iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** V **Month of publication:** May 2026

DOI: https://doi.org/10.22214/ijraset.2026.83289

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue V May 2026- Available at www.ijraset.com

Artificial Intelligence, National Security, and Scientific Governance: A Policy Framework for the United States

Prof. Md Shahin Kabir[1], Sabrina Sinthia Oshin[2], Md Raihan Kabir[3], Tanvir Rahman Tuhin[4], Jaharna Rafi Chowdhury[5], Easmat Jabin Sumi[6]

[1]*Associate Professor of Law at LCIT Bilaspur, India*
[2]*Former Masters Student at National University, Bangladesh*
[3]*MBA Student at Kyungsung University, South Korea*
[4]*BSS Student at National University, Bangladesh*
[5]*PhD Fellow at Putra Business School, Malaysia*
[6]*PhD Fellow at ISCTE, Portugal*

Abstract: ***Artificial intelligence (AI) is becoming a strategic national capability for the United States, affecting defense readiness, intelligence analysis, cybersecurity, critical infrastructure, scientific discovery, public administration, and geopolitical competition. This paper examines the future role of AI in U.S. national security and develops scientific policy advice that can be adapted by any government seeking to use AI responsibly. The study applies a qualitative policy-review methodology, drawing on recent U.S. federal AI strategies, national security guidance, NIST risk-management standards, Department of Homeland Security critical-infrastructure guidance, and AI-enabled science initiatives. The analysis finds that AI can improve threat detection, decision support, cyber defense, logistics, disaster response, biomedical discovery, and energy-system optimization. However, these benefits are inseparable from risks involving model opacity, adversarial manipulation, data leakage, deepfakes, autonomous decision-making, infrastructure dependency, workforce disruption, and public-trust erosion. The paper argues that future AI governance should move beyond a simple innovation-versus-regulation debate. Instead, governments should adopt a dual-use governance model that protects national security while preserving scientific integrity, civil liberties, democratic accountability, and international stability. The proposed framework recommends five pillars: sovereign AI infrastructure, independent scientific advisory capacity, risk-based deployment controls, secure public-sector data ecosystems, and international cooperation on AI safety and security. The paper concludes that AI should be treated as both a national security asset and a scientific public good. Any government adopting AI must therefore combine technical excellence with legal safeguards, ethical review, human accountability, and continuous empirical validation.***

Keywords: Artificial Intelligence, National Security, Scientific Advice, United States, AI Governance, Critical Infrastructure, Cybersecurity, Public Policy, Risk Management, Democratic Accountability.

I. INTRODUCTION

AI has moved from a research technology into the strategic core of government. In the United States, AI now shapes national security planning, defense modernization, cyber operations, border and transportation systems, intelligence analysis, emergency management, scientific research, and public-service delivery. This transformation is not merely technological. It changes how governments define threats, allocate resources, analyze information, and make decisions under uncertainty.

The U.S. policy environment reflects this strategic shift. Executive Order 14179, issued in January 2025, declares a policy of sustaining and enhancing U.S. global AI leadership to promote human flourishing, economic competitiveness, and national security (Executive Office of the President, 2025a). The 2025 America's AI Action Plan organizes federal priorities around accelerating innovation, building AI infrastructure, and leading international diplomacy and security (White House, 2025a). Earlier national-security guidance emphasized the use of AI in national security systems while protecting human rights, civil rights, civil liberties, privacy, and safety (White House, 2024). Together, these policy signals show that AI is increasingly understood as a core element of national power.

At the same time, AI produces risks that ordinary information-technology policy cannot fully manage. Large AI systems can generate persuasive false content, leak sensitive information, amplify bias, hallucinate unsupported claims, or be manipulated by adversaries. In security environments, an unreliable output can misdirect an investigation, trigger a mistaken operational response, or create escalation pressure during a crisis. In scientific environments, poorly validated AI can generate false discoveries, contaminate evidence pipelines, or mislead policy makers. Therefore, the central question is not whether governments should use AI, but how they can use it with sufficient security, scientific discipline, and democratic control.

This paper focuses on the United States because it is one of the most important global actors in AI research, defense technology, cloud infrastructure, semiconductor design, and scientific computing. However, the policy lessons are relevant to any government. The paper proposes a future-oriented governance model that treats AI as both a national security capability and a scientific public good.

II. RESEARCH METHODOLOGY

This study uses a qualitative policy-analysis method. It reviews U.S. federal AI policy documents, national security guidance, risk-management frameworks, critical-infrastructure recommendations, and recent science-policy initiatives. The analysis is organized around four questions: (1) How is AI being positioned in U.S. national security policy? (2) What opportunities can AI create for defense, cybersecurity, critical infrastructure, and scientific discovery? (3) What governance risks arise when AI is used by the state? and (4) What scientific advice should future governments adopt before deploying high-impact AI systems?

