NAVIGATING THE FUTURE OF CYBERSECURITY WITH ARTIFICIAL INTELLIGENCE

An AFCEA International Cyber Committee White Paper

Principal Author & Contributors: Dr. Rhonda Farrell & Mr. Ray DeMeo, Mr. Petr Jirasek, Ms. Tarrazzia Martin, Mr. Jim Payne, Mr. Marcus Sachs, Mr. Sky Sharma, Mr. Samuel Visner, Mr. Harry Wingo

*"Simply put, we are in the midst of a **fundamental transformation** in our nation's cybersecurity. It is now clear that a reactive posture cannot keep pace with fast-evolving cyber threats and a dynamic technology landscape, and that aspiring just to manage the worst effects of cyber incidents is no longer sufficient to ensure our national security, economic prosperity and democratic values."*
— Harry Coker Jr., National Cyber Director

OCTOBER 2024

EXECUTIVE SUMMARY

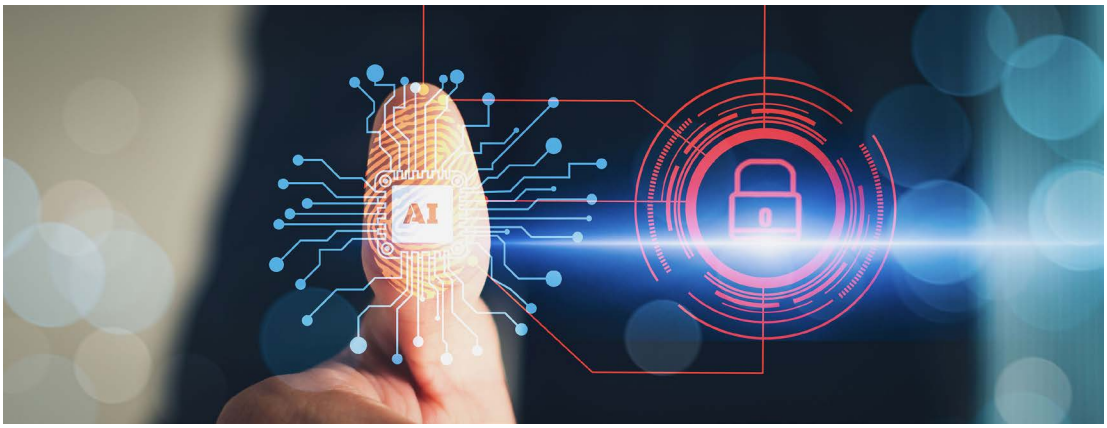
In a rapidly evolving digital landscape, cybersecurity is no longer solely a concern for the military and private sectors; it is also critically important for civilian government agencies. As cybersecurity threats grow more sophisticated, leveraging artificial intelligence (AI) becomes essential for protecting vital civilian infrastructure and services. This white paper, developed by the AFCEA International Cyber Committee, examines the transformative role of AI in enhancing cybersecurity across all sectors in the United States, and provides a comparative analysis of AI integration in Europe, Asia-Pacific and the Americas.

The paper underscores the commitment of the White House to leverage AI for cybersecurity purposes across our critical infrastructure, highlighted by directives such as the Executive Order on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence[1] and the White House memorandum M-24-10[2]. These directives aim to strengthen AI governance, appoint chief AI officers within federal agencies and establish comprehensive risk management frameworks to counter emerging cyber threats.

The integration of AI in cybersecurity is explored across defense, military and civilian agencies, as articulated in the 2023 National Cybersecurity Strategy[3] and the U.S. Department of Defense's 2023 Cyber Strategy Summary[4]. The document also discusses the broader AI integration strategy agencies at all levels are employing for real-time threat detection, automated responses to cyber incidents and predictive analytics to anticipate and mitigate potential threats, advocating for a unified approach to cybersecurity that includes comprehensive AI governance and risk management practices across all levels of government.

1 The White House. (2023). *Executive Order on Advancing American AI Leadership.* Retrieved from White House
2 Executive Office of the President, Office of Management and Budget (OMB). (2024). *Memorandum M-24-10: Advancing AI Governance and Risk Management.* Retrieved from White House
3 The White House. (2023). *National Cybersecurity Strategy.* Retrieved from White House
4 U.S. Department of Defense. (2023). *Summary of the 2023 Department of Defense Cyber Strategy.* Retrieved from Defense.gov

The paper explores the regional differences in AI adoption and regulation, with Europe focusing on regulatory compliance and ethical implications, Asia-Pacific on rapid technological adoption and innovation, and the Americas balancing innovation with strategic national security considerations.



Lastly, the paper highlights the trajectory of global and state legislation on AI ethics, advocating for a harmonized approach to manage the dual-use nature of AI technologies for both civilian and military purposes. It stresses the importance of international collaboration to develop standards that ensure AI's ethical use, particularly in critical sectors such as energy, transportation and public services.

In conclusion, "Navigating the Future of Cybersecurity With Artificial Intelligence" offers a roadmap for leveraging AI to enhance cybersecurity while managing associated risks. It calls for ongoing education and workforce development to equip professionals with the skills necessary to navigate the AI-driven cybersecurity landscape effectively. This paper serves as a crucial resource for policymakers, cybersecurity experts and industry leaders globally, providing insights for strategic decision-making to harness AI's potential responsibly and securely by outlining important recommendations regarding the application of AI into our cybersecurity technologies and operations of AI.

THE EVOLUTION AND IMPACT OF AI ACROSS DEFENSE, MILITARY OPERATIONS AND CIVILIAN AGENCIES

"Artificial intelligence (AI) is one of the most powerful, publicly accessible technologies of our time, and its continued evolution in 2023 presented opportunities and challenges for cyber risk management at scale." — 2024 Cybersecurity Posture

Since the 1940s, AI has progressively been integrated into defense and military operations, beginning with the early use of rudimentary algorithms for codebreaking during World War II[5]. As technology advanced, AI applications expanded to include automated decision-making systems, sophisticated simulations for training and strategy, and intelligent surveillance systems[6]. In recent decades, AI has been employed in autonomous vehicles, drones for reconnaissance and combat, and advanced cybersecurity measures. These technologies enhance situational awareness, optimize resource allocation and provide real-time data analysis, significantly improving operational efficiency and strategic planning in defense operations.

The Joint Artificial Intelligence Center (JAIC)[7] has profoundly influenced the progression of AI within the U.S. Department of Defense (DoD) and beyond since its establishment in 2018. The JAIC centralizes AI efforts, ensuring cohesive and strategic development and deployment of AI technologies across the DoD. By engaging with the AI industry financially, the JAIC fosters partnerships that drive innovation and accelerate the development of cutting-edge AI applications. It also plays a critical role in developing policies, standards and best practices

5 Bletchley Park. (2019). *The Codebreakers of Bletchley Park and the Role of Early AI in WWII.* Retrieved from BletchleyPark.org.uk

6 DARPA. (2020). *The Evolution of AI in Military Applications.* Retrieved from DARPA.mil

7 Department of Defense. (2018). *Establishment of the Joint Artificial Intelligence Center.* Retrieved from Defense.gov

for AI use within the DoD, ensuring responsible, ethical and secure deployment. Through initiatives like the AI and Data Accelerator (AIDA), the JAIC demonstrates how AI can enhance real-time operational capabilities in data-driven warfare by working directly with military personnel to identify and overcome implementation obstacles[8].

The JAIC's impact is further amplified by proposals to elevate its authority, enabling it to acquire its own technology and positioning it under the deputy secretary of defense. This elevation strengthens the JAIC's ability to drive rapid AI innovation and implementation. The 2022 merger of the JAIC with the Defense Digital Service and the Office of Advancing Analytics into the Chief Digital and Artificial Intelligence Office (CDAO) underscores a holistic approach to digital and AI transformation within the DoD[9]. This integration aligns AI efforts with broader digital initiatives, maximizing the impact of AI across all defense operations. The JAIC's initiatives have significantly advanced the DoD's AI capabilities, laying a foundation for continued innovation and leadership in AI technology both within the defense sector and in broader applications.

Currently, the National Institute of Standards and Technology (NIST) U.S. AI Safety Institute also plays a crucial role in advancing AI technologies, particularly in the context of defense[10]. The institute focuses on developing standards, guidelines and best practices to ensure the reliable and secure application of AI. By collaborating with various defense and military agencies, NIST aims to enhance the robustness and trustworthiness of AI systems. NIST's work includes the development of frameworks for AI risk management, ensuring that AI applications

8 JAIC. (2021). *AI and Data Accelerator Initiative.* Retrieved from JAIC.mil
9 U.S. Department of Defense. (2022). *Merger Announcement of JAIC, DDS, and OAA into CDAO.* Retrieved from Defense.gov
10 National Institute of Standards and Technology (NIST). (2020). *NIST AI Center of Excellence Overview.* Retrieved from NIST.gov

