# The National Security Memorandum on Artificial Intelligence

Ephyia Publishing

---

## The National Security Memorandum on Artificial Intelligence

A Commentary on the Memorandum of October 24, 2024 Issued by President Joe Biden

Updated, October 2025

Dr Alex Bugeja, PhD

---

## Table of Contents

**Introduction**

**Chapter 1:** The Urgency of AI Leadership for US National Security **Chapter 2:** Understanding the AI Paradigm Shift and its Implications **Chapter 3:** Promoting Progress and Innovation in US AI Development **Chapter 4:** Attracting and Retaining Top AI Talent: A National Security Priority **Chapter 5:** Securing the Computational Foundation of US AI Dominance **Chapter 6:** Protecting US AI from Foreign Intelligence Threats: A Critical Mission **Chapter 7:** Safeguarding the AI Supply Chain from Foreign Interference **Chapter 8:** Managing Risks to AI Safety, Security, and Trustworthiness **Chapter 9:** The Role of the AI Safety Institute in Pre-Deployment Testing **Chapter 10:** Evaluating Frontier AI Models for Potential National Security Threats **Chapter 11:** Establishing Benchmarks for Assessing AI Capabilities and Limitations **Chapter 12:** Classified Evaluations of AI for Cyber, Nuclear, and Radiological Risks **Chapter 13:** Mitigating Chemical and Biological Risks from AI Advancements **Chapter 14:** Strengthening Foundational Understanding of AI Safety and Trustworthiness **Chapter 15:** Protecting Classified Information in the Age of AI **Chapter 16:** Harnessing AI for National Security Objectives: Partnerships and Policies **Chapter 17:** Developing AI Talent within the US Government **Chapter 18:** Modernizing Acquisition and Procurement for AI Systems **Chapter 19:** Developing Policies for Responsible AI Use in National Security **Chapter 20:** International Collaboration in AI Development and

Deployment **Chapter 21:** Improving Internal Coordination for AI Use on National Security Systems **Chapter 22:** Strengthening AI Governance and Risk Management for National Security **Chapter 23:** Developing a Framework for Responsible AI Use in National Security **Chapter 24:** Fostering a Stable and Responsible International AI Governance Landscape **Chapter 25:** Ensuring Effective Coordination and Reporting of AI Policy **Chapter 26:** The AI National Security Coordination Group: A Collaborative Approach **Afterword:** The Evolving Legacy of the Biden AI Memorandum (2025 Update)

---

# Introduction

On October 24, 2024, President Joe Biden issued a pivotal National Security Memorandum on Artificial Intelligence, marking a significant moment in the United States' approach to this transformative technology. This memorandum, a direct response to the evolving landscape of AI and its growing implications for national security, lays out a comprehensive strategy for ensuring the US maintains its leadership in AI while simultaneously mitigating its potential risks.

This book serves as a detailed commentary on the memorandum, exploring its key provisions, analyzing their potential impact, and offering insights into the future of AI in the context of US national security. It aims to provide a clear and accessible understanding of the memorandum's objectives, its strategic directions, and the challenges and opportunities it presents.

The memorandum acknowledges AI as an "era-defining technology" with profound implications for national security. It recognizes the potential benefits of AI in enhancing national security functions, but also highlights the potential risks if misused or inadequately safeguarded. The document emphasizes the need for the US to lead the world in the responsible application of AI, particularly in the national security domain.

The memorandum outlines three core objectives guiding the US government's activities concerning AI and national security:

1. **Leading the development of safe, secure, and trustworthy AI:** This involves strengthening the US AI ecosystem, promoting innovation and competition, protecting against foreign intelligence threats, and managing risks to AI safety, security, and trustworthiness.

2. **Harnessing AI to achieve national security objectives:** This entails adapting partnerships, policies, and infrastructure to effectively utilize AI

capabilities while upholding democratic values, including human rights, civil rights, civil liberties, privacy, and safety.

3. **Cultivating a stable and responsible international AI governance framework:** This aims to foster safe and trustworthy AI development and use globally, manage risks, promote democratic values, and realize the worldwide benefits of AI.

The memorandum directs specific actions across various government agencies to achieve these objectives. These actions encompass:

- **Promoting progress and innovation in US AI development:** Including attracting and retaining top AI talent, investing in computational resources, and streamlining administrative processes.
- **Protecting US AI from foreign intelligence threats:** This involves identifying and mitigating threats to the US AI ecosystem, including intellectual property theft and supply chain vulnerabilities.
- **Managing risks to AI safety, security, and trustworthiness:** This encompasses establishing testing infrastructure, developing safety guidelines, and conducting classified evaluations of AI systems for potential threats.
- **Harnessing AI to achieve national security objectives:** This involves adapting partnerships, policies, and infrastructure to effectively utilize AI capabilities while upholding democratic values.
- **Fostering a stable and responsible international AI governance landscape:** This includes advancing international agreements, collaborations, and norms to promote responsible AI development and use globally.

This book will delve into each of these areas, providing a comprehensive analysis of the memorandum's directives and their implications. It will examine the potential impact of these actions on the US national security landscape, the challenges and opportunities they present, and the future trajectory of AI in this crucial domain.

The memorandum's issuance signifies a critical juncture in the US's engagement with AI. It reflects a deep understanding of AI's transformative potential and the need for a proactive and comprehensive approach to harness its benefits while mitigating its risks. This book aims to contribute to a broader understanding of this crucial document and its significance for the future of US national security in the age of AI.

---