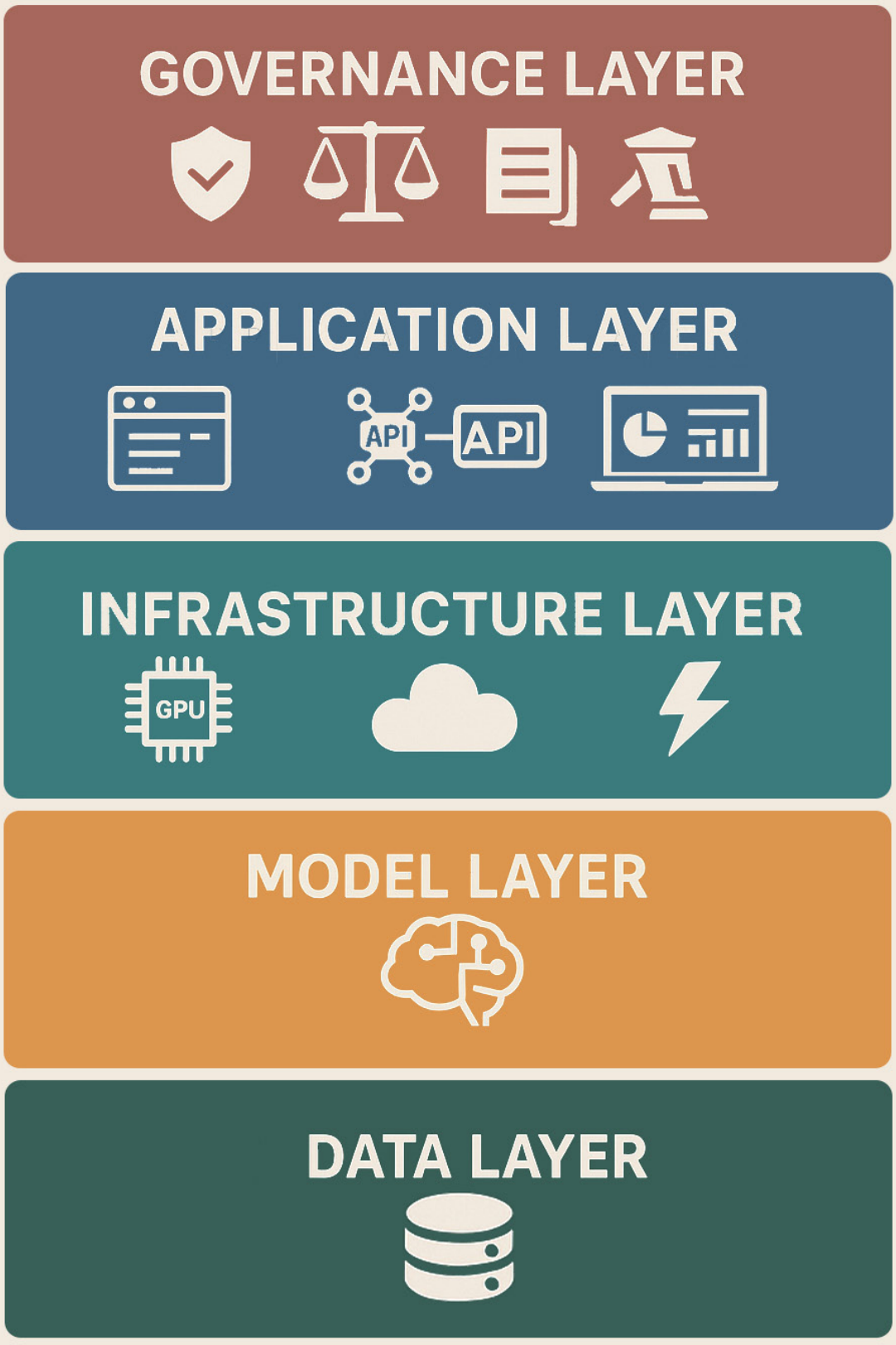
THE AI TECH STACK:

A Primer for Tech and Cyber Policy



ABOUT THIS REPORT

This report is intended as a primer for public policy and cybersecurity practitioners to better understand the dynamic, diffuse, and emerging landscape of Artificial Intelligence (AI) in which both audiences intersect—and must act. The audience should take away an understanding of the different elements of the AI technology stack and be positioned to approach security solutions across and within each layer of the AI tech stack deliberately.