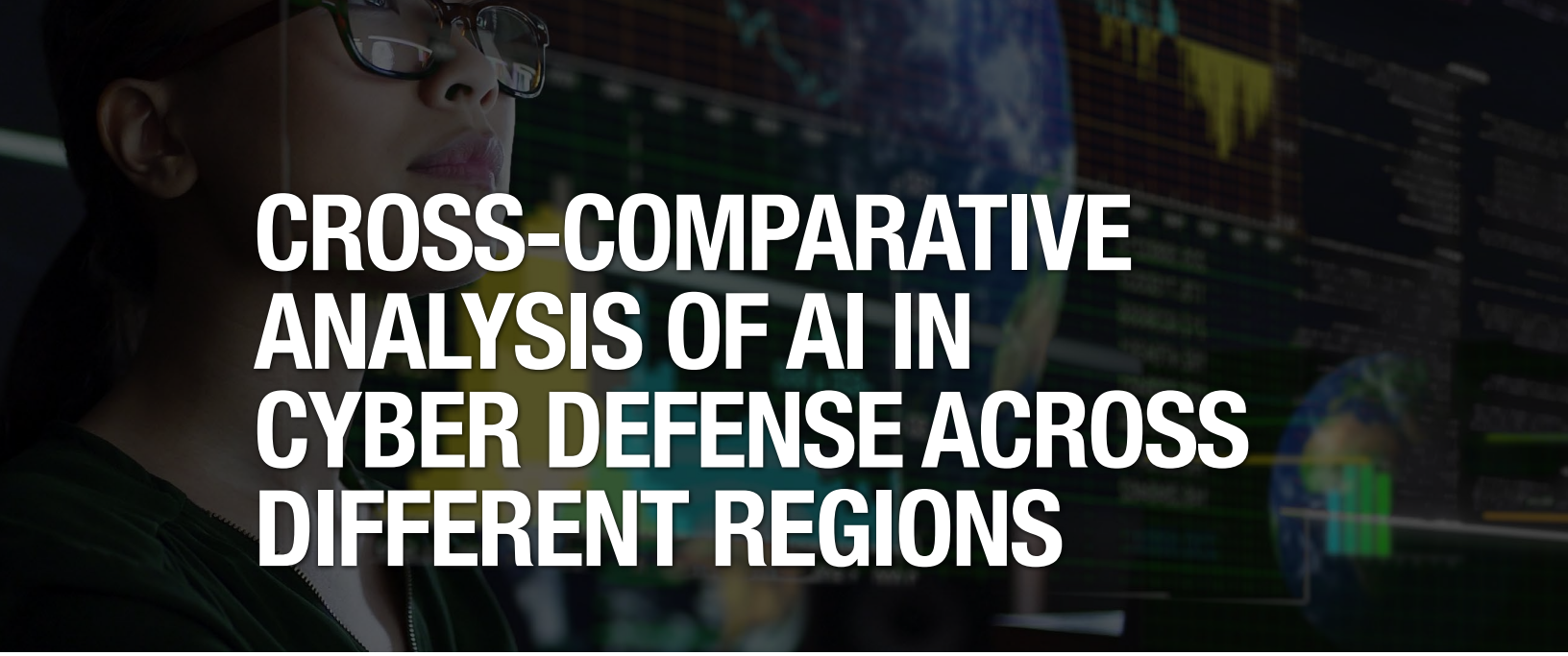
in defense are not only effective but also ethical and secure. This contribution is pivotal in maintaining the technological edge and operational superiority of modern military forces.

Informing the National Cybersecurity Community

This paper seeks to provide valuable insights and guidance to the national cybersecurity community by addressing the complex and evolving role of AI across the broader cybersecurity mission area. As AI becomes increasingly integrated into cyber defense strategies, it brings both unprecedented opportunities and significant challenges that must be navigated carefully. The potential of AI to enhance cybersecurity capabilities is vast, from improving threat detection and automating defenses to enabling proactive risk management. However, the introduction of AI also raises critical issues, such as the threat of adversarial AI,

ethical dilemmas and technical vulnerabilities within AI systems themselves. We explore these dual aspects—highlighting the existing opportunities that AI offers to strengthen cybersecurity while also identifying and addressing the challenges it presents. By providing targeted guidance for research and development, and suggesting effective strategies to mitigate cyber threats, this paper aims to equip cybersecurity professionals with the knowledge and tools necessary to harness AI's potential responsibly and effectively.

For detailed explanations and definitions of the AI terms mentioned throughout this document, please refer to Appendix A, which provides a comprehensive glossary covering a wide range of concepts, from core AI techniques and specialized models to human interaction, ethics and emerging AI technologies.



CROSS-COMPARATIVE ANALYSIS OF AI IN CYBER DEFENSE ACROSS DIFFERENT REGIONS

Cyber Defense Across Different Regions

Multiple government sectors across different regions are actively integrating AI into their cyber defense strategies, updating regulatory frameworks, identifying ethical considerations, and investing in technological advancements that shape AI deployment. Europe's regulatory focus ensures that AI applications in cybersecurity adhere to strict ethical guidelines, while Asia-Pacific countries rapidly adopt innovative AI technologies, sometimes outpacing regulatory development. In the Americas, balancing innovation with national security remains a priority, with a growing emphasis on integrating AI into public sector cybersecurity initiatives. This analysis reveals significant regional variations in the adoption and regulation of AI technologies, driven by differing cultural, political and economic contexts[11,12].

Figure Source CSIS.

11 United Nations. (2021). *Recommendation on the Ethics of Artificial Intelligence.* Retrieved from UNESCO
12 Organisation for Economic Co-operation and Development (OECD). (2019). *Recommendation of the Council on Artificial Intelligence.* Retrieved from OECD

Europe: Emphasis on Regulatory Compliance and Ethical AI

In Europe, the integration of AI into cyber defense is heavily influenced by regulatory compliance and the ethical implications of AI usage[13]. The General Data Protection Regulation (GDPR) is a testament to Europe's commitment to data privacy and security, setting stringent standards for data handling and processing. This regulatory framework extends to AI applications, ensuring that AI systems used in cybersecurity are transparent, accountable and respect user privacy[14]. European countries prioritize the development of AI technologies that adhere to ethical guidelines, which can sometimes slow down technological adoption but ensure robust and responsible AI deployment. This cautious approach aims to balance innovation with societal values, fostering trust in AI systems among the public.

Asia-Pacific: Rapid Technological Adoption and Innovation

The Asia-Pacific region is characterized by its rapid technological adoption and innovation, particularly in AI and cybersecurity. Countries like China, Japan[15] and South Korea[16] are at the forefront of AI research and development, deploying cutting-edge technologies at an accelerated pace. However, the regulatory landscape in the Asia-Pacific region is more varied, with some countries having well-defined regulations and others lagging behind. This disparity leads to a dynamic but fragmented approach to AI in cyber defense. For instance, China has made significant strides in AI capabilities, focusing on state-led initiatives and extensive data collection, albeit with less emphasis on privacy concerns compared to Europe[17]. The region's agility in adopting new technologies allows for swift advancements in AI-driven cybersecurity solutions, though this rapid pace also raises concerns about regulatory oversight and ethical considerations.

---

13 European Commission. (2021). *Proposal for a Regulation laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts.* Retrieved from European Commission

14 European Parliament and Council. (2016). *General Data Protection Regulation (GDPR).* Retrieved from GDPR.eu

15 Ministry of Internal Affairs and Communications, Japan. (2021). *AI Strategy 2021*. Retrieved from MIC Japan

16 Korea Internet & Security Agency (KISA). (2020). *Korea's AI Policies and Future Directions*. Retrieved from KISA

17 Kshetri, N. (2020). *The Rapid Rise of China's AI Firms: How This Will Affect the Global Market.* IEEE IT Professional, 22(1), 72-77. Retrieved from IEEE Xplore

Americas: Balancing Innovation With National Security

In the Americas, particularly in the United States, there is a distinct balance between fostering innovation and addressing strategic national security considerations. The U.S. has been proactive in integrating AI into its national defense mechanisms, with initiatives such as the establishment of the AI Security Center at the National Security Agency (NSA) exemplifying a targeted approach[18]. This center focuses on leveraging AI to enhance national security, emphasizing the importance of innovation in maintaining a competitive edge. The U.S. approach involves significant federal investment in AI research and development, coupled with policies that encourage public-private partnerships[19]. This strategy aims to harness the potential of AI while safeguarding critical infrastructure and addressing security challenges[20]. The state of regulation in each region reflects progress based on geopolitical considerations and the ability to get appropriate legislation and regulation enacted.

The 2022 National Security Strategy outlined the United States' strategic approach to safeguarding its interests and values in an increasingly complex global landscape[21]. This comprehensive strategy focused on addressing a range of security challenges, including great power competition, cybersecurity threats, climate change and global health crises. Emphasizing the importance of a whole-of-government approach, the strategy highlighted the need for diplomatic engagement, economic cooperation and military deterrence to promote a more stable and secure international environment. It also prioritized strengthening alliances and partnerships, underscoring the significance of working with like-minded nations to address shared security concerns and uphold democratic values. Also underscored, was the importance of emerging technologies, such as AI, quantum computing and biotechnology, in shaping the future security landscape. By emphasizing resilience, innovation and strategic foresight, the aim was to position the United States as a proactive and adaptive leader in addressing evolving security threats and promoting global stability.

---

18 National Security Agency (NSA). (2021). *Establishment of the AI Security Center.* Retrieved from NSA.gov

19 Executive Office of the President. (2020). *AI in Government Act of 2020.* Retrieved from Congress.gov

20 U.S. Department of Defense. (2021). *Summary of the 2020 Department of Defense AI Strategy.* Retrieved from Defense.gov

21 White House. (2022). *Biden-Harris Administration's National Security Strategy.* Retrieved from https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.

The cross-comparative analysis underscores the varied approaches to AI in cyber defense across different regions, each shaped by unique regulatory environments, cultural values and strategic priorities. Europe's focus on ethical AI and regulatory compliance, Asia-Pacific's rapid innovation and adoption, and the Americas' balance of innovation with national security considerations illustrate the diverse pathways through which AI is being integrated into global cybersecurity efforts. Understanding these regional differences is crucial for developing comprehensive and cohesive global strategies to address the evolving landscape of cyber threats.

LEGISLATIVE TRENDS IN AI FOR CYBERSECURITY

Legislative trends on the use of AI for cybersecurity purposes are evolving rapidly, reflecting the growing recognition of AI's potential and associated risks. In the European Union, the AI Act represents a significant step toward comprehensive regulation of AI systems[22,23]. The AI Act categorizes AI applications into different risk levels, with higher-risk systems subject to stricter regulations. Cybersecurity applications of AI, given their critical role in protecting sensitive data and infrastructure, are likely to fall into these higher-risk categories. This means that companies developing or deploying AI for cybersecurity in the EU will need to adhere to stringent requirements, including thorough risk assessments, robust data governance and ongoing monitoring to ensure compliance.

The AI Act also emphasizes the need for human oversight, ensuring that AI systems in cybersecurity are not operating autonomously without human intervention, especially in critical decision-making processes. This reflects a cautious approach to AI integration, aiming to mitigate potential risks while leveraging AI's capabilities to enhance cybersecurity defenses.

