ARTIFICIAL INTELLIGENCE IN DEFENSE AND INTELLIGENCE:

A Framework for Philippine Defense Agencies

Research Report on Global AI Implementation in Counterterrorism, Threat Detection, and National Security Operations

Prepared by:

Koleen Baes Paunon

Risk Intelligence Engineer

BPxAI

February 13, 2026

EXECUTIVE SUMMARY

Artificial Intelligence (AI) has fundamentally transformed defense and intelligence operations globally. In 2025, leading nations deploy AI-powered systems for threat prediction, counterterrorism, surveillance, and strategic decision-making. This report examines the current state of AI implementation in defense agencies worldwide and presents a comprehensive, actionable framework for the Philippine defense sector.

Global intelligence agencies have demonstrated that AI increases threat detection accuracy by up to 94.5%, reduces incident response times by over 90%, and enables the processing of petabytes of data that would be impossible for human analysts alone. The United States, United Kingdom, Israel, and other advanced nations have invested billions in AI-driven defense capabilities, establishing dedicated organizational structures and ethical frameworks to govern their deployment.

The Philippines stands at a critical juncture. With the Department of Science and Technology (DOST) targeting an AI-powered nation by 2028 through the National AI Strategy, and the country improving from 61st to 53rd in the UN Global Cybersecurity Index, we have momentum. However, defense-specific AI implementation remains nascent compared to peer nations in ASEAN and globally.

This report provides a plug-and-play framework that Philippine defense agencies can implement immediately. The framework addresses five critical dimensions: technical infrastructure, workforce development, operational integration, ethical governance, and international cooperation. Each component includes specific requirements, implementation steps, and success metrics tailored to Philippine context and constraints.

TABLE OF CONTENTS

1. INTRODUCTION

2. GLOBAL AI IMPLEMENTATION IN DEFENSE AND INTELLIGENCE

3. TECHNICAL CAPABILITIES AND APPLICATIONS

4. PHILIPPINE CONTEXT AND READINESS ASSESSMENT

5. IMPLEMENTATION FRAMEWORK FOR PHILIPPINE DEFENSE AGENCIES

6. REQUIREMENTS AND RESOURCE ALLOCATION

7. IMPLEMENTATION ROADMAP

8. RISK MANAGEMENT AND ETHICAL CONSIDERATIONS

9. RECOMMENDATIONS AND CONCLUSION

1. INTRODUCTION

1.1 Background and Context

The threat landscape facing nations in 2025 is fundamentally different from any previous era. Terrorism has evolved from centralized organizations like Al-Qaeda to decentralized networks and lone actors radicalized online. Extremist groups such as the Islamic State Khorasan Province (ISKP) leverage generative AI to produce propaganda in 13 languages simultaneously, creating polished videos and synthetic voice clips that rival professional journalism. The Philippines faces its own unique challenges with Abu Sayyaf, communist insurgency, and transnational threats that require sophisticated intelligence capabilities.

The volume of intelligence data has grown exponentially. The National Geospatial-Intelligence Agency (NGA) transports more data globally than any other U.S. agency. Intelligence communities worldwide face a fundamental constraint: not scarcity of information but abundance. The human analyst has become the limiting factor when processing surveillance footage, communications intercepts, social media posts, and open-source intelligence. This data deluge demands AI-powered solutions.

1.2 Research Objectives

This research aims to:

- Analyze how leading nations deploy AI for counterterrorism and threat detection
- Identify specific AI technologies and their defense applications
- Assess the Philippines' current AI readiness in defense sectors
- Develop an implementation framework adaptable to Philippine defense agencies
- Define requirements, resources, and implementation steps
- Establish ethical guidelines and governance structures

1.3 Methodology

This research synthesizes publicly available defense strategies, academic literature, and recent developments in AI-powered defense systems from 2024-2025. Primary sources include the U.S. Department of Defense AI strategy, UK Ministry of Defence AI framework, Israeli defense AI initiatives, and Philippine national AI strategies. The framework development draws from operational best practices, technical requirements documented in military AI implementations, and international governance standards including the Political Declaration on Responsible Military Use of AI.

2. GLOBAL AI IMPLEMENTATION IN DEFENSE AND INTELLIGENCE

2.1 United States

Organizational Structure

The U.S. established the Joint Artificial Intelligence Center (JAIC) in 2018, later integrated into the Chief Digital and Artificial Intelligence Office (CDAO) in 2021, which now oversees all Pentagon AI strategy. The Intelligence Community prioritizes automating each stage of the intelligence cycle, processing all available data through AI-enabled analytic systems before human analyst review.