PALADIN
GLOBAL INSTITUTE

ABOUT THE PALADIN GLOBAL INSTITUTE

The Paladin Global Institute's mission is to protect global critical infrastructure from cyber, AI, and deep tech threats and enhance the safety of people online by investing in research and advocacy, making informed policy recommendations, and bringing together the public and private sectors to share knowledge and create and invest in innovative technologies.

ABOUT THE AUTHORS

Kemba Walden is the President of the Paladin Global Institute and former Acting United States National Cyber Director.

Devin Lynch is the Senior Director of the Paladin Global Institute and a former Director for Cyber Policy & Strategy Implementation at the Office of the National Cyber Director (ONCD).

ACKNOWLEDGEMENTS

Many thanks to our reviewers including Roberta Campbell, Eric Wengrowski, Ben Colman, Fred Heiding, Chris Inglis, Ciaran Martin, David Hoffman, Merritt Cahoon, and Trey Herr.

COVER PHOTO

This image was created using OpenAI's DALL-E from a prompt based on text from the following report.

Executive Summary

As AI systems[1] increasingly form the backbone of critical infrastructure, economic activity, and national security, policymakers and cybersecurity practitioners must develop deep technical literacy to craft practical guidelines and defensive strategies. Those practitioners who successfully integrate security throughout the AI tech stack will lead the digital economy, establish the norms, standards, and best practices that define responsible AI development worldwide, and strengthen national security.

This report serves as a comprehensive primer on the AI technology stack,[2] offering public policy and cybersecurity practitioners insights into this dynamic landscape where their domains increasingly intersect.

The AI technology stack comprises five distinct yet interdependent layers:

1. **GOVERNANCE LAYER:** The framework that effectively wraps around the whole AI Technology Stack—a layer that aims to ensure responsible deployment through security protocols, legal constraints, ethical principles, and policies.
2. **APPLICATION LAYER:** The user interface that transforms complex AI capabilities into accessible tools through browsers, APIs, dashboards, and other user interfaces.
3. **INFRASTRUCTURE LAYER:** The essential computational foundation that powers AI systems, enabling the intensive demands of training and inference through specialized hardware, cloud platforms, and energy resources.
4. **MODEL LAYER:** The core computational component that processes data according to sophisticated algorithms to recognize patterns and generate predictions or decisions. This includes the machine learning approaches that enable systems to learn without explicit programming.
5. **DATA LAYER:** The foundation of AI systems, providing the raw material that fuels models. The quality, diversity, and quantity of this data largely determine the intelligence and capabilities of the final model.

Robust security across this stack is a technical necessity and a strategic imperative. AI security extends traditional cybersecurity concepts to confront unique vulnerabilities within machine learning systems, including adversarial attacks, model poisoning, and data exploitation. Organizations that prioritize comprehensive AI security not only mitigate risks but also position themselves as leaders in tomorrow's innovation networks, capable of rapidly integrating advancements while sustaining trust. By embedding security measures early in the development process, organizations gain downstream competitive advantages, including faster deployment cycles, greater stakeholder confidence, and better products.

The first step to this process is understanding the AI Tech Stack. This primer develops a framework for understanding how Artificial Intelligence systems work, similar to how cybersecurity professionals understand the Open Systems Interconnection (OSI) model or Transmission Control Protocol/Internet Protocol (TCP/IP) protocols, as the foundation for discovering and implementing layered security.

Introduction

AI represents a technological transformation comparable to the introduction electricity, the automobile, and the advent of the Internet, reshaping how we work, learn, and interact across society. The criticality of unleashing its potential and setting its course on a responsible and secure trajectory is paramount.

Today, 25 years into the 21st century and 50 years into the information age, AI stands at an inflection point similar to the production of the lightbulb and automobile at the beginning of the 20th century. Just as the mass-produced automobile democratized personal transportation, emerging AI systems democratized access to information and cognitive capabilities once reserved for specialists. And in the same manner that the Model T's impact extended far beyond transportation, AI's influence will likely ripple through every sector of society. Where the lightbulb and automobile reshaped cities, labor markets, manufacturing, social patterns, and national infrastructure, similarly, AI will transform not just technology but our entire socioeconomic landscape, including health care,[3] business,[4] and education.[5]

The economic transformation to AI will be as profound as the shift from animal power to combustion engines, and from oil lamps to electric light. No less so than when the world transitioned from conducting business via the interstate highway system to the World Wide Web. The Internet enabled the rapid transfer of information such as sound, video, and graphics and swiftly broke down barriers, catalyzed commerce, and reshaped society.