In the United States, while there is no overarching federal law specifically targeting AI ethics and cybersecurity, state-level legislation has been proactive. California leads with the California Consumer Privacy Act (CCPA), which includes provisions on AI accountability and consumer protection[24]. The state has also introduced bills like AB-13 to regulate government use of automated decision-making systems, highlighting the importance of transparency and ethical considerations in AI deployment[25]. New York has proposed bills such as S4824 ascertaining proper regulations regarding AI-enabled facial recognition technology and S9401 which mandates impact assessments

22 European Commission. (2021). *Proposal for a Regulation laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts*. Retrieved from European Commission

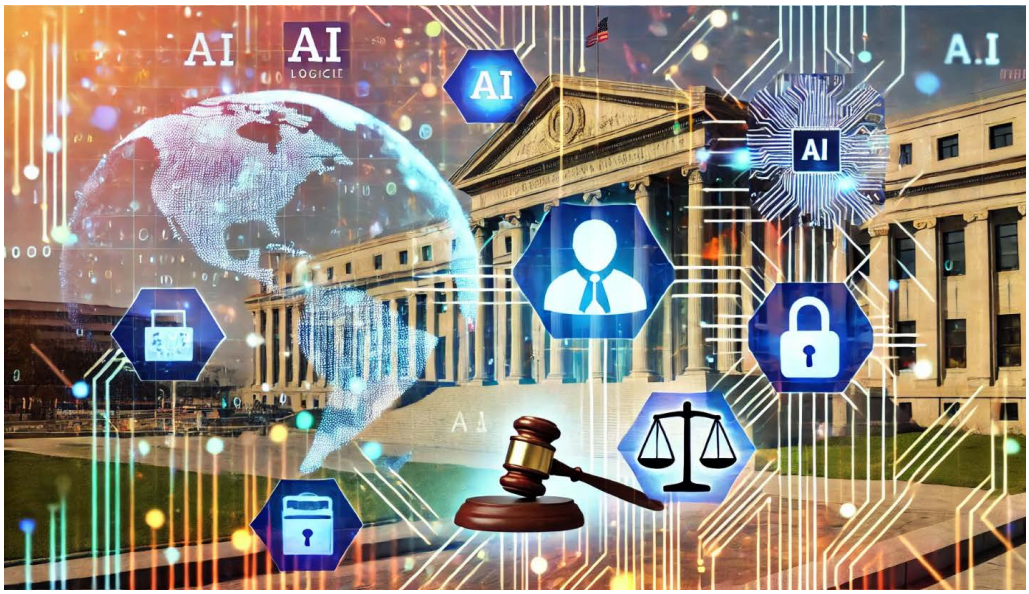
23 On August 1st, 2024, the European Artificial Intelligence Act (AI Act) entered into force.

24 California Legislature. (2018). *California Consumer Privacy Act (CCPA).* Retrieved from California Legislative Information

25 California Legislature. (2021). *AB-13 State Government: Automated Decision Systems.* Retrieved from California Legislative Information

before deploying AI systems[26,27]. Similarly, Washington state has enacted laws like SB-5116 to leverage AI in reducing greenhouse gas emissions, demonstrating the diverse applications of AI in legislative efforts[28].

Internationally, the United Nations has issued guidelines emphasizing ethical AI use, focusing on principles such as transparency, accountability and nondiscrimination[29]. These guidelines aim to provide a global framework for AI deployment, encouraging countries to adopt policies that promote ethical and secure AI practices. As AI continues to integrate into various sectors, including cybersecurity, these legislative trends reflect a growing commitment to harnessing AI's potential while safeguarding against its risks. By establishing clear regulations and guidelines, both at the national and international levels, policymakers aim to ensure that AI technologies contribute positively to society and enhance cybersecurity resilience.



AI-generated image

26 New York State Senate. (2023). *S4824 Bill Text - facial recognition technology study act.* Retrieved from NY State Senate

27 New York State Senate. (2023). *S9401 Bill Text - Establishes the New York workforce stabilization act requiring certain businesses to conduct artificial intelligence impact assessments on the application and use of such artificial intelligence.* Retrieved from NY State Senate

28 Washington State Legislature. (2019). SB 5116 - *Reducing Greenhouse Gas Emissions.* Retrieved from Washington State Legislature

29 United Nations. (2021). *Recommendation on the Ethics of Artificial Intelligence.* Retrieved from UNESCO

ADVANCEMENTS IN AI GOVERNANCE AND RISK MANAGEMENT

"The recent AI memorandum M-24-10 marks a significant step forward in advancing AI governance, innovation and risk management within federal agencies. This directive aims to seize AI's opportunities while managing its risks, particularly those affecting public rights and safety." — Shalanda D. Young, Director of the U.S. Office of Management and Budget

The recent AI memorandum M-24-10, issued by Shalanda D. Young, marks a significant step forward in advancing AI governance, innovation and risk management within federal agencies. This directive, consistent with the AI in Government Act of 2020[30], the Advancing American AI Act[31] and Executive Order 14110[32], aims to seize AI's opportunities while managing its risks, particularly those affecting public rights and safety[33]. The memorandum sets new requirements for AI governance, innovation and risk management, impacting the maturation of AI across the people, process and technology spectrums.

People

The memorandum mandates the designation of chief AI officers (CAIOs) in each agency, ensuring dedicated leadership and accountability for AI initiatives. This move will foster a culture of AI literacy and responsibility, driving agencies to recruit and retain AI talent. The CAIOs are tasked with coordinating AI activities, promoting AI innovation, managing risks and ensuring compliance with the memorandum's requirements. This leadership role will be crucial in building a workforce capable of leveraging AI technologies effectively and ethically, thus accelerating AI maturity within the federal government.

30 U.S. Congress. (2020). *AI in Government Act of 2020.* Retrieved from Congress.gov
31 U.S. Congress. (2021). *Advancing American AI Act.* Retrieved from Congress.gov
32 The White House. (2022). *Executive Order on Advancing American AI Leadership.* Retrieved from White House
33 Executive Office of the President, Office of Management and Budget (OMB). (2024). *Memorandum M-24-10: Advancing AI Governance and Risk Management*. Retrieved from White House

Process

The memorandum introduces robust governance structures and processes to manage AI's use in federal operations. Agencies are required to develop AI strategies, conduct impact assessments and follow minimum risk management practices for AI systems that impact public rights and safety. These processes ensure that AI deployments are transparent, accountable and aligned with the agency's mission and ethical standards. By standardizing AI governance practices, the memorandum aims to create a consistent approach to AI adoption and risk management across all federal agencies, thus streamlining processes and fostering a more mature AI ecosystem.

Technology

On the technology front, the memorandum emphasizes the need for agencies to develop and adopt AI responsibly. It requires agencies to test AI systems in real-world contexts, monitor their performance and mitigate emerging risks. The focus on data quality, cybersecurity and information technology infrastructure will enhance the reliability and effectiveness of AI technologies. Moreover, the directive encourages the sharing and reuse of AI models, code and data across agencies, promoting collaboration and innovation. These technological advancements will not only improve the functionality and efficiency of AI systems but also ensure they are used in a manner that protects public safety and rights.

The National Artificial Intelligence Initiative expands on these efforts and represents a concerted effort by the government to harness the transformative potential of AI technologies across various sectors[34]. This initiative aims to accelerate AI research and development, promote ethical AI deployment and advance the United States' competitiveness in the global AI landscape. Through strategic investments in AI innovation, workforce training and infrastructure development, the National Artificial Intelligence Initiative seeks to drive economic growth, enhance national security and address societal challenges through AI-driven solutions.

34 National Artificial Intelligence Initiative Office. (2022). *National Artificial Intelligence Initiative.* Retrieved from https://www.ai.gov

The initiative also prioritizes collaboration between government agencies, industry partners, academic institutions and other stakeholders to foster a vibrant AI ecosystem that fosters innovation and responsible AI use. By promoting the responsible development and adoption of AI technologies, the initiative aims to ensure that AI tools and systems align with ethical guidelines, respect privacy rights and promote inclusivity and fairness. Through a comprehensive and coordinated approach, the National Artificial Intelligence Initiative aims to position the United States as a global leader in AI innovation and drive progress toward a future enriched by the benefits of AI.

LEGISLATIVE DEVELOPMENTS IN AI FOR CYBERSECURITY AND INNOVATION

"By codifying principles of responsible AI use, the U.S. is driving international policy formulation, ensuring AI applications are not only effective but also secure and ethically aligned." — Michael C. Horowitz, U.S. Department of Defense

Future of Artificial Intelligence Innovation Act of 2024 (S.4178)

The Future of Artificial Intelligence Innovation Act of 2024 aims to establish a robust framework for AI standards, metrics and evaluation tools, fostering an environment conducive to innovation and capacity building across the AI industry[35]. The bill addresses key drivers across people, processes and technology, promoting a comprehensive approach to AI development and deployment. This initiative seeks to ensure that the United States remains at the forefront of AI advancements by setting high standards and encouraging continuous improvement in AI technologies.

Creating Resources for Every American To Experiment With Artificial Intelligence Act of 2023 (CREATE AI Act of 2023)

The CREATE AI Act of 2023 seeks to democratize access to computational resources and large datasets critical for cutting-edge AI research, traditionally limited to large technology companies[36]. The National Artificial Intelligence Research Resource (NAIRR) is designed to foster innovation, support diverse talent and maintain U.S. leadership in AI by providing equitable access to AI resources. By leveling the playing field, this act aims to spur creativity and innovation across a broader range of researchers and developers, ensuring that breakthroughs in AI are not confined to a few large entities.

35 U.S. Congress. (2024). *Future of Artificial Intelligence Innovation Act of 2024.* Retrieved from Congress.gov
36 U.S. Congress. (2023). *CREATE AI Act of 2023.* Retrieved from Congress.gov

National Security Commission on Artificial Intelligence (NSCAI) Final Report

The NSCAI Final Report provides a strategic roadmap for the United States to maintain and enhance its leadership in AI and related technologies. It emphasizes AI's critical role in national security, advocating for its integration into defense systems to address emerging threats effectively. Key recommendations include expanding the talent pool, strengthening research and development infrastructure and ensuring that AI advancements align with democratic values, such as privacy and civil liberties. This comprehensive approach aims to balance the imperatives of national security with the ethical considerations inherent in AI deployment.

