Advanced Threat Detection and Prevention. *Sch J Eng Tech*, *6*, 401-423. https://doi.org/10.36347/sjet.2025.v13i06.005

3) Banerjee, R., Islam, M. M., Mitra, R., Mukherjee, D., Nath, S., & Biswas, M. (2025). The Impact of Artificial Intelligence on Threat Detection and Response in Cybersecurity. *Cuestiones de Fisioterapia*, *54*(3), 2200-2210. https://doi.org/10.48047/e3b7qf51

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 12:2025
DOI: 10.5281/zenodo.18126209

4) Mohamed, N. Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms. *Knowl Inf Syst* **67**, 6969–7055 (2025). https://doi.org/10.1007/s10115-025-02429-y

5) Arif, M. H., Rabby, H. R., Nadia, N. Y., Tanvir, M. I. M., & Al Masum, A. (2025). AI-Driven Risk Assessment in National Security Projects: Investigating machine learning models to predict and mitigate risks in defense and critical infrastructure projects. *Journal of Computer Science and Technology Studies*, *7*(2), 71-85. https://doi.org/10.32996/jcsts.2025.7.2.6

6) The Role of Artificial Intelligence-Driven Big Data Analytics in Strengthening Cybersecurity Frameworks for Critical Infrastructure. (2023). *Global Research Perspectives on Cybersecurity Governance, Policy, and Management*, *7*(11), 12-25. http://hammingate.com/index.php/GRPCGPM/article/view/2023-11-07

7) Raji, A., Olawore, A., Mustapha, A., & Joseph, J. (2023). Integrating Artificial Intelligence, machine learning, and data analytics in cybersecurity: A holistic approach to advanced threat detection and response. *World Journal of Advanced Research and Reviews*, *20*(3), 2005-2024. https://doi.org/10.30574/wjarr.2023.20.3.2741

8) Ijiga, O. M., Idoko, I. P., Ebiega, G. I., Olajide, F. I., Olatunde, T. I., & Ukaegbu, C. (2024). Harnessing adversarial machine learning for advanced threat detection: AI-driven strategies in cybersecurity risk assessment and fraud prevention. *J. Sci. Technol*, *11*, 001-024.
9) https://doi.org/10.53022/oarjst.2024.11.1.0060

10) Kunaparaju, C. (2025). AI-Driven Cyber Defense Systems: Strengthening National Security through Intelligent Threat Prediction and Response. *Algora*, *2*(1), 1–30. https://doi.org/10.63084/algora.v2i1.50

11) Kancherla, V. M. (2021). AI and Cybersecurity: Strengthening National Infrastructure with AI-Driven Threat Detection. *International Journal of Emerging Trends in Computer Science and Information Technology*, *2*(1), 55-62. https://doi.org/10.63282/3050-9246.IJETCSIT-V2I1P107

12) Abiodun Sunday Adebayo, Naomi Chukwurah, & Olanrewaju Oluwaseun Ajayi. (2025). Artificial Intelligence and Machine Learning Algorithms for Advanced Threat Detection and Cybersecurity Risk Mitigation Strategies. *Engineering and Technology Journal*, *10*(3), 4080–4094. https://doi.org/10.47191/etj/v10i03.18

13) Ali, T. E., Ali, F. I., Eyvazov, F., & Zoltán, A. D. (2025). Integrating AI Models for Enhanced Real-Time Cybersecurity in Healthcare: A Multimodal Approach to Threat Detection and Response. *Procedia Computer Science*, *259*, 108-119. https://doi.org/10.1016/j.procs.2025.03.312

14) Ankhi, R. B. (2025). Leveraging Business Intelligence and AI-Driven Analytics to Strengthen US Cybersecurity Infrastructure. *International Journal of Engineering & Extended Technologies Research (IJEETR)*, *7*(2), 9637-9652. https://doi.org/10.15662/IJEETR.2025.0702003

15) Faruk, M. I., Plabon, F. W., Saha, U. S., & Hossain, M. D. (2025). AI-Driven Project Risk Management: Leveraging Artificial Intelligence to Predict, Mitigate, and Manage Project Risks in Critical Infrastructure and National Security Projects. *Journal of Computer Science and Technology Studies*, *7*(6), 123-137. https://doi.org/10.32996/jcsts.2025.7.6.16

16) Ejiofor, O. E. (2023). A comprehensive framework for strengthening USA financial cybersecurity: integrating machine learning and AI in fraud detection systems. *European Journal of Computer Science and Information Technology*, *11*(6), 62-83. https://doi.org/10.37745/ejcsit.2013/vol11n66283