Already, AI is transforming how the world conducts business. As the world transitioned online, the civilian safety protocols that enabled commerce via the interstate highway system did not similarly transition to the information superhighway. We can do better. Now, at the dawn of the AI era, is the time to secure the AI tech stack to unleash the full potential and benefits of today's economic transformation.

Industries will soon reorganize around AI capabilities—just as they did with the Internet—creating entirely new job categories while retiring others.[6] Geographic constraints on, and definitions of, knowledge work will further dissolve, with AI tools and agents augmenting and enhancing online work. Security paradigms will evolve, with nations racing for AI advantage in the defense technology and national security sectors, as they once competed for automotive manufacturing prowess to fuel military production.

AI will transform our daily lives and social interactions, much like electricity, automobiles and the Internet did before. Initially, this change will happen gradually (as we're seeing now), but it will accelerate as applications mature, and society adapts.[7] Over time, our learning methods, creative processes, communication styles, and decision-making approaches will all evolve to incorporate these new cognitive tools. Like previous technological revolutions, AI will require supporting infrastructure and systems across personal, business, and national security domains.

We stand at a moment of both tremendous opportunity and uncertainty. At this inflection point, we must understand the AI tech stack, consider ways to secure its foundations at the onset, and begin to craft thoughtful governance for AI development while unleashing its benefits and promoting its potential.

The AI Tech Stack

The goal of AI is to make machines smarter. This is done, in part, through machine learning (ML). Whereas AI is the overarching concept of creating machines that can perform tasks requiring human intelligence, ML is a specific subset of AI that focuses on enabling machines to learn from data without explicit programming.[8]

The development, security, and deployment of AI capabilities require a deliberate approach to organizing the complex interplay of technologies that enable modern AI systems. Understanding the resulting structure and the interplay of its various sub-components is essential for effective policy development and comprehensive security analysis.

The fundamental components enabling AI capabilities, including ML, were clearly conceptualized for policymakers in 2020 in 13 words: "Machine learning systems use computing power to execute algorithms that learn from data."[9] Three essential elements - algorithms, compute, and data - form the AI Triad. The algorithms are a collection of mathematical techniques, statistical methods, and computational approaches that provide parameters for machines to perform tasks requiring intelligence. The computational resources that execute algorithms at scale, including specialized hardware like Graphics Processing Units, Tensor Processing Units, and AI accelerators, refer to the computing power that has made training increasingly sophisticated models possible. Last is the raw information, or data, that algorithms process to develop knowledge representations, identify patterns, and generate outputs. The scale, quality, and nature of available data fundamentally constrain what AI systems can accomplish.

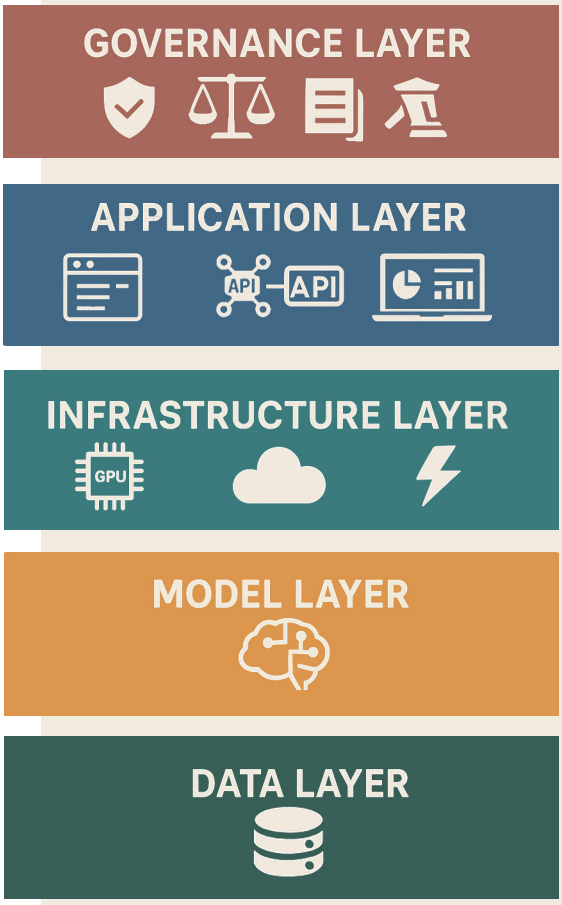
The AI Triad proved valuable for understanding AI's core technical elements, especially as the technology grew in popularity and emerged on the public's radar. However, as AI and ML evolve from research projects to deployed applications integrated into critical business functions and infrastructure, this model has become insufficient for practical or policy purposes.