National Cybersecurity Strategy and Implementation Plan

President Joe Biden's National Cybersecurity Strategy emphasizes a comprehensive approach to securing critical infrastructure, disrupting threat actors and investing in future resilience[37]. AI plays a pivotal role in defending critical infrastructure by enabling real-time monitoring, predictive analytics and automated response mechanisms. The strategy also leverages AI to shape market forces, encouraging the adoption of secure-by-design and secure-by-default technologies. The associated forward-looking implementation plan integrates AI into the core of cybersecurity efforts, ensuring that the United States can preemptively address threats and maintain robust defenses against cyber attacks[38].

37 The White House. (2023). *National Cybersecurity Strategy.* Retrieved from White House
38 The White House. (2023). *National Cybersecurity Implementation Plan.* Retrieved from White House

AI: NAVIGATING CHALLENGES AND OPPORTUNITIES IN CYBERSECURITY[39]

"[It] is necessary to fundamentally shift the underlying dynamics of the digital world to make it defensible, resilient and aligned with our values. If we succeed, the digital ecosystem can be a strong foundation for a prosperous, connected future that benefits every American. While we remain postured to forcefully respond to malicious cyber threats, we will not let our adversaries dictate our path forward." – 2024 Cybersecurity Posture – Harry Coker Jr., National Cyber Director

AI presents both significant challenges and immense opportunities for the future of cybersecurity. We are already witnessing heightened innovation in the area of commercial cybersecurity products with AI capabilities designed to detect anomalous behavior indicative of cyber exploits and attacks. AI has the power to dynamically adjust cyber defenses based on data from external cybersecurity reporting, intrusion detection systems and other tools. It also holds the potential to create "on-the-fly" antivirus software tailored to combat new exploits and zero-day vulnerabilities.

However, adversaries are equally likely to harness AI for malicious purposes. AI can be used to probe defenses, launch and control rapidly changing attacks, identify previously unknown vulnerabilities and craft malware opportunistically. Generative AI could develop both defensive and offensive strategies, possibly integrating these strategies with disinformation campaigns. Current and prospective cybersecurity technologies must rise to the challenge of adversarial AI use while simultaneously enhancing security posture initiatives, like zero trust, by automating and increasing the efficiency of user-to-resource mediation required by zero-trust frameworks.

AI systems themselves may face cybersecurity challenges. Concerns have emerged regarding the security of AI software development environments

39 National Security Commission on Artificial Intelligence. (2021). *Final Report.* Retrieved from NSCAI.gov

and strategies that could cause AI systems to misinterpret reality or generate "hallucinations"—dangerously incorrect inferences that could result in severe damage to infrastructures and human life.

The integration of AI into cybersecurity presents both significant challenges and promising opportunities. As AI becomes increasingly embedded in cyber defense strategies, it is essential to carefully navigate the ethical, legal, technical and strategic implications of its use. Challenges such as ensuring compliance with international laws, managing technical vulnerabilities and avoiding an arms race are critical considerations that need to be addressed to mitigate potential risks. Simultaneously, AI offers substantial opportunities to enhance situational awareness, automate defense systems and optimize logistics and supply chain management in military operations. To explore these topics in greater detail, including the nuances of policy challenges associated with autonomous intelligent cyber defense agents (AICAs) and the strategic opportunities AI provides in cybersecurity, please refer to Appendix B of this document.

AI-generated image

Government and Industry Case Studies

The transformative role of AI in cybersecurity is evidenced by numerous case studies across both government and industry sectors. AI's capabilities in detecting, analyzing and responding to complex cyber threats have proven to be more effective than traditional methods, offering enhanced security and operational resilience. For a more detailed analysis of these AI applications and the strategies to minimize cybersecurity risks while maximizing adoption, please refer to Appendix C, which highlights various real-world applications of AI in cybersecurity, showcasing its impact on threat detection, network security, fraud prevention and more. These case studies, which include AI-driven solutions by leading companies like Darktrace, NVIDIA, Cisco and IBM, as well as implementations in government agencies such as the U.S. Department of Homeland Security (DHS) and the U.K. government, illustrate the broad spectrum of AI's influence.

Unlocking AI's Potential in Defense, Military and Commercial Sectors

As artificial intelligence (AI) continues to advance, its transformative potential is being harnessed across various sectors, including defense, military operations, and commercial industries. This section explores the significant impact AI is having on enhancing cybersecurity, operational efficiency, and strategic decision-making.

AI is revolutionizing the way defense and military operations are conducted. From autonomous systems to advanced cybersecurity measures, the integration of AI technologies is reshaping the landscape. Key areas of impact include:

- Autonomous Systems and Drones
- Cybersecurity & Threat Detection
- Intelligence, Surveillance, and Reconnaissance (ISR)

The commercial sector is also leveraging AI to drive innovation and improve operational efficiency. Key applications include:

- Cybersecurity enhancements
- Supply chain optimization
- Fraud detection

While AI presents significant opportunities for enhancing security and efficiency, it also poses challenges that must be addressed, including ethical considerations and technical vulnerabilities.

Ethical Considerations

The deployment of AI raises ethical questions regarding privacy, accountability, and decision-making processes. Organizations must develop robust governance frameworks to ensure responsible AI use.

Technical Vulnerabilities

AI systems can be susceptible to attacks, including adversarial attacks that exploit weaknesses in algorithms. Ensuring the robustness and security of AI technologies is crucial for maintaining trust and effectiveness.

Unlocking AI's potential in defense, military, and commercial sectors requires a strategic approach that balances innovation with ethical considerations and robust governance. By leveraging AI technologies, organizations can enhance their operational capabilities, improve cybersecurity, and drive sustainable growth. Collaboration across sectors will be vital in navigating the complexities of AI integration and ensuring its responsible use for national security and public service. For a more detailed analysis of these AI applications and the strategies to minimize cybersecurity risks while maximizing adoption, please refer to Appendix D.

AI Applications To Minimize Cybersecurity Risks and Maximize Adoption and Use[40]

The Software Engineering Institute's (SEI's) recent publications provide a comprehensive overview of the critical advancements, challenges and opportunities in leveraging AI to enhance cybersecurity and software engineering practices[41]. The topics covered include the use of large language models (LLMs) in cybersecurity, generative AI in software development, zero-trust architectures, national security applications of AI and the cybersecurity implications of quantum computing. The findings emphasize the need for rigorous evaluation of LLMs to prevent spurious results and ensure their alignment with real-world cybersecurity tasks. The publications also address the integration of generative AI tools, highlighting the importance of expert oversight to mitigate security risks and unforeseen failures. In the context of supply chain risk management, effective governance is crucial to maintaining operational resilience, especially in light of ongoing cyber threats like those related to Log4j exploits. The research further explores how tailored applications of AI can enhance national security and offers guidance on developing robust evaluation criteria for AI tools. Additionally, it advocates for the responsible integration of AI into software engineering processes and the importance of advancing quantum computing security. Collectively, these insights offer a strategic roadmap for organizations to navigate AI adoption, balancing the mitigation of cybersecurity risks with the maximization of innovation opportunities.

For a more comprehensive exploration of these topics, including detailed insights and recommendations on leveraging AI to enhance cybersecurity, and software engineering practices and minimizing risk, please refer to Appendix E.

40 Adewusi, A., & Daraojimba, D. O. (2024). *Artificial Intelligence in Cybersecurity: Protecting National Infrastructure.* Retrieved from ResearchGate

41 Software Engineering Institute (SEI). (2024). *AI and Cybersecurity Publications.* Retrieved from SEI

RECOMMENDATIONS

The rapid evolution of AI presents both unprecedented opportunities and complex challenges for defense and military operations. As these technologies continue to advance, executive defense personnel and military leaders must adopt strategic approaches to fully leverage AI's potential while mitigating associated risks. The following recommendations aim to guide leaders in integrating AI into their operations effectively, enhancing security through zero-trust architectures, fostering innovation through industry collaboration and ensuring robust governance frameworks for ethical AI deployment. These steps are essential for maintaining technological superiority, operational efficiency and overall mission success in the modern defense landscape.

Recommendations for Executive Defense Personnel and Military Leaders

As advancements in AI continue to reshape the landscape of defense and military operations, it is imperative for executive defense personnel and military leaders to stay ahead of the curve. The following recommendations focus on integrating AI technologies to enhance operational capabilities, adopting zero-trust architectures for robust security, fostering collaboration with the AI industry to drive innovation and prioritizing AI governance to ensure ethical and responsible deployment. By embracing these strategies, defense leaders can significantly improve situational awareness, decision-making and operational efficiency while safeguarding against both internal and external threats.

- **Embrace AI Integration:** Invest in advanced AI technologies to enhance operational capabilities. This includes autonomous systems, drones, and AI-driven intelligence, surveillance and reconnaissance (ISR) systems. These technologies can improve situational awareness, decision-making and operational efficiency, reducing risks to personnel and assets.
- **Adopt Zero-Trust Architectures:** Implement zero-trust security models enhanced by AI. This involves continuous monitoring, dynamic access control and real-time threat detection to protect against both internal and external threats. Ensure all access requests are authenticated, authorized and encrypted.
- **Collaborate With the AI Industry:** Foster partnerships with the AI industry to drive innovation and accelerate the development of cutting-edge AI applications. Engage with initiatives like the CDAO to stay at the forefront of AI advancements and ensure cohesive deployment across defense operations.
- **Prioritize AI Governance:** Develop robust governance structures and processes for AI deployment. Designate CAIOs to oversee AI initiatives, promote AI literacy and ensure ethical and responsible use of AI technologies. Conduct regular impact assessments and risk management practices.

