Letter of Transmittal

FROM: Aykhan Pashayev

TO: Professor Miguel "Mike" Asencio

DATE: 7/18/2025

SUBJECT: AI as a Double-Edged Sword: Enhancing vs. Undermining Cyber Defense

Dear Professor Asencio,

I'm excited to present to you, the Cybersecurity Policy Paper titled "AI as a Double-Edged Sword: Enhancing vs. Undermining Cyber Defense". The paper highlights my analysis on the dual use of artificial intelligence in cybersecurity.

I conducted an in-depth analysis, which included collecting valuable resources from the internet and researching with the help of AI tools (for education purposes). Based on the results, I suggested recommendations for reform to enhance governance, oversight, and defensive strategies.

Sincerely,

Aykhan Pashayev

AI as a Double-Edged Sword:

Enhancing vs. Undermining Cyber Defense

Aykhan Pashayev

ISS 3613 – Issues in Global Cybersecurity

Policy

Professor Miguel "Mike" Asencio

July 18, 2025

Executive Summary

Artificial intelligence (AI) has the potential to significantly improve cybersecurity through better threat detection and automated responses. Nowadays, we see almost every company start integrating AI into their cybersecurity infrastructures. Because AI makes things easier and faster.

However, AI creates new and rising offensive cyber risks, exposing a significant dual-use dilemma. This study contends that the existing U.S. cybersecurity policy structure is insufficiently prepared to deal with this complexity, resulting in severe vulnerabilities. In order to prevent this situation some recommendations are included in the paper.

Recommendations include better governance, more focused supervision, stronger defense capabilities, and integrated civil-military policy agendas.

Table of Contents

Introduction

AI technologies have transformed cybersecurity by offering capabilities that greatly improve threat detection, predictive analytics, and automated defensive responses in a very short time. AI driven cybersecurity threat detection tools are getting developed to advanced levels in multiple tech companies. However, when adversaries employ sophisticated AI-driven attacks, the same AI capabilities utilized for defense are swiftly evolving into potent attacking tools. I call this nature of humanity; some people always find a way to use wonderful tools for evil purposes. This dual-use nature of AI has serious policy implications for national security, emphasizing the importance of explicit tactics for balancing defensive advantages and offensive threats.

Opportunities for AI-Enhanced Cyber Defense

AI has significantly improved cybersecurity by enabling quick detection, predictive threat modeling, and automated incident response. AI's capability of handling massive amounts of data in few seconds, rapid growth and fast integration affecting positively to cyber defense field. CISA's AI Cybersecurity Collaboration Playbook outlines how AI-enhanced public-private collaborations may improve threat intelligence sharing. [2] Furthermore, rules for securely integrating AI in key infrastructures emphasize federal efforts to incorporate sophisticated protective mechanisms. [4] AI-powered automation enables real-time threat mitigation, dramatically decreasing human response times and preventing possible breaches. [3]

In this field the main goal is to automate almost every possible process because most of the time security incidents happen because of human error. Now, AI is becoming a great tool for cybersecurity professionals to solve this issue. Faster response time, capabilities on analytics and situational awareness are all essential for protecting digital security, guess what AI has all of these necessary skills.

Furthermore, the combination of NIST cybersecurity principles with AI lifecycle management results in effective, layered protection methods. Ee et al. suggest for a defense-in-depth approach that incorporates continuous AI monitoring, threat databases, and predictive analytics. [6] Such frameworks are critical steps toward ensuring secure AI deployment and effective cyber protection.

AI as an Emerging Threat Vector

Despite these breakthroughs, AI also increases offensive cyber capabilities. Malicious use cases include automated phishing, social engineering, quick vulnerability finding, and sophisticated data poisoning techniques. Everyone can do great social engineering attack even by using ChatGPT, realistic email can be written, or realistic website and domain can be created. Also, by using deepfakes – basically, by using someone's voice or face, creating fake voice or video messages. All these resources are publicly accessible by everyone but of course there's a lot of people who do not know about that. Roy Chua underlines the growing threat from generative AI, which enables both social-engineering efforts and vulnerability identification on new scales. [14] Open-weight Large Language Models (LLMs) increase these concerns by democratizing access to strong offensive weapons, resulting in major cybersecurity risks that are not adequately addressed by present legislative frameworks. [5]

Furthermore, RAND Corporation identifies key vulnerabilities relating to the theft and misuse of AI model weights, which allow attackers to exploit private data or conduct targeted assaults. [10] Thus, AI-driven cyber threats are fast expanding beyond present defensive capabilities, revealing systemic flaws in current regulations.