The AI Triad does not fully represent how AI is built, deployed, and governed today. Applications of AI, such as robotics, natural language processing, deep learning, generative AI, virtual assistants, and speech recognition, made possible by the vast availability of data, exponential growth in computing capabilities, and other advancements have transformed the field of AI. Production environments, transformers, and applications of AI further reveal additional complexities in security, operations, and governance for which we must now account.

THE AI TECH STACK

The AI 'tech stack' refers to the layered collection of technologies used to build and deploy AI systems. Everything from the hardware and infrastructure to the data, models, and applications; it is "the collection of tools, AI frameworks, and platforms that you use to develop AI applications,"[10] serving as the foundation upon which AI systems are built.

As AI systems have matured, open-source models have democratized the use of AI, and the spread of AI has diffused globally, a more comprehensive architectural model takes shape. The AI ecosystem has cohered into five distinct and interdependent layers, each serving an individual function in developing and applying AI systems. They are the:



The governance layer comprises the rules of the road and the operating environment in which AI is developed and deployed, including protocols that aim to ensure that the AI system operates within the defined values of the organization and meets defined security and safety goals.

The application layer serves as the user interface — the dashboard, chatbot, search feature, or voice of the AI system delivers desired functionality as humans interact with, interrogate, and leverage its capabilities.

The infrastructure — data centers, GPUs, networking, energy systems, and backend services — provides the engine that powers the model to the user.

The AI model— the algorithms and architectures trained on vast datasets to learn patterns and generate outputs – functions like the central nervous system, and is the core computational component.

At the base of any AI system lies data — the raw material that fuels the model.

The AI Triad remains intact with the algorithm, compute, and data within the model, infrastructure, and data layers. On top of that, the Application Layer becomes where the user interfaces with the AI; it brings the AI to life, animating it through chatbots, voice assistants, and agents, and provides another dimension to the technology through the user interface (UI). The Governance Layer emerges as a necessary addition, spanning all components and providing the critical framework and risk management required in increasingly consequential AI deployments.

The interdependencies up and down the stack are many and shape AI systems dynamically and non-linearly. For example, the infrastructure layer is essential for energizing the stack, hosting and storing the data, training an AI model, and its compute power is similarly requisite when the AI system receives input via the application layer. Both things can be true, and securing each layer for all foreseeable instances is what lies ahead. Capturing every fluctuation and movement within AI systems (including those not yet invented) will be a dynamic pursuit for policymakers and security practitioners. These five layers create a cohesive framework that accounts for AI system development and deployment, supports innovation, and prioritizes accountability and societal benefit.

Defending AI Systems Matters

For AI to thrive across industries, digital trust, defensibility, and resilience are table stakes. Without robust security measures, AI systems risk operating outside of acceptable organizational norms because of poor or complacent design, or, worse, becoming conduits for cyber threats, powerful weapons for threat actors—and potentially rogue actors themselves—undermining the utility, adoption, and promise of this incredible capability.

Robust security and safety integration across the entire AI development process is essential. AI security significantly extends traditional cybersecurity concepts, resolving the unique vulnerabilities inherent to machine learning systems. While conventional security practices focus on protecting data and infrastructure, AI security must additionally safeguard training datasets, model architectures, and detection processes, among other concerns.

TABLE: SECURITY RISKS IN THE AI TECH STACK BY LAYER

LAYER	KEY SECURITY RISKS	EXAMPLE VULNERABILITIES	POTENTIAL IMPACT
Governance	Superintelligence, rogue agents, AI sentience, compliance failures	AI agent building harmful weapons, acts without a 'human in the loop'	Diminish national security, degrade critical infrastructure
Application	Prompt injection, API exploitation	Unsafe content generation, data leakage	Reputational damage, harmful content, data exposure, surveillance
Infrastructure	Physical attack, unauthorized access, resource hijacking, supply chain disruptions	Compromised access controls leading to zero trust violations	Financial damage, training data theft, regulatory penalties
Model	Adversarial attacks, model theft, model inversion, model misclassification	Inputs designed to trick the system into making incorrect decisions. Hallucinated outputs	IP theft, manipulated model outputs, security bypass, malicious code injection
Data	Data poisoning, privacy violations	Training data manipulation, PII exposure, deepfakes	Data spillage, bias, privacy violations, content violations

Securing AI Systems

Securing the AI tech stack requires a systemic approach. Isolated technical safeguards will not suffice. Risks within one layer can cascade through the system—a poisoned training dataset can corrupt a model, leading to unpredictable behavior in deployed applications and, ultimately, governance failures with public consequences. Similarly, weak infrastructure controls can expose models to unauthorized training or theft, undermining intellectual property protections and national security. This interdependence demands cross-layer governance, where threat models, security protocols, and oversight mechanisms mitigate vulnerabilities holistically. Policymakers and security leaders must abandon siloed approaches and adopt a system-level view of AI risk to ensure resilience and trust.