Recommendations for Civilian Government Leaders

As AI continues to advance, its integration into civilian government operations is becoming increasingly essential for enhancing cybersecurity, improving public service delivery and ensuring the ethical use of emerging technologies. Civilian government leaders play a pivotal role in shaping the strategies and frameworks that will guide AI deployment across public sector institutions. The recommendations outlined below provide a strategic roadmap for leveraging AI effectively while addressing the unique challenges and responsibilities faced by civilian agencies. These recommendations emphasize the importance of robust AI governance, enhanced cybersecurity measures and fostering collaboration across government, private sector and academic institutions to build a resilient and secure public infrastructure.

- **Strengthen AI Governance:** Establish robust AI governance frameworks within civilian government agencies to ensure responsible AI deployment. This includes appointing CAIOs, conducting regular risk assessments and adhering to ethical guidelines.
- **Enhance Public Sector Cybersecurity:** Integrate AI into public sector cybersecurity strategies to improve threat detection, response times and overall security posture. Focus on protecting critical infrastructure and public services from cyber threats.
- **Promote Collaboration:** Encourage collaboration between civilian government agencies, private sector partners and academic institutions to foster innovation in AI-driven cybersecurity. Share best practices and develop joint initiatives to enhance cybersecurity resilience across all sectors.

Recommendations for Protecting the National Infrastructure

As the digital landscape continues to evolve, the protection of national infrastructure becomes increasingly critical, demanding innovative approaches that can keep pace with emerging threats. AI offers powerful tools to enhance the security, resilience and efficiency of vital systems. This section outlines key recommendations for leveraging AI to safeguard critical infrastructure. From enhancing cybersecurity measures with real-time threat detection and automated defenses to implementing predictive analytics for proactive risk management,

these strategies emphasize the importance of using AI to stay ahead of potential disruptions. Additionally, adopting AI-powered surveillance systems for continuous monitoring and collaborating with leading organizations to develop robust standards and best practices are essential steps to ensure the ethical and secure application of AI in protecting our nation's most essential assets.

- **Enhance Cybersecurity Measures:** Utilize AI for real-time threat detection, automated defense mechanisms and proactive risk management. Implement AI-driven systems to analyze data, detect anomalies and respond to cyber threats swiftly. Prioritize the protection of critical infrastructure from evolving cyber threats.
- **Implement Predictive Analytics:** Leverage AI for predictive analytics in supply chain security and infrastructure maintenance. This can help identify potential risks and disruptions, allowing for proactive measures to ensure continuity and security.
- **Adopt AI in Surveillance and Monitoring:** Deploy AI-powered surveillance systems for continuous monitoring of critical infrastructure. AI can process data from various sensors and detect unusual activities, enabling timely interventions to prevent potential threats.
- **Collaborate on Standards and Best Practices:** Work with organizations like the NIST AI Safety Institute to develop standards, guidelines and best practices for the reliable and secure application of AI. Ensure AI systems in critical infrastructure are ethical, robust and trustworthy.

Recommendations for Policymakers

As AI rapidly transforms multiple sectors, policymakers play a crucial role in shaping the frameworks that govern its development and deployment. Establishing comprehensive AI legislation is vital to creating a balanced environment that fosters innovation while ensuring safety, ethics and accountability. This section offers key recommendations for policymakers, emphasizing the need to develop robust legal frameworks, promote ethical AI use and support AI research and development. By enhancing AI governance and risk management within government agencies and fostering international collaboration, policymakers can ensure that AI technologies are deployed responsibly and effectively, aligning with societal values and global standards. These recommendations are designed to guide policymakers in crafting laws and policies that not only advance AI innovation but also safeguard the public interest in this rapidly evolving field.

- **Develop Comprehensive AI Legislation:** Enact laws that establish a robust framework for AI standards, metrics and evaluation tools. The Future of Artificial Intelligence Innovation Act of 2024 and similar bills should address key drivers across people, processes and technology, fostering an environment conducive to innovation and capacity building.
- **Promote Ethical AI Use:** Emphasize transparency, accountability and nondiscrimination in AI deployment. Encourage policies that ensure AI systems are developed and used responsibly, with a focus on ethical considerations and societal values.
- **Support AI Research and Development:** Provide equitable access to AI resources through initiatives like the CREATE AI Act of 2023. Democratize access to computational resources and large datasets to foster innovation and support diverse talent in AI research.
- **Enhance AI Governance and Risk Management:** Implement directives like memorandum M-24-10 to advance AI governance within federal agencies. Designate CAIOs to oversee AI initiatives, promote innovation and manage risks. Develop AI strategies and conduct impact assessments to ensure ethical and responsible AI use.
- **Foster International Collaboration:** Encourage international collaboration to develop global standards and guidelines for AI use. Align with United Nations guidelines on ethical AI deployment, and work toward harmonized regulations to manage the dual-use nature of AI technologies.

CONCLUSION

The integration of AI into cybersecurity strategies represents a pivotal shift toward more resilient, responsive and adaptive defense mechanisms against cyber threats, especially for critical infrastructures. As AI continues to shape the future of cybersecurity, it is essential for civilian government agencies to embrace these technologies to protect critical infrastructure and public services. By integrating AI into their cybersecurity strategies, civilian governments can enhance their ability to detect and respond to cyber threats, safeguard public trust and ensure the continued delivery of essential services in an increasingly digital world.

This white paper also highlights the necessity of a balanced, informed approach that fosters innovation and addresses the complexities of governance and ethical implications across different global regions. As the U.S. and other nations continue to refine their national strategies and international cooperation, the focus must remain on creating robust frameworks that leverage AI's capabilities to enhance security while safeguarding civil liberties and ensuring equitable outcomes. By fostering a collaborative international environment that encourages the sharing of knowledge and best practices, we can better harness AI's transformative power and secure our critical infrastructures against the evolving landscape of cyber threats.

The AFCEA Cyber Committee looks forward to engaging with stakeholders in government and industry who are likely to employ AI-based cybersecurity, as well as those responsible for the research and development of advanced AI-based cybersecurity technologies.

APPENDICES

Appendix A – AI Glossary

1. Core AI Concepts and Techniques

- **Algorithm:** A set of rules or instructions given to an AI/ML model or other computer systems to help them perform a task.
- **Artificial Intelligence (AI):** A field of computer science aimed at building machines capable of performing tasks that typically require human intelligence. These tasks include decision-making, speech recognition, visual perception and language translation.
- **Bayesian Networks:** A type of probabilistic graphical model that uses Bayesian inference for probability computations. Bayesian networks aim to model conditional dependence, and therefore causation, by representing conditional dependence by edges in a directed graph.
- **Convolutional Neural Network (CNN):** A class of deep neural networks, most commonly applied to analyzing visual imagery. CNNs use a variation of multilayer perceptrons designed to require minimal preprocessing.
- **Deep Learning:** A subset of machine learning that uses neural networks with many layers (deep networks) to analyze various factors of data. It is particularly useful for tasks such as image and speech recognition.
- **Decision Trees:** A decision support tool that uses a tree-like model of decisions and their possible consequences, including chance event outcomes, resource costs and utility. It is one way to display an algorithm that only contains conditional control statements.
- **Exhaustive Learning:** A theoretical model of learning where the learning algorithm is iterated until no further improvements can be made. It's often more a conceptual model than one used in practical applications due to computational constraints.
- **Federated Learning:** This technique allows multiple decentralized devices to collaboratively learn a shared model while keeping their data locally, enhancing privacy and security.

- **Gradient Boosting Machines (GBM):** A machine learning technique used for regression and classification problems, which produces a prediction model in the form of an ensemble of weak prediction models, typically decision trees.
- **Hyperparameter Tuning:** The process of selecting a set of optimal hyperparameters for a learning algorithm. A hyperparameter is a parameter whose value is set before the learning process begins.
- **Long Short-Term Memory (LSTM):** A special kind of recurrent neural network (RNN), capable of learning long-term dependencies. LSTMs are explicitly designed to avoid the long-term dependency problem, remembering information for long periods.
- **Machine Learning (ML):** A subset of AI that involves training algorithms to learn from and make predictions or decisions based on data, without being explicitly programmed.
- **Model Overfitting:** This occurs when a statistical model or machine learning algorithm captures the noise of the data rather than the intended outputs. Overfitting is more likely with nonparametric and nonlinear models that have more flexibility when learning a target function.
- **Model Underfitting:** This occurs when a statistical model or machine learning algorithm cannot capture the underlying trend of the data. Underfitting would occur, for example, if fitting a linear model to nonlinear data. Such a model would have poor predictive performance.
- **Multilayer Perceptron:** A type of feedforward neural network consisting of fully connected neurons with a nonlinear kind of activation function. It is widely used to distinguish data that is not linearly separable.
- **Neural Architecture Search (NAS):** An automated method for designing neural network architectures. NAS algorithms iteratively search for the best architecture by optimizing predefined criteria, improving the efficiency and performance of AI models.
- **Neural Network:** A series of algorithms that attempt to recognize underlying relationships in a set of data through a process that mimics the way the human brain operates.
- **Principal Component Analysis (PCA):** A statistical procedure that uses an orthogonal transformation to convert a set of observations of possibly correlated variables into a set of values of linearly uncorrelated variables called principal components.

- **Recurrent Neural Network (RNN):** A type of neural network where connections between nodes form a directed graph along a temporal sequence. This allows it to exhibit temporal dynamic behavior for a time sequence. RNNs are used in applications like language modeling and speech recognition.
- **Reinforcement Learning:** A type of learning where an agent learns to behave in an environment by performing actions and seeing the results.
- **Supervised Learning:** A type of machine learning where the model is trained on labeled data, i.e., data that includes the input and the correct output.
- **Support Vector Machines (SVM):** A set of supervised learning methods used for classification, regression and outlier detection. The advantage of SVMs is their effectiveness in high-dimensional spaces and their use in cases where the number of dimensions exceeds the number of samples.
- **Transfer Learning:** A research problem in machine learning that focuses on storing knowledge gained while solving one problem and applying it to a different but related problem. For example, using a model trained in one language to bootstrap learning in another language.
- **Unsupervised Learning:** A type of machine learning used to draw inferences from datasets consisting of input data without labeled responses.

2. Specialized AI Models and Methods

- **Adversarial Machine Learning:** A technique employed in the field of machine learning that attempts to fool models through malicious input. This can be used to understand the flaws and vulnerabilities of AI models.
- **Autoencoder:** A special type of neural network that is trained to copy its input to its output. For example, given an image of a handwritten digit, an autoencoder first encodes the image into a lower dimensional latent representation then decodes the latent representation back to an image.
- **Automated Machine Learning (AutoML):** The method of automating the end-to-end process of applying machine learning to real-world problems. It covers the complete pipeline from the raw dataset to the deployable machine learning model.
- **Capsule Networks (CapsNets):** A type of artificial neural network that can be used to better model hierarchical relationships. The idea is to add structures called “capsules” to a CNN and to use a dynamic routing algorithm to ensure that the output of each capsule is sent to appropriate parent capsules in the next layer.

- **Dimensionality Reduction:** The process of reducing the number of random variables under consideration by obtaining a set of principal variables. Techniques such as PCA, t-distributed stochastic neighbor embedding (t-SNE) and others are used.
- **Expert System:** A computer system emulating the decision-making ability of a human expert. Expert systems are designed to solve complex problems by reasoning through bodies of knowledge, represented mainly as if-then rules rather than through conventional procedural code.
- **Few-Shot Learning:** A machine learning method that enables a model to learn information about categories from very few training examples, making it useful for applications with limited labeled data.
- **Generative Adversarial Network (GAN):** A class of machine learning frameworks designed by Ian Goodfellow and his colleagues in 2014. Two neural networks contest with each other in a game (in the sense of game theory, often but not always in the form of a zero-sum game).
- **Generative AI:** This type of AI refers to algorithms that can be used to create content, such as images, videos and text, which resemble human-created content. It includes techniques like generative adversarial networks (GANs) and variational autoencoders (VAEs).
- **Iterative Dichotomiser 3 (ID3):** An algorithm used to generate a decision tree. ID3 is typically used in machine learning and natural language processing. The algorithm creates a multiway tree, finding for each node (i.e., in a greedy manner) the categorical feature that will yield the largest information gain for categorical targets.
- **Quantum Machine Learning:** A research area at the intersection of quantum computing and machine learning. Quantum computers use quantum bits (qubits), which can exist in multiple states simultaneously, potentially allowing them to process information in ways that traditional computers cannot.
- **Random Forest:** An ensemble learning method for classification, regression and other tasks that operates by constructing a multitude of decision trees at training time. For classification tasks, the output of the random forest is the class selected by most trees.
- **Self-Supervised Learning:** A form of unsupervised learning where the system learns to predict part of its input from other parts, reducing the need for large amounts of labeled data.

- **Transformers:** A type of deep learning model that has been designed to handle sequential data, like text, for tasks such as translation and text summarization. Unlike previous models that process data in order, transformers allow for much more parallelization and have significantly improved the performance of many natural language processing tasks.
- **Variational Autoencoder (VAE):** A type of autoencoder that provides a probabilistic manner for describing an observation in latent space. Unlike a traditional autoencoder, which maps the input onto a latent vector, VAE maps the input data into the parameters of a probability distribution, such as the mean and variance of a Gaussian distribution.

3. AI in Human Interaction and Ethics

- **AI Governance:** The idea of legal and ethical policies and guidelines that govern the AI life cycle. This includes how AI systems are researched, developed, trained, controlled and deployed to ensure they benefit individuals and society as a whole.
- **Bias:** In AI, bias is often a nonrandom error in a model's predictions due to erroneous assumptions in the machine learning process. Bias can arise from the data used to train the algorithm if that data has skewed representations or incomplete features.
- **Chatbot:** A software application used to conduct an online chat conversation via text or text to speech, in lieu of providing direct contact with a live human agent. It is designed to convincingly simulate the way a human would behave as a conversational partner.
- **Computer Vision:** A field of AI that trains computers to interpret and understand the visual world. Machines can accurately identify and classify objects—and then react to what they "see"—using digital images from cameras, videos and deep learning models.
- **Data Privacy:** The consideration of how data is collected, stored and used, ensuring compliance with regulations like GDPR and maintaining user trust.
- **Ethics in AI:** Concerns the moral implications and decisions made during the creation and implementation of AI technologies. This includes considerations of fairness, accountability, transparency and potential impacts on society.
- **Explainable AI (XAI):** Refers to methods and techniques in the application of AI technology such that the results of the solution can be understood by human experts. It contrasts with the concept of the "black box" in machine learning where even their designers cannot explain why the AI arrived at a specific decision.

- **Fairness in AI:** Strategies and methodologies to ensure AI systems do not perpetuate biases or inequalities, fostering equitable outcomes across diverse populations.
- **Natural Language Generation (NLG):** The process of using AI to generate natural language text from structured data. It is used in various applications, such as generating textual weather forecasts from data.
- **Natural Language Processing (NLP):** A field of AI focused on the interaction between computers and humans through natural language. The goal is to read, decipher, understand and make sense of human languages in a valuable way.
- **Semantic AI:** Refers to aspects of AI that involve understanding the meanings and relationships of words and concepts in human language. It is often applied in natural language processing tasks.

4. AI Applications and Emerging Technologies

- **Anomaly Detection:** The identification of rare items, events or observations that raise suspicions by differing significantly from the majority of the data. This is applicable in various domains, including fraud detection, network security, fault detection and system health monitoring.
- **Augmented Reality (AR) and Virtual Reality (VR):** AR enhances the real world with digital elements such as visuals, sounds or other sensory stimuli, while VR creates a completely artificial environment. Both can utilize AI to enhance user interactions.
- **Data Mining:** The process of discovering patterns and relationships in large volumes of data by using machine learning, statistics and database systems.
- **Digital Twins:** Virtual replicas of physical systems used to simulate, predict and optimize performance. In cybersecurity, digital twins can help model and protect infrastructure.
- **Edge AI:** The deployment of AI algorithms directly on a hardware device where data is generated (like smartphones, IoT devices, etc.), allowing for real-time data processing without the need for internet connectivity.
- **F1 Score:** The harmonic mean of precision and recall. It is a measure of a test's accuracy. The F1 score reaches its best value at 1 (perfect precision and recall) and worst at 0.
- **Natural Language Understanding (NLU):** An AI subfield focusing on machine reading comprehension. NLU systems interpret and understand human language in a nuanced way, enabling more sophisticated interactions.

- **Precision and Recall:** Performance metrics used to evaluate the relevance of results in machine learning. Precision is the fraction of relevant instances among the retrieved instances, while recall is the fraction of relevant instances that were retrieved.
- **Recommender Systems:** A subclass of information filtering systems that seeks to predict the “rating” or “preference” a user would give to an item. They are used extensively in recommending movies, music, products and even social media content.
- **Robotics:** The branch of technology that deals with the design, construction, operation and use of robots, often incorporating AI systems to handle tasks such as navigation, motor control and decision-making.

Appendix B – Challenges and Opportunities in AI Cybersecurity

Challenges

The integration of AI into cybersecurity brings forth several critical challenges that require careful consideration and management:

- **Ethical and Legal Concerns:** The use of AI in cybersecurity raises significant ethical and legal questions. Ensuring compliance with international humanitarian law and principles of distinction, proportionality and necessity is crucial. There are also concerns about accountability and responsibility for AI-driven actions.
- **Technical and Operational Risks:** AI technologies can introduce new risks. AI systems can be vulnerable to hacking, manipulation and malfunctions. Ensuring the reliability and robustness of AI systems in the face of adversarial attacks is essential. Overreliance on AI could lead to critical failures if systems are compromised or malfunction.
- **Escalation and Arms Race:** The deployment of AI in cybersecurity can lead to an arms race and increase the risk of conflict escalation. As nations develop advanced AI systems, there is a risk of an arms race that could destabilize global security. The rapid pace of AI development can outstrip the establishment of international norms and agreements.
- **Strategic and Political Implications:** The use of AI in cybersecurity has far-reaching strategic and political implications. AI can alter the balance of power between nations, potentially leading to geopolitical instability. The deployment of AI can have unforeseen consequences, affecting civilian populations and infrastructure.

Navigating Policy Challenges in AI Cyber Defense

The deployment of AICAs introduces complex policy issues, particularly within the rapidly evolving global information technology ecosystem. This ecosystem, characterized by extensive connectivity through billions of IoT devices, advanced 5G and future networks, and interconnected critical infrastructures, necessitates a nuanced approach to AICA deployment. Policies must ensure that AICA operations are effective yet secure and ethical. The "persistent engagement" and "defend forward" strategies exemplify proactive measures the U.S. employs, necessitating precise calibration of AICA tools to achieve strategic objectives without unintended escalation. These strategies highlight the importance of continuous adaptation of civil and military doctrines to effectively integrate AICAs into comprehensive cyber defense frameworks. The dynamic nature of the information ecosystem underscores the need for robust policy frameworks to guide the ethical and secure use of AICAs, ultimately ensuring the protection of national security and critical infrastructures while maintaining public trust and compliance with international norms.

Opportunities

The application of AI in cybersecurity offers significant opportunities for enhancing security measures and operational efficiency:

- **Enhanced Situational Awareness and Decision-Making:** AI can significantly improve situational awareness and decision-making processes. AI algorithms can process vast amounts of data from various sources (e.g., satellites, drones, sensors) in real time, providing actionable insights. Machine learning models can predict threats and recommend optimal courses of action.
- **Autonomous Weapons Systems:** AI enables the development of autonomous systems that can operate without human intervention. Autonomous drones and robotic systems can perform tasks such as surveillance and reconnaissance, reducing human risk and increasing operational efficiency.

---

42 Visner, Samuel Sanders. "Policy Issues in Artificial Intelligence Cyber Defense." In *Navigating the Future of Cybersecurity: AI and Its Impact.* Chapter 17, pp. 299-320. 2024.