Key Programs and Applications

- Project Maven: Incorporates computer vision and AI algorithms into intelligence-gathering cells for hostile activity identification. By 2024, it became one of NGA's most popular products with demand straining computing resources.
- Air Combat Evolution (ACE): Enhances autonomous air-to-air combat capabilities
- MQ-9 Reaper Drone: Uses AI for target identification and tracking
- Terrorism Prediction Models: Air Force develops models using Global Terrorism Database with 98% attack attribution accuracy using techniques like Shapley Additive Explanations (SHAP) and Local Interpretable Model-Agnostic Explanations (LIME)
- DARPA Media Forensics (MediFor): Automatically detects deepfakes and media manipulations

Investment and Resources

DARPA announced a multi-year investment exceeding $2 billion in the AI Next campaign. The 2025 National Defense Authorization Act (NDAA) establishes robust cybersecurity policies for all AI systems and requires creation of assessment frameworks by June 2026, with completion by June 2027.

2.2 United Kingdom

Strategic Framework

The UK Defence AI Strategy, published June 2022 and reinforced by Joint Service Publication 936 (November 2024), serves as the principal policy framework for safe and responsible AI adoption. The Defence AI Playbook (February 2024) facilitates industry collaboration. The June 2025 Strategic Defence Review mandates greater use of autonomy and AI within conventional forces as part of military modernization.

Key Principles

- Transform into an 'AI Ready' organization
- Strengthen UK's defense AI ecosystem through industry partnerships
- Shape global AI developments to promote security and democratic values

- Emphasize governance, development, and assurance throughout AI lifecycle
- Build on existing military doctrine and international laws around armed conflict

2.3 Israel

In January 2025, Israel's Defence Ministry created a new AI and Autonomy Administration to lead research, development, and acquisition across all branches of the Israel Defence Forces. Israel's approach integrates AI into algorithmic warfare with minimal human oversight in certain applications, though this raises significant ethical concerns internationally.

2.4 Other Notable Implementations

Japan

In August 2024, Japan allocated ¥18 billion for an AI surveillance system and procurement of unmanned drones and automated warships, primarily to counter declining enlistment and the perceived threat from China.

Singapore and ASEAN

Singapore has emerged as a regional leader in AI governance, implementing sector-specific frameworks. The ASEAN region is developing collaborative approaches to AI in defense while maintaining sovereign control over military applications.

3. TECHNICAL CAPABILITIES AND APPLICATIONS

3.1 Core AI Technologies in Defense

Computer Vision

Applications:

- Facial recognition in CCTV networks for continuous surveillance beyond human limitations
- Behavior analysis and anomaly detection in public spaces
- Autonomous drone surveillance with real-time target tracking
- Satellite imagery analysis for geospatial intelligence
- Weapon detection and crowd movement pattern prediction

Natural Language Processing (NLP)

Applications:

- Social media monitoring for radical or harmful content flagging
- Multilingual speech recognition and translation in noisy environments
- Sentiment analysis to gauge public opinion and identify unrest
- Automated processing of communications intercepts and documents
- Extraction of intelligence from captured enemy materials

Machine Learning and Predictive Analytics

Applications:

- Terrorism activity prediction with 72-98% accuracy rates
- Financial anomaly detection for terrorism financing prevention
- Behavioral analytics for insider threat detection
- Network traffic analysis for cyber threat identification
- Temporal dynamics modeling using recurrent neural networks and LSTM

3.2 Operational Use Cases

Counterterrorism

- Early warning systems predicting attack locations and timing
- Online radicalization detection through social media pattern analysis
- Counter-narrative generation tailored to local communities
- Terrorist network mapping and relationship analysis

Cyber Defense

- Real-time cyber-attack detection with 95.1% faster response times
- Automated vulnerability assessment and patching
- Advanced Persistent Threat (APT) identification
- Zero-trust architecture implementation with AI-driven policy tuning

Border Security and Critical Infrastructure

- Automated border monitoring with smart drones
- Critical infrastructure threat assessment
- Maritime domain awareness for archipelagic defense

4. PHILIPPINE CONTEXT AND READINESS ASSESSMENT

4.1 Current AI Initiatives

The Philippines has made significant strides in establishing AI governance and strategy. President Ferdinand Marcos Jr. approved the National AI Strategy for the Philippines (NAIS-PH) following a sectoral meeting in October 2025, tasking DOST to lead AI development. The strategy spans five key areas: infrastructure, workforce, innovation, ethics and policy, and deployment, with phased implementation from 2024 to 2028.