The paper does not claim to measure the performance of a single AI system. Instead, it develops a normative and practical governance framework. This is appropriate because national AI strategy is shaped not only by technical performance but also by institutional design, public trust, democratic accountability, data governance, and international coordination.

III. U.S. AI POLICY AND NATIONAL SECURITY CONTEXT

The United States has recently framed AI as a strategic technology linked to economic competitiveness, national security, and global leadership. The 2024 National Security Memorandum on AI directed federal agencies to harness AI for national security while protecting civil rights, civil liberties, privacy, and safety. This is important because it recognizes that security and rights are not separate domains; they must be designed together when AI is deployed by agencies with coercive power.

The 2025 U.S. AI Action Plan further emphasizes three policy pillars: innovation, infrastructure, and international diplomacy/security. This indicates a shift from viewing AI mainly as a software issue to viewing it as a full national system involving data centers, energy supply, chips, cloud systems, model evaluation, skilled labor, procurement, and allied coordination. The same approach is visible in federal guidance for agencies. OMB Memorandum M-25-21 directs agencies to accelerate AI use while maintaining governance and public trust, and it requires safeguards proportionate to risk, including attention to privacy, civil rights, and civil liberties (Office of Management and Budget, 2025).

The U.S. approach also links AI to scientific competitiveness. The 2025 Genesis Mission executive order describes a coordinated national effort to use AI for accelerated scientific discovery and high-priority national challenges (Executive Office of the President, 2025c). This reflects a broader recognition that future national security depends not only on weapons systems or intelligence capabilities, but also on scientific capacity in energy, biotechnology, materials, climate resilience, manufacturing, and health.

IV. OPPORTUNITIES FOR FUTURE AI IN U.S. NATIONAL SECURITY

A. Intelligence and Decision Support

AI can help analysts process large volumes of text, imagery, signals, open-source intelligence, and sensor data. It can identify patterns that human teams may miss and reduce time spent on routine classification or summarization. In crisis situations, decision-support systems can assist with scenario planning, logistics forecasting, and risk mapping. However, such tools must remain advisory. National security decisions require judgment, legal interpretation, and political accountability that cannot be delegated to a model.

B. Cybersecurity and Critical Infrastructure

AI can improve cyber defense by detecting anomalies, prioritizing vulnerabilities, generating defensive code, and supporting incident response. It can also support the resilience of energy grids, water systems, transportation networks, hospitals, financial systems, and telecommunications.

The Department of Homeland Security has already emphasized roles and responsibilities for AI in critical infrastructure, including risk management across developers, deployers, infrastructure operators, civil society, and government (Department of Homeland Security, 2024). The opportunity is substantial, but the risk is also high: adversaries may use AI to automate phishing, discover vulnerabilities, generate malware, or manipulate industrial control systems.

C. Defense Logistics and Operational Readiness

Military effectiveness depends heavily on maintenance, supply chains, workforce readiness, and logistics. AI can forecast equipment failure, optimize supply routes, support training simulations, and improve situational awareness. These uses are often less visible than autonomous weapons but may produce major strategic advantages. They are also generally more appropriate for early deployment because they support human planning without directly selecting targets or authorizing force.

D. Scientific Discovery and Strategic Innovation

AI can accelerate scientific discovery by analyzing large datasets, proposing hypotheses, designing experiments, supporting simulation, and improving modeling in domains such as energy systems, advanced materials, fusion research, biomedical science, and climate resilience. If governed well, AI-enabled science can strengthen national security by reducing dependence on fragile supply chains, improving health preparedness, and accelerating technologies needed for energy independence and disaster resilience.

V. MAJOR RISKS AND GOVERNANCE CHALLENGES

A. Model Reliability and Hallucination

AI systems can produce confident but incorrect outputs. In low-risk settings, this may cause inconvenience. In national security or scientific-policy settings, it can cause serious harm. A hallucinated intelligence summary, a false cyber attribution, or an unsupported scientific claim can mislead officials and damage public trust. Therefore, high-impact government AI should require source traceability, uncertainty reporting, domain-expert review, and post-deployment monitoring.

B. Data Security and Information Leakage

Government AI systems may process sensitive, classified, proprietary, or personally identifiable information. If data governance is weak, sensitive data can leak through prompts, model outputs, training pipelines, vendor systems, or insecure application programming interfaces. Public-sector AI should therefore use secure data environments, access controls, audit logs, encryption, and clear rules about what data can be used for model training or fine-tuning.