- **Cyber Warfare and Defense:** AI is crucial in both offensive and defensive cyber operations. AI can detect and respond to cyber threats more quickly and effectively than traditional methods. In offensive operations, AI can be used to develop sophisticated malware and hacking tools to disrupt enemy communications and infrastructure.
- **Logistics and Supply Chain Management:** AI can optimize military logistics, ensuring that supplies and personnel are delivered where and when needed. Predictive analytics can forecast demand and streamline supply chain operations, reducing costs and improving efficiency.

Appendix C – Government and Industry Case Studies

Multiple case studies across government and industry illustrate the transformative role that AI is playing within the cybersecurity space, providing capabilities in detecting, analyzing and responding to complex threats more effectively than traditional methods.

AI-Powered Threat Detection at Darktrace[43]

In 2024, Darktrace, a leading cybersecurity company, successfully thwarted a sophisticated non-English phishing attack on a customer's network appearing to come from an international food chain. Darktrace's product focuses on behavioral analysis, and its self-learning AI understands what is considered normal for every user within an organization's email environment, bypassing any limitations that would come from relying on English language-trained models. When the phishing attempt was launched, the AI immediately understood that the sender never had any previous correspondence with the organization or its employees and therefore treated the emails with caution from the onset. Not only was Darktrace able to detect this new sender, but it also identified that the emails had been sent from a domain located in China and contained an attachment with a Chinese file name.

43 https://darktrace.com/blog/lost-in-translation-darktrace-blocks-non-english-phishing-campaign-concealing-hidden-payloads

These emails were sent from a legitimate domain associated with a trusted organization and seemed to be coming from the correct connection source. They were verified by sender policy framework (SPF) and were able to evade the customer's native email security measures. Darktrace's AI recognized that these emails were actually sent from a user located in Singapore, not China. The phishing emails contained a Word document that included a QR code. Normally these documents will pass through traditional security software, but Darktrace's AI was able to identify the presence of the QR code and scan its destination, revealing it to be a suspicious domain that had never previously been seen on the customer's network.

In this example, attackers attempted to use non-English language phishing emails originating from a trusted source and containing a multistage payload hidden behind a QR code. As traditional email security measures typically rely on pre-trained language models or the signature-based detection of blacklisted senders or known malicious endpoints, this multistage phishing attempt would likely bypass native protection. Darktrace's AI was able to autonomously scan attachments and detect QR codes within them, while also identifying the embedded links. This ensured that the customer's email environment was protected against this phishing threat, preventing potential financial and reputation damage.

AI-Enabled Spear Phishing Defense With NVIDIA Morpheus[44]

In 2023, NVIDIA's Morpheus framework was instrumental in defending organizations against sophisticated spear phishing attacks. Spear phishing, which targets specific individuals or organizations with personalized messages, poses a significant threat due to its high success rate and potential to bypass traditional security measures. NVIDIA Morpheus uses AI to implement digital fingerprinting workflows, creating unsupervised behavioral models for every user, suborganization and the entire enterprise. These models detect subtle deviations from normal behavior that indicate phishing attempts. By analyzing

44 https://developer.nvidia.com/blog/nvidia-morpheus-helps-defend-against-spear-phishing-with-generative-ai/

vast amounts of data and continuously learning from it, Morpheus can identify and block malicious emails with high accuracy. For example, Morpheus was able to detect a spear phishing campaign targeting a financial institution by analyzing patterns in email metadata, content and sender behavior. The AI flagged emails that deviated from normal communication patterns and were part of the phishing attempt, effectively preventing the attack from reaching its intended targets.

In addition, using the NVIDIA Morpheus LLM engine integration, NVIDIA built a pipeline to address common vulnerabilities and exposures (CVE) risk analysis using a technique known as retrieval-augmented generation (RAG)[45]. Security analysts can determine whether a software container includes vulnerable and exploitable components using LLMs and RAG. This method enables analysts to investigate individual CVEs four times faster, on average, and identify vulnerabilities with high accuracy so patches can be prioritized and addressed accordingly.

AI-Driven Network Security at Cisco — Proactive Threat Hunting[46]

In 2023, Cisco implemented AI-driven network security solutions that transformed their approach to threat hunting. Cisco's AI-based tool continuously monitors network traffic and user behavior to identify unusual patterns that could indicate a security threat. For example, the AI detected a sophisticated attack where the intruders attempted to move laterally across the network using legitimate credentials. By analyzing network flow data and identifying deviations from established baselines, the AI flagged the suspicious activity and automatically isolated the compromised segments of the network, preventing the attackers from reaching their target.

AI-Enhanced Endpoint Security at CrowdStrike Real-Time Malware Detection[47]

CrowdStrike uses AI to enhance endpoint security by providing real-time malware detection and response. In 2024, CrowdStrike's AI identified a new

45 https://blogs.nvidia.com/blog/what-is-retrieval-augmented-generation/
46 Cisco. (2023). *AI-Powered Network Security Solutions.* Retrieved from Cisco
47 CrowdStrike. (2024). *Next-Generation Endpoint Protection.* Retrieved from CrowdStrike

strain of ransomware that traditional signature-based detection systems missed. By employing machine learning algorithms to analyze the behavior of files and applications in real-time, CrowdStrike's AI detected the ransomware's attempts to encrypt files and immediately quarantined the affected systems. This proactive measure stopped the ransomware before it could propagate, protecting the organization's data and minimizing downtime.

AI-Enabled Fraud Detection at JPMorgan Chase — Financial Transaction Monitoring[48]

JPMorgan Chase employs AI to detect and prevent financial fraud. In 2023, the company's AI system analyzed millions of transactions in real time, identifying suspicious activities indicative of fraud. The AI flagged transactions that deviated from typical spending patterns, such as unusually large transfers or purchases from high-risk locations. By integrating AI with fraud detection workflows, JPMorgan Chase significantly reduced the incidence of false positives and detected actual fraudulent activities more efficiently, protecting both the bank and its customers.

AI-Based Identity and Access Management at IBM — Adaptive Authentication[49]

IBM uses AI to improve identity and access management through adaptive authentication techniques. In 2024, IBM implemented an AI-driven system that continuously evaluates risk based on user behavior, device health and network context. For instance, if an employee attempted to access sensitive data from an unfamiliar device or location, the AI system would prompt additional verification steps, such as multi-factor authentication or biometric verification. This approach ensured that access to critical resources was secure and that any anomalies were addressed promptly, enhancing overall security posture.

48 JPMorgan Chase. (2023). *AI in Financial Fraud Detection.* Retrieved from JPMorgan Chase
49 IBM. (2024). *Adaptive Authentication with AI.* Retrieved from IBM

AI in Supply Chain Security at Microsoft — Predictive Analytics for Risk Management[50]

Microsoft has integrated AI into its supply chain security to manage risks and ensure the integrity of its supply chain. In 2023, Microsoft's AI system used predictive analytics to assess potential risks from suppliers based on historical data, geopolitical factors and supplier behavior. The AI identified potential disruptions and security threats, allowing Microsoft to proactively address vulnerabilities and maintain a resilient supply chain. This capability was crucial in mitigating risks associated with third-party components and services, ensuring continuity and security in their operations.

AI-Powered Insider Threat Detection at IBM — Behavioral Analytics[51]

IBM implemented an AI-powered insider threat detection system that uses behavioral analytics to identify potential security threats from within the organization. In 2023, the AI system flagged an employee who was accessing sensitive data outside of their typical work patterns. The AI detected deviations in the employee's behavior, such as accessing files they had never accessed before and working irregular hours. Upon investigation, it was discovered that the employees' credentials had been compromised. The AI system's timely detection and alerting prevented a potential data breach and safeguarded the organization's sensitive information.

AI-Driven Cybersecurity at the U.S. Department of Homeland Security (DHS)

DHS uses AI to enhance its cybersecurity infrastructure, protecting critical civilian networks and public services[52,53,54]. The AI systems deployed by DHS analyze vast amounts of data in real time to detect and respond to cyber threats, ensuring the security of essential government functions.

---

50 Microsoft. (2023). *Applying next-generation AI to the Microsoft Supply Chain Platform.* Retrieved from Microsoft

51 IBM. (2023). *Behavioral Analytics for Insider Threat Detection.* Retrieved from IBM

52 U.S. Department of Homeland Security. (2022). *Artificial Intelligence Strategy.* Retrieved from DHS.gov

53 U.S. Department of Homeland Security. (2023). *Using AI and Machine Learning to Enhance Cybersecurity.* Retrieved from DHS.gov

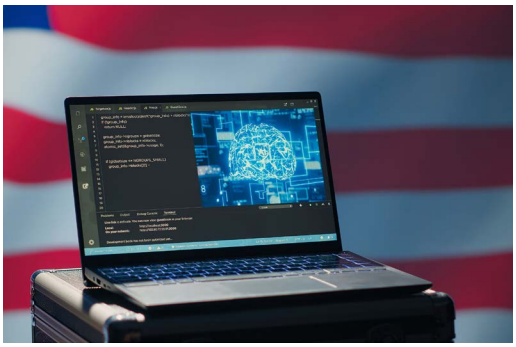
54 Cybersecurity and Infrastructure Security Agency. (2023). *AI-Powered Threat Detection and Response Systems*. Retrieved from CISA.gov

AI-Powered Fraud Detection in Civilian Government Agencies

AI is also being used to detect and prevent fraud in civilian government agencies. By analyzing transaction data and identifying suspicious patterns, AI systems help ensure the integrity of public funds and protect against financial cybercrime[55,56,57].

AI for Public Service Cybersecurity in the United Kingdom

The U.K. government has implemented AI-driven cybersecurity measures to protect its public services from cyber threats. This case study highlights the U.K.'s approach to integrating AI in civilian government cybersecurity, emphasizing collaboration between government agencies, private sector partners and academic institutions[58,59,60].



These additional use cases highlight the diverse applications of AI in enhancing cybersecurity across various domains, from network security and endpoint protection to fraud detection and supply chain security. Each example underscores AI's potential to detect and respond to sophisticated threats in real time, significantly improving organizational resilience and security.