Policy Gaps and Structural Vulnerabilities

The existing United States cybersecurity legislation has substantial holes in handling AI's dual-use nature due to AI's rapid growth. Richard Danzig of RAND highlights significant flaws in national security infrastructure, focusing on old bureaucratic processes that are unsuited to rapid technological advancements. [1] These policy deficiencies are exacerbated by poor monitoring of dual-use AI models and ineffective interagency cooperation.

Furthermore, the Atlantic Council emphasizes that civil AI rules frequently ignore national security considerations, resulting in regulatory blind spots that enemies exploit. [12] The civil-military gap in AI supervision precludes coordinated, unified policy responses, making key infrastructure exposed to dual-use threats.

Maybe time has come to regulate the companies that develop large-scale AI technologies. Instead of letting them only build cool stuff, some regulations and rules should be applied to these companies due to their AI technology development before it's going to too late.

U.S. Policy Responses and Initiatives

The United States has launched many solutions to AI-driven cybersecurity risks in past few years, including presidential directives, voluntary industry standards, and strategic federal initiatives. President Biden's 2025 executive order requires AI-focused cybersecurity upgrades across government agencies and key infrastructure sectors. [8] The CISA Roadmap for AI recommends comprehensive initiatives to reduce AI misuse and improve protection systems against AI-driven threats. [11]

NIST's new standards expressly address dual-use concerns from core AI models, recommending structured monitoring and mitigation techniques. [13] Despite these attempts, the

policy environment remains fragmented, with little integration of civilian regulatory frameworks and national security requirements.

Recommendations for Policy Reform

To properly handle AI's dual-use concerns, significant regulatory measures are required:

First, governance structures must adjust quickly to ensure logical interagency collaboration and efficient communication routes. RAND's ideas for government modernization can help drive this change, with an emphasis on policy agility to keep up with AI's pace. [1]

Second, enhanced supervision mechanisms must expressly target dual-use AI technology by including civilian and military factors. The Atlantic Council's appeal to bridge the civil-military gap emphasizes the importance of integrated regulatory frameworks that manage dual-use hazards holistically. [12]

Third, federal investment in advanced defensive capabilities is critical, as evidenced by the CISA plan, which includes extending AI-driven automation and real-time threat analytics. [2] To protect critical infrastructure from new risks, federal projects should emphasize secure AI deployment processes, as outlined in joint guidance materials. [4]

Finally, international collaboration and standardization must be strengthened. The United States should work on global AI cybersecurity guidelines to address weaknesses such as open-weight models and intellectual property theft, as identified by RAND. [10]

Conclusion

AI creates an evident dual-use challenge in cybersecurity, improving defense capabilities but also enabling adversaries. Current US cybersecurity regulations do not effectively handle this complexity, exposing systemic flaws that must be addressed immediately. Comprehensive governance changes, integrated monitoring, focused defense spending, and international

collaboration are important steps toward properly addressing AI's dual-use issues. Proactive policy changes now will considerably reduce tomorrow's cybersecurity dangers.

Annotated Bibliography

1. Richard Danzig, Artificial Intelligence, Cybersecurity, and National Security: The Fierce, Urgency of Now, RAND Corporation, July 14, 2025.[1]

https://www.rand.org/pubs/perspectives/PEA4079-1.html

Danzig argues that national security institutions are woefully unprepared for AI's rapid cyber implications, and he proposes ten detailed recommendations for U.S. government modernization. This is foundational for framing my paper's national security and strategic policy sections by highlighting gaps and policy needs.

2. CISA, AI Cybersecurity Collaboration Playbook, January 14, 2025.[2]

https://www.cisa.gov/resources-tools/resources/ai-cybersecurity-collaboration-playbook

This playbook outlines voluntary mechanisms for AI firms and infrastructure operators to share threat data with CISA and the Joint Cyber Defense Collaborative. It's real-world example of public–private defensive cooperation that I can cite in my collaboration & governance section.

3. CISA, Best Practices for Securing Data Used to Train & Operate AI Systems, May 22, 2025.[3]

https://www.cisa.gov/resources-tools/resources/ai-data-security-best-practices-securing-data-used-train-operate-ai-systems

This guide discusses lifecycle threats to AI models—like poisoning and integrity compromises—and concrete strategies to mitigate them. It supports my discussion of technical safeguards and legal/ethical risk management frameworks.

4. CISA, Joint Guidance on Deploying AI Systems Securely, April 15, 2024.[4]

https://www.cisa.gov/news-events/alerts/2024/04/15/joint-guidance-deploying-ai-systems-securely

A collaborative document between CISA and other U.S. agencies, it defines best practices for securely integrating third-party AI solutions into critical systems. This will fit well in outlining defensive capabilities and government-approved deployment policies.

5. Alfonso de Gregorio, "Mitigating Cyber Risk in the Age of Open-Weight LLMs: Policy Gaps and Technical Realities," arXiv, May 21, 2025.[5]

https://arxiv.org/abs/2505.17109

De Gregorio explores emerging cybersecurity risks tied to fully public large language models and emphasizes policy lacunae in current regimes like the EU AI Act. This fresh academic insight helps strengthen my regulatory gaps and international policy critique section.

6. Shaun Ee et al., "Adapting Cybersecurity Frameworks to Manage Frontier AI Risks: A Defense-in-Depth Approach," arXiv, August 15, 2024.[6]

https://arxiv.org/abs/2408.07933

The authors recommend integrating NIST CSF, AI development lifecycles, and threat databases into a layered approach for AI-secure environments. I'll use this to support my recommendations for lifecycle-based policy and infrastructure resilience.

7. Miles Brundage et al., "The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation," arXiv, February 20, 2018.[7]

https://arxiv.org/abs/1802.07228

A seminal work mapping AI-enabled offensive threats in digital, physical, and political domains, with a taxonomy and high-level policy suggestions. This source will anchor my section on offensive cyber threats and historical context.

8. Politico, "Upcoming executive order aims to use AI to enhance federal cybersecurity efforts," January 10, 2025.[8]

https://www.politico.com/news/2025/01/10/executive-order-ai-federal-cybersecurity-00197656

This article outlines Biden's AI-focused cybersecurity executive order, including mandates on defense, cloud, and energy sector pilots. I'll reference this to illustrate executive-level regulatory action in federal cybersecurity strategy.

9. Wikipedia contributors, "Regulation of AI in the United States," updated July 2025.[9]

https://en.wikipedia.org/wiki/Regulation_of_AI_in_the_United_States

The entry provides a clear overview of U.S. AI regulation, including the AI Bill of Rights, voluntary industry commitments, and recent state efforts. While Wikipedia is secondary, it gives a useful regulatory timeline and multiple primary links for deeper research.

10. RAND Corporation, Securing AI Model Weights, June 2024. [10]

https://www.rand.org/pubs/research_reports/RRA2849-1.html

This report examines how model-weight theft threatens AI security and advises threat model updates for frontier AI labs. It enriches my discussion on intellectual property, industrial policy, and defense strategies.

11. CISA, Roadmap for AI, (publication date not specified, probably 2025). [11]

https://www.cisa.gov/resources-tools/resources/roadmap-ai

This strategic plan outlines how CISA aims to bolster AI for cyber defense, protect AI systems from misuse and deter AI-driven attacks on critical infrastructure. It's ideal for grounding policy recommendations and defensive strategy chapters.

12. Atlantic Council, Second-order Impacts of Civil Artificial Intelligence Regulation on Defense: Why the National Security Community Must Engage (Atlantic Council, April 2025).[12]

https://www.atlanticcouncil.org/in-depth-research-reports/report/second-order-impacts-of-civil-artificial-intelligence-regulation-on-defense-why-the-national-security-community-must-engage/

This report analyzes how a lack of civil AI regulations can create blind spots in defense applications, warning that U.S. policy frameworks designed for civilian uses often fail to anticipate military and offensive use cases. It argues for integrated policy design that bridges the civil–military divide in AI oversight—perfectly underscoring your thesis on structural policy gaps.

13. U.S. AI Safety Institute (AISI), Managing Misuse Risk for Dual-Use Foundation Models, NIST AI 800-1 (Second Public Draft, January 2025).[13]

https://www.nist.gov/news-events/news/2025/01/updated-guidelines-managing-misuse-risk-dual-use-foundation-models

This draft provides detailed guidance on monitoring and mitigating risks from dual-use AI models—highlighting threats from open weights enabling automated cyber-offensive operations, while also acknowledging their defensive utility. The document frames U.S. government as underprepared structurally, advocating for evidence-driven interagency monitoring and capacity building.

14. Roy Chua, "AI in Cybersecurity: Offensive AI, Defensive AI & the Crucial Data Foundation, Part 1," Enea Insights, June 5, 2025.[14]

https://www.enea.com/insights/ai-in-cybersecurity-part-1-offensive-ai/

Chua's analysis illustrates how generative AI is already amplifying social engineering and vulnerability discovery for attackers, while simultaneously scaling defensive detection systems.

It emphasizes the “AI vs AI” shift in cyber warfare and warns of a speed mismatch highlighting U.S. enterprises and policy frameworks lagging in automated defense adoption.