C. Adversarial Manipulation and Deepfakes

AI increases the speed and scale of deception. Deepfakes, synthetic documents, automated disinformation, and voice cloning can target elections, diplomacy, financial markets, and emergency response. Adversaries may also attack AI systems directly through data poisoning, prompt injection, model extraction, or adversarial examples. National AI strategy must therefore combine model security, media authentication, public communication capacity, and rapid incident-response mechanisms.

D. Civil Liberties and Democratic Oversight

When AI is used by government, it can affect rights, benefits, surveillance, policing, immigration, and public safety. Even a technically accurate system may be unacceptable if it lacks transparency, legal authority, appeal rights, or human review. AI governance must therefore include democratic oversight, independent auditing, clear procurement standards, and meaningful mechanisms for affected individuals to challenge harmful decisions.

E. Overdependence and Institutional Deskilling

A future government may become dependent on automated systems for tasks that require human expertise. If analysts, scientists, or public administrators rely too heavily on AI, agencies may lose critical judgment skills. This is especially dangerous when a system fails during a crisis. Governments should preserve human expertise, conduct manual fallback exercises, and train personnel to question AI outputs rather than accept them automatically.

VI. SCIENTIFIC ADVICE FOR ANY GOVERNMENT

The following scientific advice is designed for any government, not only the United States. It assumes that AI will continue to expand across public services, national security, and research. The goal is to help governments gain value from AI without sacrificing public trust, safety, or democratic accountability.

1) Treat AI as critical infrastructure: AI should be governed like energy, telecommunications, and cybersecurity infrastructure because failure can affect national resilience.
2) Build an independent scientific AI advisory council: Governments need independent experts in AI, law, ethics, security, social science, statistics, and domain science to review high-impact uses.
3) Require risk-based classification: Systems should be classified as low, medium, high, or prohibited risk depending on their impact on rights, safety, national security, and public trust.
4) Use mandatory pre-deployment testing: High-impact AI should undergo red-teaming, bias evaluation, cybersecurity testing, privacy review, and stress testing before use.
5) Keep humans accountable: AI should support decisions, but a legally responsible human official must remain accountable for high-impact government action.
6) Protect public-sector data: Governments should develop secure data trusts, data-minimization rules, access logs, and limits on vendor reuse of public data.
7) Require transparency registers: Agencies should maintain public inventories of AI systems, purposes, risk levels, vendors, data categories, and oversight mechanisms, except for narrowly justified security exemptions.
8) Invest in workforce literacy: Civil servants, judges, military leaders, scientists, teachers, and procurement officers need practical AI literacy and risk-management training.
9) Separate scientific evidence from political pressure: Scientific AI advice should be published when possible and protected from manipulation, selective reporting, or partisan filtering.
10) Cooperate internationally: Governments should coordinate on AI safety, cyber norms, export controls, incident reporting, and protection against AI-enabled disinformation.

VII. PROPOSED FUTURE AI GOVERNANCE FRAMEWORK

This paper proposes a five-pillar framework for future AI governance. The framework is designed for the United States but can be adapted by other governments.

A. *Sovereign and Resilient AI Infrastructure*

Governments should ensure secure access to computing resources, energy, data centers, cloud services, chips, and technical talent. AI leadership depends on physical infrastructure as much as software. However, infrastructure expansion must be linked to energy planning, cybersecurity, environmental review, and supply-chain resilience.

B. *Independent Scientific Advisory Capacity*

A permanent scientific AI advisory body should review government AI strategy and high-impact deployments. It should include technical experts, legal scholars, social scientists, civil society representatives, national security experts, and domain specialists. Its advice should be transparent whenever national security does not require confidentiality.

C. *Risk-Based Deployment Controls*

Not all AI systems require the same level of oversight. A chatbot for internal document search does not create the same risk as a system used for biometric identification, benefits eligibility, immigration screening, or military targeting support. Governments should adopt risk tiers with escalating requirements for documentation, evaluation, authorization, monitoring, and appeal.

D. *Secure Public Data Ecosystems*

AI performance depends heavily on data quality. Public agencies often hold valuable data, but those data may be incomplete, biased, sensitive, or legally restricted. Governments should improve data quality, metadata standards, privacy-preserving analytics, and secure data-sharing agreements. No agency should deploy high-impact AI if it cannot explain the data used, the population covered, and the known limitations of the dataset

E. International AI Security Cooperation

AI risk is transnational. Cyberattacks, disinformation campaigns, model theft, and unsafe autonomous systems do not stop at national borders. The United States and allied governments should coordinate on AI security standards, incident reporting, export controls, evaluation methods, and norms for responsible military use. International cooperation should also support lower-resource countries so AI does not deepen global inequality.