55 U.S. Government Accountability Office. (2022). *Using AI to Detect and Prevent Fraud in Government Programs.* Retrieved from GAO.gov.
56 U.S. Department of the Treasury. (2023). *Leveraging AI to Combat Fraud in Civilian Agencies.* Retrieved from Treasury.gov
57 International Public Sector Fraud Forum. (2023). *Artificial Intelligence in Public Sector Fraud Detection and Prevention.* Retrieved from PublicSectorFraud.org.
58 UK Government. (2021). *AI Sector Deal: Government and Industry Partnership to Enhance Cybersecurity.* Retrieved from Gov.uk
59 National Cyber Security Centre. (2022). *AI in Cybersecurity: Enhancing Public Service Protection*. Retrieved from NCSC.gov.uk
60 UK Government. (2023). *Public-Private Partnerships for AI-Driven Cybersecurity.* Retrieved from Gov.uk

Appendix D — Unlocking AI's Potential in Defense, Military and Commercial Sectors

AI is revolutionizing a wide array of applications across defense, military and commercial sectors, driving innovation and enhancing operational capabilities[61]. From autonomous systems and drones to advanced cybersecurity measures and intelligence analysis, AI's integration is reshaping the landscape. Below, we delve into key areas where AI is making a significant impact.

Autonomous Systems and Drones

AI is transforming the use of autonomous systems and drones in defense and military operations. These systems perform a wide range of tasks, from surveillance and reconnaissance to combat missions and logistics support. AI enables drones and autonomous vehicles to operate with a high degree of autonomy, allowing them to navigate complex environments, identify and track targets, and make real-time decisions based on data analysis. This reduces the risk to human personnel and increases the efficiency and effectiveness of military operations. For example, AI-powered drones can conduct intelligence, surveillance and reconnaissance (ISR) missions, providing real-time situational awareness and actionable intelligence to military commanders.

Cybersecurity and Threat Detection

AI plays a crucial role in enhancing cybersecurity and threat detection capabilities in the defense sector. With the increasing sophistication of cyber threats, AI systems are essential for identifying and responding to attacks in real time. AI algorithms can analyze vast amounts of data to detect anomalies and patterns indicative of cyber exploits, such as malware or unauthorized access. These systems can automate responses to mitigate threats, reducing the time it takes to address vulnerabilities and preventing potential damage. Additionally, AI can

61 Adewusi, A., & Daraojimba, D. O. (2024). *Artificial Intelligence in Cybersecurity: Protecting National Infrastructure.* Retrieved from ResearchGate

be used to predict future attacks by analyzing trends and behaviors, enabling proactive defense measures. This capability is vital for protecting sensitive military information and infrastructure from adversaries who are constantly evolving their tactics.

Intelligence, Surveillance and Reconnaissance

AI significantly enhances ISR capabilities within defense and military operations. AI technologies are used to process and analyze vast amounts of data collected from various sensors, satellites and reconnaissance missions. Machine learning algorithms can sift through this data to identify patterns, detect anomalies and extract actionable intelligence. AI-driven ISR systems enable real-time monitoring and analysis, providing military personnel with timely and accurate information to make informed decisions. These systems can also predict potential threats and movements of adversaries, allowing for proactive and strategic planning. The use of AI in ISR not only improves situational awareness but also reduces the cognitive load on human analysts, enabling them to focus on higher-level decision-making tasks.

Zero-Trust Architectures for Enhanced Cybersecurity

In today's highly interconnected digital environment, traditional perimeter-based security models are increasingly inadequate. The zero-trust architecture (ZTA) model addresses these shortcomings by assuming that threats can exist both inside and outside the network. The principle of "never trust, always verify" is central to zero trust, ensuring that every access request is thoroughly authenticated, authorized and encrypted. The integration of AI within ZTA enhances its effectiveness by enabling dynamic, real-time decision-making and threat detection.

The 2022 DoD Zero Trust Strategy marks a significant shift in cybersecurity approach by emphasizing the principle of "never trust, always verify" to enhance the protection of critical defense systems and data[62]. This strategy aims to modernize the DoD's security posture by implementing a zero-trust architecture

that prioritizes continuous monitoring, strict access controls and dynamic threat response mechanisms. By adopting a zero-trust framework, the DoD seeks to mitigate cyber threats, prevent unauthorized access and bolster resilience against evolving cyber risks. The strategy also underscores the importance of integrating advanced technologies such as AI, automation and behavioral analytics to strengthen cybersecurity defenses and enable real-time threat detection and response capabilities. Through the implementation of the zero-trust model, the DoD aims to enhance its cybersecurity posture, safeguard sensitive information and ensure the resilience of defense networks and systems in the face of evolving cyber challenges.

Implementing AI in Zero-Trust Architectures

Integrating AI into zero-trust architectures significantly enhances the security posture of organizations by providing dynamic, real-time threat detection and response capabilities[63,64,65,66,67,68] Key enhancements include:

- **User and Device Authentication:** AI algorithms continuously analyze user behavior and device characteristics to establish a baseline of normal activity. Multi-factor authentication (MFA) is dynamically adjusted based on the risk profile generated by AI. For instance, an employee accessing from a usual location with a known device might face standard MFA, while access from an unfamiliar location or device triggers additional verification steps.
- **Continuous Monitoring and Anomaly Detection:** AI-powered tools analyze network traffic patterns and user behavior in real time. Machine learning models detect anomalies such as unusual data access patterns, sudden spikes in data transfers or atypical login times, triggering alerts and automated responses like session termination or access revocation.
- **Dynamic Access Control:** AI systems dynamically adjust access controls based on contextual information such as user role, behavior analytics and the sensitivity

62 Department of Defense. (2022). *Department of Defense Zero Trust Strategy.* Retrieved from https://www.defense.gov
63 Darktrace. (2024). *Case Study: Thwarting a Non-English Phishing Attack.* Retrieved from Darktrace
64 NVIDIA. (2023). *Morpheus: AI Framework for Cybersecurity.* Retrieved from NVIDIA
65 Cisco. (2023). *AI-Powered Network Security Solutions.* Retrieved from Cisco
66 CrowdStrike. (2024). *Next-Generation Endpoint Protection.* Retrieved from CrowdStrike
67 JPMorgan Chase. (2023). *AI in Financial Fraud Detection.* Retrieved from JPMorgan Chase
68 IBM. (2024). *Adaptive Authentication with AI.* Retrieved from IBM

of the data being accessed. If an AI system detects high-risk behavior, it can automatically enforce stricter access controls or require additional authentication before granting access.

- **Threat Intelligence and Response:** AI integrates with threat intelligence platforms to analyze and correlate threat data from various sources. It identifies potential advanced persistent threats and predicts their attack vectors. AI-driven systems can automate the deployment of countermeasures, such as isolating affected network segments, blocking malicious IP addresses and updating security policies in real time.
- **Data Protection and Encryption:** AI algorithms manage encryption keys and enforce encryption policies based on data sensitivity and access patterns. The AI system can dynamically apply or revoke encryption keys and adjust encryption levels to ensure data remains secure even if compromised.

Appendix E — AI Applications To Minimize Cybersecurity Risks and Maximize Adoption and Use[69]

SEI's recent publications cover a broad range of topics, including LLMs for cybersecurity, generative AI in software engineering, zero trust, national security applications of LLMs, capability-based planning, supply chain risk management, software assurance and the cybersecurity of quantum computing[70]. Each publication explores critical advancements, challenges and opportunities in these areas, highlighting ongoing efforts to address emerging issues and improve practices. A synopsis of the aggregate findings includes:

- **Large Language Models:** While LLMs offer significant potential for cybersecurity tasks, they require rigorous evaluation to avoid risks such as spurious results and misinterpretation. The publication emphasizes designing tasks that reflect real-world cybersecurity phenomena.
- **Generative AI in Software Engineering:** The rapid adoption of generative AI brings concerns about security risks, unforeseen failures and trust issues. Ensuring that generative AI tools are integrated effectively into workflows and overseen by expert judgment is crucial. By identifying suitable use cases and leveraging generative AI's

69 Adewusi, A., & Daraojimba, D. O. (2024). *Artificial Intelligence in Cybersecurity: Protecting National Infrastructure.* Retrieved from ResearchGate

70 Software Engineering Institute (SEI). (2024). *AI and Cybersecurity Publications.* Retrieved from SEI

capabilities, organizations can improve software acquisition, analysis, verification and automation, leading to increased productivity and quality.

- **Supply Chain Risk Management:** Despite reduced Log4j-related exploits, supply chain risks remain significant. Effective governance and integration of cyber risks into broader risk portfolios are essential for operational resilience.
- **LLMs for Cybersecurity:** Properly scoped and well-designed assessments can harness LLMs' potential to enhance cybersecurity measures, adapting them to dynamic threat landscapes.
- **National Security Applications of LLMs:** Customizing LLMs for specific intelligence use cases and evaluating their trustworthiness can enhance national security efforts, providing reliable tools for the intelligence community.
- **Evaluating LLMs for Cybersecurity:** Develop comprehensive evaluation criteria that go beyond factual recall, focusing on practical, real-world applications to accurately assess LLM performance.
- **Integrating Generative AI:** Redesign task flows to incorporate generative AI tools effectively, ensuring they are used responsibly and enhance software engineering processes.
- **Strengthening Supply Chain Risk Management:** Implement robust metrics and standards for assessing cybersecurity in open-source software, ensuring thorough data collection and analysis to validate these metrics.
- **Advancing Quantum Computing Security:** Focus research on creating a cyber protection discipline for quantum computing, addressing the unique challenges posed by this emerging technology.

These insights provide a roadmap for organizations to navigate the complexities of AI adoption, mitigating risks while maximizing opportunities for innovation and improvement in cybersecurity and software engineering.

AFCEA's Committees produce topical white papers that highlight critical issues and propose solutions. To see submissions and review the extensive collection of relevant materials, please visit AFCEA's Resource Library.

The AFCEA International Cyber Committee White Paper Series

afcea.org/about-afcea/committees/cyber-committee

AFCEA