17) Sunkara, G. (2021). AI Powered Threat Detection in Cybersecurity. *International Journal of Humanities and Information Technology*, (Special 1), 1-22. https://doi.org/10.21590/ijhit3.1.1

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 12:2025
DOI: 10.5281/zenodo.18126209

18) Sarker, I.H., Furhad, M.H. & Nowrozy, R. AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions. *SN COMPUT. SCI.* **2**, 173 (2021). https://doi.org/10.1007/s42979-021-00557-0

19) Marapu, N. R. (2022). Future-proofing national cybersecurity: the role of AI in proactive threat hunting and framework optimization. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, *3*(4), 27-37. https://doi.org/10.63282/3050-9262.IJAIDSML-V3I4P104

20) Al Waro, M. N. A. L. (2024). Enhancing Security through Intelligent Threat Detection and Response: The Integration of Artificial Intelligence in Cyber-Physical Systems. *Security Intelligence Terrorism Journal (SITJ)*, *1*(1), 1-11. https://doi.org/10.70710/sitj.v1i1.1

21) Mintoo, A. A., Saimon, A. S. M., Bakhsh, M. M., & Akter, M. (2022). National Resilience through Ai-Driven Data Analytics and Cybersecurity for Real-Time Crisis Response and Infrastructure Protection. *American Journal of Scholarly Research and Innovation*, *1*(01), 137-169. https://doi.org/10.63125/sdz8km60

22) Atif, M., & Alamgir, A. (2025). A Comprehensive Framework for Enhancing National Security through AI. *Journal of Political Stability Archive*, *3*(3), 1443-1462. https://doi.org/10.63468/jpsa.3.3.96

23) Shimu, F. (2025). Intelligent Cybersecurity Framework Machine Learning-Driven Data Protection and Threat Intelligence Integration for Modern Digital Communications. *International Journal of Applied Mathematics*, *38*(8s), 620-632. https://doi.org/10.12732/ijam.v38i8s.595

24) Hernández-Rivas, A., Morales-Rocha, V., Sánchez-Solís, J.P. (2024). Towards Autonomous Cybersecurity: A Comparative Analysis of Agnostic and Hybrid AI Approaches for Advanced Persistent Threat Detection. In: Rivera, G., Pedrycz, W., Moreno-Garcia, J., Sánchez-Solís, J.P. (eds) Innovative Applications of Artificial Neural Networks to Data Analytics and Signal Processing . Studies in Computational Intelligence, vol 1221. Springer, Cham. https://doi.org/10.1007/978-3-031-69769-2_8

25) Zacharis, A., Katos, V. & Patsakis, C. Integrating AI-driven threat intelligence and forecasting in the cyber security exercise content generation lifecycle. *Int. J. Inf. Secur.* **23**, 2691–2710 (2024). https://doi.org/10.1007/s10207-024-00860-w

26) Chowdhury, T. K. (2025). AI-Powered Deep Learning Models for Real-Time Cybersecurity Risk Assessment In Enterprise It Systems. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 675-704. https://doi.org/10.63125/137k6y79

27) Chukwu, B. (2021). AI-Driven Risk Management: Strengthening Cybersecurity and Market Stability in the US Financial Sector. *Volume*, *17*, 1967-1976. https://doi.org/10.30574/wjarr.2025.28.1.3647

28) Rakibul Hasan Chowdhury (2025). “Next-Generation Cybersecurity through Blockchain and AI Synergy: A Paradigm Shift in Intelligent Threat Mitigation and Decentralised Security”. International Journal of Research and Scientific Innovation (IJRSI), 12(8), https://doi.org/10.51244/IJRSI.2025.120800051

29) Jabed, M. M. I., & Ferdous, S. (2024). Integrating Business Process Intelligence with AI for Real-Time Threat Detection in Critical US Industries. *International Journal of Research and Applied Innovations*, *7*(1), 10120-10134. https://doi.org/10.15662/IJRAI.2024.0701004

30) Khatun, M., & Oyshi, M. S. (2025). Advanced Machine Learning Techniques for Cybersecurity: Enhancing Threat Detection in US Firms. *Journal of Computer Science and Technology Studies*, *7*(2), 305-315. https://doi.org/10.32996/jcsts.2025.7.2.31

31) Androutsopoulou, M., Carayannis, E.G., Askounis, D. *et al.* Towards AI-Enabled Cyber-Physical Infrastructures—Challenges, Opportunities, and Implications for a Data-Driven eGovernment Theory, Policy, and Practice. *J Knowl Econ* (2025). https://doi.org/10.1007/s13132-025-02726-5