VIII. DISCUSSION

The central policy challenge is that AI is simultaneously a tool of innovation, a security asset, and a source of systemic risk. Governments that regulate too slowly may allow harmful deployments, but governments that regulate without scientific understanding may block useful innovation. The solution is not simply more regulation or less regulation; it is better institutional design.

The U.S. case shows the importance of aligning AI infrastructure, procurement, risk management, national security, and scientific discovery. The NIST AI Risk Management Framework offers a useful foundation because it organizes trustworthy AI around governance, mapping, measurement, and management (NIST, 2023). The NIST Generative AI Profile adds more specific guidance for risks associated with generative systems, including information integrity, misuse, and evaluation challenges (NIST, 2024). These frameworks should be treated as living systems, not static checklists.

For any government, the most important scientific principle is validation. AI systems should not be accepted because they appear advanced, are produced by a famous vendor, or provide confident answers. They should be tested against real-world tasks, monitored after deployment, audited independently, and withdrawn when they fail. Scientific advice must remain independent enough to challenge both political leaders and technology companies.

IX. RECOMMENDATIONS

First, governments should create a national AI security and science office that coordinates policy across defense, intelligence, health, energy, education, and infrastructure. Second, all high-impact public-sector AI systems should require an impact assessment before deployment. Third, governments should maintain public AI inventories and explainable procurement records unless a specific national security exemption is justified. Fourth, government AI systems should include human accountability, appeal mechanisms, and independent audits. Fifth, governments should invest in AI literacy for civil servants and the public. Sixth, national AI strategies should include scientific integrity protections to ensure that AI-generated evidence is not misused in policy-making. Finally, governments should participate in international AI security cooperation to reduce the risk of escalation, disinformation, and unsafe deployment.

X. CONCLUSION

AI will shape the future of national security and scientific governance. In the United States, AI is already being positioned as a strategic capability linked to defense, cybersecurity, critical infrastructure, economic competitiveness, and scientific discovery. This creates major opportunities, but it also creates risks that cannot be solved by technology alone. Future governments must treat AI as a dual-use public capability: powerful enough to strengthen security and science, but risky enough to require oversight, validation, and democratic accountability.

The best path forward is a balanced governance model. Governments should invest in AI infrastructure and scientific discovery, but they should also require risk-based controls, independent advisory systems, secure data governance, human accountability, and international cooperation. AI should not replace public judgment. It should strengthen the ability of democratic governments to make evidence-based decisions while protecting rights, safety, and trust.