Key Achievements

- Improved from 61st (2020) to 53rd (2024) in UN Global Cybersecurity Index
- Rose from 65th (2023) to 56th (2024) in Government AI Readiness Index
- Invested over PHP 2.3 million in 113 AI-related projects through DOST-PCIEERD
- Established framework through DOST, DTI, DepEd collaboration since 2017
- Target: 43rd place in Global Innovation Index by 2028

4.2 Defense Sector Specific Context

The Department of National Defense (DND) is pursuing the Comprehensive Archipelagic Defense Concept through Armed Forces of the Philippines (AFP) modernization. The Asian Defense and Security Exhibition (ADAS) 2024 highlighted focus areas: asymmetric warfare, information security, cyber defense, and cybersecurity. However, AI integration in defense operations remains limited compared to civilian sectors.

Current Applications

- Transport systems enhancement
- Financial services modernization
- Energy and environmental monitoring
- Limited applications in national defense and public security

4.3 Challenges and Gaps

- Data Governance: Siloed data between agencies, limited interoperability
- Legacy Infrastructure: Outdated systems requiring integration with AI platforms
- Skills Gap: Global cybersecurity talent shortage affects Philippines
- Budget Constraints: Limited defense budget compared to threat complexity
- Computing Resources: Planned 26-fold HPC increase by 2028 still in progress
- Ethical Framework: Defense-specific AI ethics guidelines not yet established

4.4 Strategic Opportunities

- ASEAN Cooperation: Regional collaboration on defense AI development
- International Partnerships: Access to allied nation AI systems and expertise
- Vibrant Tech Sector: Growing Filipino AI development community

- Youth Demographics: Large pool of trainable analysts and technicians
- Government Support: Presidential directive and DOST leadership on AI strategy

5. IMPLEMENTATION FRAMEWORK FOR PHILIPPINE DEFENSE AGENCIES

This framework provides a comprehensive, modular approach that defense agencies can adapt to their specific operational needs and constraints. It follows the Defense AI lifecycle: Planning → Development → Testing → Deployment → Monitoring → Refinement.

5.1 Organizational Structure

Create AI Coordination Office (ACO)

Purpose:

Centralized coordination points for AI initiatives across AFP branches and intelligence agencies, like U.S. CDAO model but scaled for Philippine context.

Key Responsibilities:

- Develop and enforce AI governance policies
- Coordinate inter-agency AI projects
- Manage AI procurement and vendor relationships
- Oversee training programs and workforce development
- Monitor ethical compliance and human rights protections

Establish Defense AI Ethics Advisory Panel

Composition:

- Defense officials
- AI technical experts
- Legal scholars
- Human rights advocates
- Civil society representatives

5.2 Technical Infrastructure Development

Phase 1: Foundation (Months 1-6)

- Conduct infrastructure audit of existing systems
- Establish secure cloud environment (private or hybrid)
- Deploy high-performance computing (HPC) nodes at strategic locations
- Implement data governance framework and classification system
- Create secure data integration layer for inter-agency information sharing

Phase 2: Core Capabilities (Months 7-18)

- Deploy Computer Vision Platform for surveillance and reconnaissance
- Implement NLP Engine for communications analysis and social media monitoring
- Establish Predictive Analytics System for threat forecasting

- Deploy Cyber Threat Intelligence Platform with automated detection
- Create Intelligence Dashboard for unified situational awareness

Phase 3: Advanced Integration (Months 19-36)

- Deploy autonomous systems for border and maritime surveillance
- Implement AI-powered decision support systems
- Establish continuous learning and model improvement pipelines
- Integrate with regional security cooperation frameworks

5.3 Workforce Development

Training Programs

Tier 1: AI Awareness (All Personnel)

- Duration: 2-day workshop
- Content: AI basics, ethical considerations, operational implications
- Target: 100% of defense analysts and officers within 12 months

Tier 2: AI Users (Analysts and Operators)

- Duration: 2-week intensive course
- Content: System operation, data interpretation, query optimization
- Target: 500 personnel in first year

Tier 3: AI Specialists (Technical Staff)

- Duration: 6–12-month program
- Content: ML engineering, model development, system integration
- Partnership: DOST, universities, international allies
- Target: 50-100 specialists within 24 months

Retention Strategy

- Implement STEM pay supplements (following DIA model)
- Create career progression pathways for AI specialists
- Establish partnerships with private sector for knowledge exchange
- Provide continuous learning opportunities and certifications

6. REQUIREMENTS AND RESOURCE ALLOCATION

6.1 Technical Requirements

Component	Specifications	Estimated Cost (PHP)
High-Performance Computing Cluster	200+ GPU nodes, 10 PetaFLOPS capacity	500M - 800M
Secure Cloud Infrastructure	Private cloud, multi-region, 1PB storage	300M - 500M annually
AI Software Platforms	Computer vision, NLP, analytics suites	200M - 400M
Network Infrastructure	High-bandwidth secure network, encryption	150M - 250M
Sensors & IoT Devices	Cameras, drones, maritime sensors	400M - 600M
TOTAL INFRASTRUCTURE	**Initial 3-year investment**	**1.55B - 2.55B**

6.2 Personnel Requirements

Role	Headcount	Qualifications
AI Program Director	1	Senior defense official, AI strategy experience
AI Engineers/Data Scientists	50-75	MS/PhD in CS, AI/ML, 3+ years experience
Intelligence Analysts (AI-trained)	200-300	Existing analysts + 2-week AI training
System Administrators	20-30	IT/Cybersecurity background, cloud expertise
Ethics & Compliance Officers	5-10	Legal/policy background, AI ethics training

7. IMPLEMENTATION ROADMAP

7.1 Year 1: Foundation (2026)

Q1 (Jan-Mar):

- Establish AI Coordination Office and appoint leadership
- Form Ethics Advisory Panel
- Conduct comprehensive infrastructure and capability assessment
- Begin stakeholder consultations with DOST, DICT, NSC

Q2 (Apr-Jun):

- Finalize AI governance framework and policy documents
- Launch Tier 1 awareness training for all defense personnel
- Issue procurement requests for HPC and cloud infrastructure
- Identify pilot projects and use cases

Q3 (Jul-Sep):

- Deploy initial HPC nodes and secure cloud environment
- Begin Tier 2 training for 100 initial analysts
- Launch 2-3 pilot projects (e.g., social media monitoring, cyber threat detection)
- Establish data governance protocols

Q4 (Oct-Dec):

- Evaluate pilot project outcomes
- Recruit and onboard 20 AI engineers/data scientists
- Complete infrastructure Phase 1
- Present Year 1 progress report to DND leadership

7.2 Year 2: Expansion (2027)

- Deploy computer vision platform for surveillance systems
- Implement NLP engine for communications intelligence
- Launch predictive analytics for counterterrorism
- Train additional 200 Tier 2 analysts
- Expand AI engineer team to 50 personnel
- Begin regional HPC site establishment
- Establish partnerships with allied nations for knowledge sharing

7.3 Year 3: Integration (2028)

- Deploy autonomous systems for maritime and border surveillance
- Implement unified intelligence dashboard across all agencies
- Achieve full operational capability for core AI systems
- Complete Tier 3 specialist training program

- Establish continuous improvement and innovation pipeline
- Conduct comprehensive program evaluation and publish outcomes

8. RISK MANAGEMENT AND ETHICAL CONSIDERATIONS

8.1 Ethical Framework

Drawing from UK Ministry of Defence principles and the Political Declaration on Responsible Military Use of AI (endorsed by 60+ nations including key allies), the Philippines must establish clear ethical guidelines:

Core Principles:

- Human Accountability: Humans must remain responsible for all AI-assisted decisions, particularly those involving use of force
- Transparency: AI systems must be explainable and their decision-making processes auditable
- Fairness: AI must not discriminate based on race, religion, gender, or other protected characteristics
- Reliability: Systems must be thoroughly tested and operate within defined parameters
- Compliance: All AI deployments must comply with international humanitarian law and human rights obligations
- Privacy Protection: Balance security needs with constitutional rights to privacy

8.2 Risk Mitigation Strategies

Risk	Impact	Mitigation
Algorithm Bias	Discriminatory outcomes, false positives affecting minorities	Diverse training data, bias testing, human review of high-impact decisions
Adversarial Attacks	System manipulation, data poisoning	Adversarial training, continuous monitoring, air-gapped critical systems
Privacy Violations	Unconstitutional surveillance, data breaches	Data minimization, encryption, access controls, regular audits
Mission Creep	Expansion beyond authorized uses	Clear legal mandates, oversight mechanisms, periodic reviews
Over-reliance	Reduced human judgment, automation bias	Training on AI limitations, human-in-the-loop design
Vendor Lock-in	Dependence on foreign technology	Open standards, local capability development, diverse vendor relationships

8.3 Oversight and Accountability

- Regular audits by Ethics Advisory Panel
- Annual public transparency reports (within security constraints)
- Congressional oversight and reporting requirements
- Whistleblower protection mechanisms
- Independent technical audits of high-risk systems

9. RECOMMENDATIONS AND CONCLUSION

9.1 Immediate Actions (Next 6 Months)

1. Secure Executive Approval: Present this framework to DND Secretary and National Security Council for formal adoption
2. Allocate Initial Budget: Request PHP 500-800M for Year 1 infrastructure and personnel in 2027 budget cycle
3. Establish Governance: Create AI Coordination Office and Ethics Advisory Panel with clear mandates
4. Launch Pilot Projects: Select 2-3 low-risk, high-value use cases to demonstrate capability
5. Begin Training: Initiate Tier 1 awareness programs for leadership and key personnel

9.2 Strategic Priorities

- Build Domestic Capability: Invest in Filipino AI talent to reduce foreign dependence
- Forge International Partnerships: Leverage alliances for technology transfer and best practices
- Ensure Ethical Implementation: Make human rights and accountability cornerstone principles
- Integrate with National Strategy: Align defense AI with DOST's NAIS-PH framework
- Maintain Operational Focus: Prioritize capabilities that address real Philippine threats

9.3 Success Metrics

By 2028, Philippine defense agencies should achieve:

- 90% reduction in manual data processing time for intelligence analysis
- 80%+ accuracy in threat prediction models
- 50% faster incident response times for cyber and physical threats
- 100% of analysts trained in AI-assisted operations
- Zero verified cases of AI-related human rights violations
- Recognition as ASEAN leader in responsible defense AI implementation

9.4 Conclusion

Artificial Intelligence represents the most significant evolution in defense and intelligence capabilities since the digital revolution. Nations that successfully harness AI while maintaining ethical standards and democratic accountability will possess decisive advantages in protecting their citizens and interests.

The Philippines has a unique opportunity to leapfrog traditional development pathways. We need not replicate the decades-long evolution of Western defense establishments. With the right strategy, partnerships, and investments, we can build modern, AI-powered defense capabilities that reflect Filipino values and address our specific security challenges.

This framework provides a clear path forward. It is comprehensive yet flexible, ambitious yet realistic, technologically advanced yet ethically grounded. Success requires sustained commitment from leadership, adequate resource allocation, and most importantly, a shared vision among all defense agencies.

The threats we face—terrorism, insurgency, cyber-attacks, maritime incursions—are evolving rapidly. Our defensive capabilities must evolve faster. AI is not a silver bullet, but it is an essential force multiplier that enables our analysts, operators, and decision-makers to work smarter, faster, and more effectively.

The time to act is now. As we approach 2028—the target year for both DOST's national AI strategy and this defense framework—we have a narrow window to establish the foundations that will protect the Philippines for decades to come. With unity of effort and proper execution, we can transform our defense posture from reactive to predictive, from resource-constrained to AI-augmented, from vulnerable to resilient.

The future of Philippine national security depends on decisions made today. This framework provides the blueprint. The rest depends on our collective will to implement it.

REFERENCES

1. U.S. Department of Defense. (2024). National Defense Authorization Act for Fiscal Year 2025.

2. UK Ministry of Defence. (2022). Defence Artificial Intelligence Strategy.

3. Department of Science and Technology, Philippines. (2025). National AI Strategy for the Philippines (NAIS-PH).

4. Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy. (2023). U.S. Department of State.

5. Brennan Center for Justice. (2025). AI Provisions in the National Defense Policy Bill.

6. Institute for National Security Studies. (2019). Artificial Intelligence and National Security in Israel.

7. Combating Terrorism Center at West Point. (2021). Data, AI, and the Future of U.S. Counterterrorism.

8. The Soufan Center. (2025). Assessment of the Global Terrorism Threat Landscape in Mid-2025.

9. Northwestern University. (2023). Advancing AI Systems in Cybersecurity, Counterterrorism, and International Security.

10. Philippine News Agency. (2025). DOST eyes AI-powered Philippines by 2028.

11. Government of Philippines. (2025). PBBM: Make Best Use of AI for National Development.

12. OpenGov Asia. (2025). Fortifying Data with AI: A New Era for the Philippines' Security.

13. Breaking Defense. (2026). Artificial Intelligence is Everywhere: 2025 Review.

14. Chatham House. (2019). Artificial Intelligence Prediction and Counterterrorism.

15. European Parliament Think Tank. (2025). Defence and Artificial Intelligence.

END OF REPORT