The evolution of security practices must also accelerate in response to emerging AI-specific threats and pacing threats from nation-state actors.[11] At the same time, the prioritization of securing each layer is of no less importance. Here, AI Security is distinct from Responsible AI. The core focus of AI security is to defend AI systems against cyber threats and espionage in all reasonably foreseeable instances. In contrast, the core focus for Responsible AI seeks to ensure fairness, transparency, and accountability. While both are important to ensuring business viability, this construct of the AI tech stack is best suited for enabling a defense-in-depth strategy to security.[12]

The data and model layers are of chief importance to getting AI security right. As AI systems collect, process, store, and produce massive amounts of publicly available and sensitive data, securing the Data Layer becomes a top priority. So fundamental to AI systems are data that a data poisoning attack could fundamentally compromise AI system integrity at its source and create cascading adverse effects across each layer of the tech stack. Securing the Data Layer through encryption, access controls, and data masking is critical for preventing data breaches, securing intellectual property, maintaining user trust, and ensuring compliance with regulations.

Next for prioritization is the Model layer. The models at the core of modern AI systems require high volumes of sensitive enterprise data, leverage an open-source ecosystem, proliferate globally, and employ self-learning that is difficult to foresee. This makes models high-value targets for attackers seeking to manipulate outputs, nation-states seeking advantages and access to frontier models, or criminals seeking to steal valuable data and model intellectual property from innovators. Establishing secure AI environments through appropriate access controls and firewalls, with API and endpoint security, will provide baseline protections for the model layer.

To be sure, securing the Infrastructure and Applications layers is essential. Many organizations already benefit from robust infrastructure cybersecurity practices offered by cloud service providers, large cyber hyperscalers, and critical infrastructure owners and operators that can extend to AI systems.

Adhering to standards like the National Institute of Standards and Technology's (NIST) NIST SP 800-53,[13] SOC2,[14] and ISO/IEC 27001[15] reinforces many of these software security advantages. Supply chain risk management and energy security considerations merit equal measure for the outsourced hardware that comprises cloud services. Without cutting-edge semiconductor chips or power, the whole AI stack will flummox.

Infrastructure-based protections and controls provide some cybersecurity at the Application layer. To prevent prompt injection attacks and malicious inputs to proprietary AI systems, data sanitization and continuous monitoring offer needed protections. Such efforts benefit further from API (Application Programming Interface) and AI gateways, role-based access controls, and encryption protocols via the web interface's Transport Layer Security (TLS). The NIST's AI Risk Management Framework,[16] ISO/IEC 42001,[17] and the OWASP Top Ten[18] stand out among guidance to identify and promote secure, responsible, and sustainable AI applications.

The Governance layer is the least mature yet essential for AI trust. It demands something different: moving beyond rigid regulation and toward dynamic protocol development.

As was done for the Internet with the foundational infrastructure of the TLS, Hypertext Transfer Protocol Secure (HTTPS), Domain Name System Security Extensions (DNSSEC), and Border Gateway Protocol (BGP), industry-crafted interoperable standards should lead. Protocols that safeguard AI security and reliability while accommodating the evolving landscape of AI systems would build trust in AI technologies and provide a flexible, adaptive framework that evolves with technology. Interoperable standards that remain relevant as AI technology advances would promote international adoption, prevent regulatory obsolescence, and maintain essential security protections across the AI ecosystem.[19]

AI-specific vulnerabilities introduce unique challenges that ask for proactive AI-enhanced solutions. These threats escalate in scale and complexity and adapt rapidly to defensive measures, outpacing traditional security frameworks. Neglecting AI security leaves organizations vulnerable to increasingly sophisticated adversaries. By embedding security into AI systems across the tech stack, organizations can mitigate these risks, protect sensitive data and intellectual property, and preserve their bottom line.

The Imperative for Policymakers and Practitioners

Understanding the AI tech stack is no longer optional for policymakers and cybersecurity professionals—it's a strategic necessity. As AI becomes central to critical infrastructure, economic systems, and national security, leaders must develop technical literacy to craft effective regulations and defense strategies. Without this foundation, policies risk being either excessively restrictive or alarmingly ineffective.

The global AI landscape is rapidly transforming, with a high-stakes competition emerging between the United States and China that reshapes economic markets and security paradigms. AI-powered network platforms are consolidating global influence and raising urgent questions about digital sovereignty as nations increasingly depend on foreign-designed systems. While America leads in research and talent, China's swift progress narrows this advantage, Europe leverages regulatory expertise despite lacking homegrown platforms, India's untapped potential could further redefine the balance, and deep investments from Gulf States expand the AI ecosystem.

In the evolving landscape of global power dynamics, a new paradigm is quickly taking shape. AI is a means and the goal of national and international advancement. As nations position themselves in this technological race, the question becomes not whether AI will transform global affairs, but how countries will navigate the complex pathways to achieve AI supremacy, and what this means for the international order.

To sustain its leadership, the United States must prioritize investments in innovation, attain semiconductor independence and energy security, and develop a comprehensive AI strategy that unleashes economic competitiveness and confronts AI's distinct security and safety concerns. None of these initiatives can succeed in the absence of another.

AI brings both advantages and challenges to the security landscape. AI and cybersecurity converge to create unprecedented challenges and opportunities. Policymakers who understand the technical intricacies of AI can develop frameworks that strike the right balance, safeguarding innovation while implementing essential guardrails. Similarly, cybersecurity practitioners versed in the AI tech stack can enhance defenses to counter emerging threats while leveraging AI's transformative potential to strengthen security measures.

Collaborative efforts between stakeholders are vital for defending and building a secure and competitive AI ecosystem on the global stage. Nations and organizations that embed security throughout the AI tech stack today will shape tomorrow's digital economy, lead global adoption of AI systems, and set the benchmarks for responsible development.

Driving Innovation and Enabling Trust

AI is a strategic driver of innovation. As AI systems become increasingly interconnected, security standards will emerge as the common language enabling safe and seamless interoperability. Standards and frameworks lead the developer and the user to risk-aware, actionable, and adaptable guidance for AI security. The NIST and ISO/IEC frameworks lead efforts to promote how to develop and deploy responsible and sustainable AI systems. These standards can ensure that outputs from one system can reliably serve as inputs to another, fostering ecosystems of learning and collaboration while maintaining strong protections.

Organizations that establish leadership in AI security today position themselves as the cornerstones of tomorrow's innovation networks, able to rapidly integrate advancements across the ecosystem while sustaining trust.[20] Secure-by-design principles amplify this advantage. [21] By embedding security measures upstream, early in the development process, organizations gain downstream competitive advantages, such as faster deployment cycles and greater stakeholder confidence. These principles, in AI system design and capital investments, lay the groundwork for scalable AI innovation that is both resilient to evolving threats and adaptable to emerging markets.

As AI applications expand across borders, anticipating and complying with international standards prevents legal pitfalls and facilitates collaboration and market growth. Similarly, AI safety considerations—rooted in democratic values, international norms, and security considerations—equip organizations to navigate emerging challenges while preserving public trust in global markets.

Trusted security frameworks fuel ecosystem-wide collaboration. Organizations adopting standardized and transparent security practices create environments conducive to sharing insights, models, and data with partners, customers, and competitors under appropriate safeguards. This collaborative model mirrors the networks of transportation systems enabled by standardized safety protocols—AI security, similarly, unlocks transformative potential across industries.

Finally, as AI systems grow increasingly interconnected, security standards will define the future of interoperability. These frameworks will serve as the universal language enabling safe integration of systems and innovations across the digital ecosystem. The organizations and nations leading in AI security today are not just defending their present; they are carving out leadership positions. By investing in security and safety now, they position themselves to leverage advancements, accelerate adoption, and drive progress on a global scale.

The Road Ahead

The future belongs to organizations that build AI systems that not only deliver unmatched capabilities but also inspire trust and increase resilience across all sectors of society. Those who build AI systems that are powerful, innovative, secure, resilient, and aligned with our values will thrive.

The five-layer AI technology stack—Data, Model, Infrastructure, Application, and Governance—provides a structured framework through which policymakers, security professionals, and organizations can systematically approach security and safety vulnerabilities while igniting innovation. Successfully integrating security throughout this stack will define the future of AI development. They will establish the technical standards, governance frameworks, and ethical guidelines that balance innovation with necessary protections. This balanced approach recognizes that effective security is not about restriction—it's about creating the trusted foundation that allows AI systems to reach their full potential.

Society eventually developed comprehensive frameworks for automotive and online safety and security only after recognizing the risks of putting powerful motor vehicles and unconstrained access in untrained hands. Many of those efforts were bolted on years later. Today, we face a similar situation with AI. The rapid advancement of AI capabilities necessitates a parallel evolution in the security of AI systems, governance protocols establishing roles, responsibility, and accountability across the AI ecosystem, and active defense measures to protect AI systems from human error and malicious actors.

AI capabilities will continue to advance, and the security landscape will grow increasingly complex. Organizations must develop sophisticated, multi-layered security strategies that resolve the unique vulnerabilities at each level of the AI stack. This also requires moving beyond traditional cybersecurity approaches to implement AI-specific protections against threats like adversarial attacks, model poisoning, and prompt injection.

This future with AI security necessitates collaboration across the AI ecosystem. Policymakers, security practitioners, innovators, investors, and business leaders must work together—and use the same words—to develop frameworks that both protect against misuse and unleash beneficial applications. By embedding security and safety considerations throughout the AI development lifecycle, we can create AIs that are powerful, trustworthy, and aligned with our values.

By learning from history and applying these lessons to AI systems, we can navigate this technological revolution responsibly, ensuring that AI serves humanity's best interests while managing its inherent risks.

Footnotes

[1] "Artificial Intelligence Systems," has meaning set forth in 15 USC 9401, and "means any data system, software, hardware, application, tool, or utility that operates in whole or in part using AI." https://uscode.house.gov/view.xhtml?req=(title:15%20section:9401%20edition:prelim)#:~:text=(b)%20The%20term%20%22artificial,influencing%20real%20or%20virtual%20environments.

[2] The framework submitted by the author follows a literature review of multiple tech stack constructions, but narrows its audience on the policymaker and practitioner, to foster thoughtful policy and security conversations. These constructions included: Moon Technologies, https://www.moontechnolabs.com/blog/ai-tech-stack/; Medium, https://medium.com/@lenaztyson/navigating-the-ai-tech-stack-an-in-depth-guide-2f722ac88703; Markovate, https://markovate.com/blog/ai-tech-stack/; 30 Coherent Solutions, https://www.coherentsolutions.com/insights/overview-of-ai-tech-stack-components-ai-frameworks-mlops-and-ides; Intel, https://www.intel.com/content/www/us/en/learn/ai-tech-stack.html?cid=sem&source=sa360&campid=2025_ao_cbu_us_gmocoma_gmocrbu_awa_text-link_generic_exact_cd_HQ-COMM-EnterpriseAI-Learn-EntAI-OBS_FC25023_google_b2b_is_non-pbm_intel&ad_group=AI-Stack-Learn_Exact&intel_term=ai+tech+stack&-sa360id=437000814696694 21&gad_source=1&gclid=Cj0KCQiAz6q-BhCfARIsAOezPxnA_nGexei_YUz-5vMneiX-GAoihC4ovgE38HYMwuKGoyn3bqReoy4caAtABEALw_wcB&gclsrc=aw.ds; IBM, https://www.ibm.com/think/topics/ai-stack#:~:text=latest%20podcast%20episodes-,The%20data%20layer,of%20this%20data%20management%20layer.; MongoDB, https://www.mongodb.com/resources/basics/artificial-intelligence/ai-stack; SmartDev, https://smartdev.com/ai-tech-stacks-the-blueprint-for-2025/; SoluLab, https://www.solulab.com/a-complete-guide-to-ai-tech-stack/; AWS, https://aws.amazon.com/blogs/machine-learning/welcome-to-a-new-era-of-building-in-the-cloud-with-generative-ai-on-aws/; Microsoft, https://www.commerce.senate.gov/services/files/148A94E5-DB50-4EE0-BD16-C52E07F8D3AE; and Google, https://thenewstack.io/googles-generative-ai-stack-an-in-depth-analysis/, among others.

[3] National Institute of Health, National Library of Medicine. (July 2021). "Artificial intelligence in healthcare: transforming the practice of medicine." https://pmc.ncbi.nlm.nih.gov/articles/PMC8285156/.

[4] IBM. (Accessed online April 2025). "Project Ripasso." https://www.ibm.com/products/project-ripasso?utm_content=SRCWW&p1=Search&p4=43700080210104633&p5=b&p9=58700008721154931&gad_source=1&-gclid=Cj0KCQjwy46_BhDOARIsAIvmcwNTRqBUfNXF8KbWPluM64YWogYHUUOCPfDEy-IoyWlXTDwZ2RJ4E-QUaAjxZEALw_wcB&gclsrc=aw.ds.

[5] University of Iowa. (August 27, 2024). "The role of AI in modern education." https://onlineprograms.education.uiowa.edu/blog/role-of-ai-in-modern-education.

[6v]Such as "AI Prompt Engineer." Metcalfe, Charlie. MIT Technology Review. (April 24, 2024). "Job titles of the future: AI prompt engineer." https://www.technologyreview.com/2024/04/24/1091125/ai-prompt-engineer-generative-ai-job-titles/.

[7] Baronchelli, Andrea. The Royal Society Publishing. (January 22, 2024). "Shaping new norms for AI." https://royalsocietypublishing.org/doi/10.1098/rstb.2023.0028.

[8] "What's the Difference Between AI and Machine Learning?". Columbia University, Engineering. (accessed online April 2025). https://ai.engineering.columbia.edu/ai-vs-machine-learning/. AWS. (Accessed online April 2025). "Artificial Intelligence (A) vs. Machine Learning." https://aws.amazon.com/compare/the-difference-between-artificial-intelligence-and-machine-learning/.

[9] Buchanan, Ben. Georgetown University, Center for Security and Emerging Technology. (August 2020). "The AI Triad and What It Means for National Security Strategy." https://cset.georgetown.edu/publication/the-ai-triad-and-what-it-means-for-national-security-strategy/.

[10] Coherent Solutions. (July 9, 2024). "Overview of AI Tech Stack: Components, AI Frameworks, MLOps & IDEs." https://www.coherentsolutions.com/insights/overview-of-ai-tech-stack-components-ai-frameworks-mlops-and-ides#:~:text=But%20first%20things%20first%3A%20what,whole%20structure%20is%20at%20risk.

[11] Office of the Director of National Intelligence. (March 2025). Annual Threat Assessment of the U.S. Intelligence Community https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf.

[12] For examining fairness, transparency, and accountability, the OECD and NIST as well as several private enterprises have developed reliable Responsible AI frameworks. See eg: https://www.nist.gov/artificial-intelligence/ai-research-identifying-managing-harmful-bias-ai and https://oecd.ai/en/ai-principles.

[13] National Institute of Standards and Technology. (December 10, 2020). Security and Privacy Controls for Information Systems and Organizations (NIST SP 800-53 Rev. 5). https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final.

[14] Palo Alto Networks. (Accessed online May 2025). "What is SOC 2 Compliance?' https://www.paloaltonetworks.com/cyberpedia/soc-2.

[15] International Organization for Standardization. (2022). *Information security, cybersecurity and privacy protection—Information security management systems--Requirements*. https://www.iso.org/standard/81230.html. https://www.iso.org/standard/27001.

[16] National Institute of Standards and Technology. (2023). "Artificial intelligence risk management framework (AI RMF 1.0)." https://www.nist.gov/itl/ai-risk-management-framework.

[17] International Organization for Standardization. (2023). "*Artificial intelligence—Management system*." https://www.iso.org/standard/81230.html.

[18] OWASP Foundation. (Accessed online May 2025). "OWASP Top Ten." https://owasp.org/www-project-top-ten/.

[19] Campbell, Lucy, et al. The Guardian. (May 13, 2025). "US tech firms secure AI deals as Trump tours Gulf states." https://www.theguardian.com/technology/2025/may/13/us-tech-ai-trump-gulf-tour.

[20] Indeed, many organizations have. Some of these include: OECD, https://www.oecd.org/en/topics/sub-issues/ai-principles.html; UNESCO, https://www.unesco.org/en/artificial-intelligence/recommendation-ethics; The U.S. Intelligence Community, https://www.intelligence.gov/principles-of-artificial-intelligence-ethics-for-the-intelligence-community; The World Economic Forum, https://www.weforum.org/stories/2021/06/ethical-principles-for-ai/; as well as fifteen AI companies, at https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2023/07/21/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-leading-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/ and https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2023/09/12/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-eight-additional-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/.

[21] Cybersecurity and Infrastructure Security Agency. (October 2023). "Secure by Design: Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software."https://www.cisa.gov/sites/default/files/2023-10/SecureByDesign_1025_508c.pdf.