REFERENCES

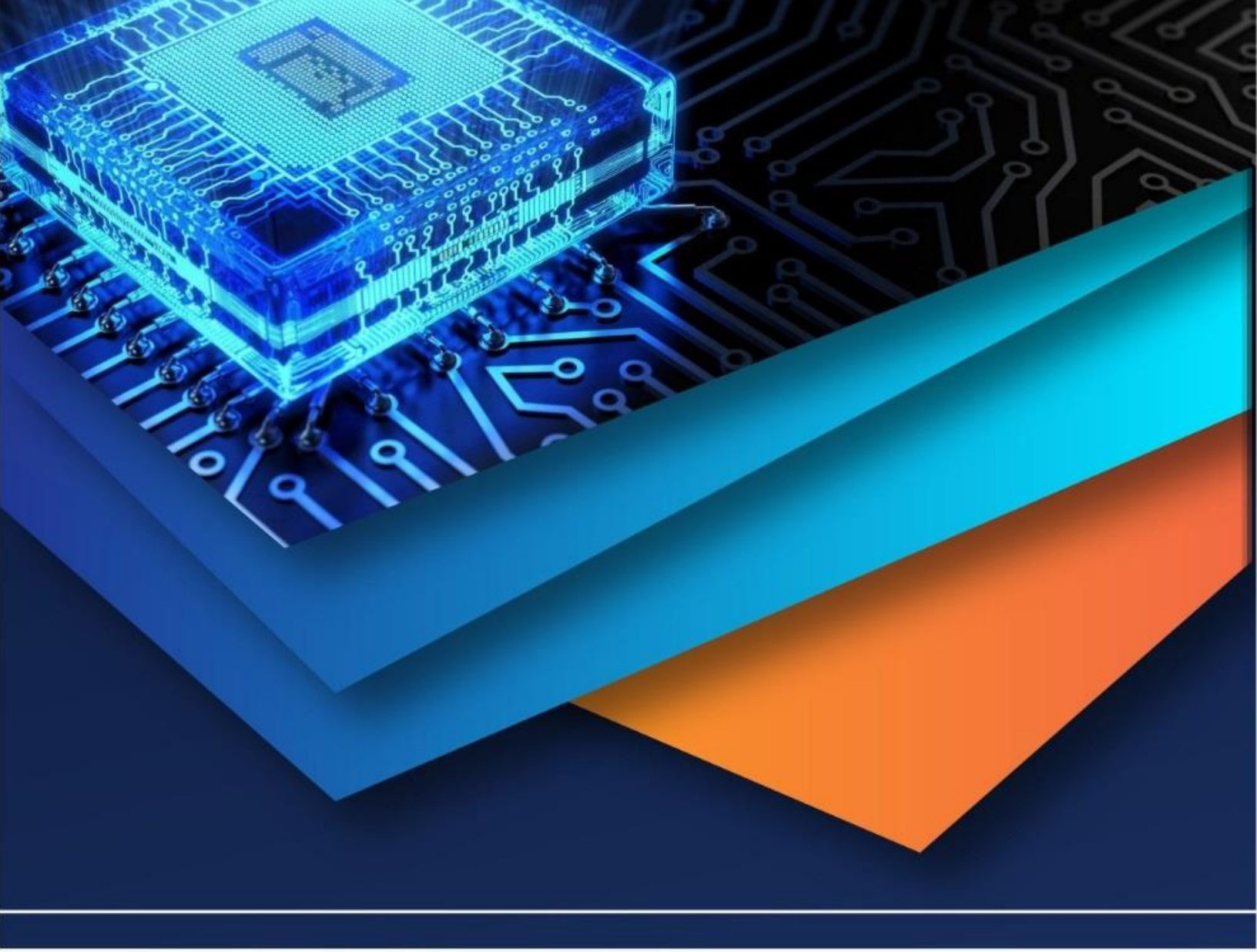
[1] Autio, C., Basu, A., Eppard, P., Hamon, R., Hutter, B., Kumar, H., & Tabassi, E. (2024). Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile (NIST AI 600-1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.AI.600-1

[2] Department of Homeland Security. (2024). Roles and responsibilities framework for artificial intelligence in critical infrastructure. U.S. Department of Homeland Security. https://www.dhs.gov/publication/roles-and-responsibilities-framework-artificial-intelligence-critical-infrastructure

[3] Executive Office of the President. (2025a). Executive Order 14179: Removing barriers to American leadership in artificial intelligence. Federal Register, 90(20), 8741-8742. https://www.federalregister.gov/documents/2025/01/31/2025-02172/removing-barriers-to-american-leadership-in-artificial-intelligence

[4] Executive Office of the President. (2025b). Executive Order 14277: Advancing artificial intelligence education for American youth. The White House. https://www.whitehouse.gov/presidential-actions/2025/04/advancing-artificial-intelligence-education-for-american-youth/

[5] Executive Office of the President. (2025c). Launching the Genesis Mission. The White House. https://www.whitehouse.gov/presidential-actions/2025/11/launching-the-genesis-mission/
[6] Kabir, M. S., & Oshin, S. S. Artificial Intelligence in Policing: Ethical, Regulatory, and Technological Challenges in the Canadian Context.
[7] National Institute of Standards and Technology. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). U.S. Department of Commerce. https://www.nist.gov/itl/ai-risk-management-framework
[8] Office of Management and Budget. (2025). Memorandum M-25-21: Accelerating federal use of AI through innovation, governance, and public trust. Executive Office of the President. https://www.whitehouse.gov/wp-content/uploads/2025/02/M-25-21-Accelerating-Federal-Use-of-AI-through-Innovation-Governance-and-Public-Trust.pdf
[9] Kabir, S., & Mustofa, J. Contemporary Development of International Humanitarian Laws with Special Reference to Refugees, Women and Prisoners.
[10] White House. (2024). National Security Memorandum on advancing the United States leadership in artificial intelligence; harnessing artificial intelligence to fulfill national security objectives; and fostering the safety, security, and trustworthiness of artificial intelligence. https://www.presidency.ucsb.edu/documents/national-security-memorandum-advancing-the-united-states-leadership-artificial
[11] Kabir, M. S. (2025). When Business Law Meets FinTech: Contracts in a Digital Age—The US Perspective. International Journal of Research Publication and Reviews.
[12] White House. (2025a). America's AI Action Plan. https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf
[13] White House. (2025b). AI.gov: President Trump's AI strategy and action plan. https://www.ai.gov/



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY