Written Testimony of Steve Faehl

US Government Security Leader, Microsoft Corporation

US House Committee on Homeland Security, Subcommittee on Cybersecurity and Infrastructure Protection

"Security to Model: Securing Artificial Intelligence to Strengthen Cybersecurity"

June 12, 2025

Chairman Garbarino, Ranking Member Swalwell and Members of the Subcommittee, thank you for the opportunity to discuss the importance of integrating AI solutions into the federal government's cybersecurity defense and resilience efforts. Microsoft takes this responsibility seriously and in my role as US Government Security Leader, I have seen first-hand how public sector organizations accelerate AI modernization efforts to strengthen national resilience.

Microsoft is on the frontlines of cybersecurity, defending US Government organizations against nation-state actors and cybercriminals. With a clear view of both threats, it is imperative for the US government to accelerate adoption of AI capabilities into their cybersecurity defense portfolio. As I explain below, this integration can have an outsized positive impact during a cybersecurity crisis. Without adopting these technologies quickly, the federal government will fall further behind in effectively countering cyber adversaries and securing their systems. Where federal agencies are most effectively utilizing AI, the results have been transformative —dramatically accelerating investigations while significantly reducing costs. Faster AI-enabled cyber analysis is allowing agencies to stay ahead of emerging threats by proactively protecting federal assets from attack. The lower cost of investigations has also opened the door for cyber defense tactics at a scale that would not be otherwise feasible.

Microsoft's telemetry and analysis demonstrate that the cyber threat landscape is only increasing in complexity, sophistication, and scale of adversarial tactics. Knowing this, Microsoft continues to advance and embrace the "security above all else" principle outlined in our Secure Future Initiative (SFI).[1] The SFI represents our commitment to design, build, test, and operate our technology to meet the highest standards for security.

At Microsoft, we see security and artificial intelligence intersecting in three ways: Security *From* AI, Security *With* AI, and Security *Of* AI. In my testimony today, I will discuss these three intersecting points by (1) summarizing the digital threat landscape, (2) explaining generative AI capabilities for cybersecurity that organizations can adopt to counter malicious adversaries; and (3) describing how Microsoft incorporates security into its AI products and services. Through this framework, I will lay out several policy recommendations to advance the use of AI for cyber defense across the US government.

The Digital Threat Landscape

Microsoft aggregates over 70 trillion security signals per day. These signals are sourced from our various cloud services, endpoints, software tools, and partner ecosystem. These signals enable Microsoft to detect and analyze threats across a wide spectrum of digital environments where we

[1] Secure Future Initiative | Microsoft

track more than 1,500 unique threat groups, including over 600 nation-state actors and 300 cybercrime organizations.[2]

As Microsoft's most recent Digital Defense Report notes, every day, Microsoft defends against more than 600 million cyberattacks targeting its customers, ranging from phishing and ransomware to identity-based intrusions and distributed denial-of-service (DDoS) attacks. In the second half of 2024 alone, Microsoft mitigated 1.25 million DDoS attacks, a fourfold increase from the previous year. This surge in threat volume underscores the growing sophistication and scale of adversarial tactics, prompting Microsoft to continuously evolve our detection and response capabilities.

To meet these escalating challenges, Microsoft commits substantial resources to cybersecurity, with approximately 34,000 full-time equivalent engineers dedicated to security initiatives. These professionals focus on enhancing defenses, developing phishing-resistant multi-factor authentication, and securing Microsoft's infrastructure and customer environments. This workforce is further supported by a network of 15,000 specialized security partners, reinforcing Microsoft's ability to respond swiftly and effectively to emerging threats.

Microsoft believes in sharing our insights about the who, what, and why of malicious cyber activity with the government, our customers, and the public. This level of transparency is critical to strengthening our cyber ecosystem and staying ahead of the threats. One key example of this is Microsoft's role in identifying and responding to the activities of two significant Chinese nation-state threat actors: Volt Typhoon and Salt Typhoon.

Volt Typhoon, active since at least mid-2021, targeted US critical infrastructure sectors—including communications, utilities, and transportation—using stealthy "living-off-the-land" techniques that rely on legitimate credentials and tools to evade detection. The threat actor maintained persistent access in an effort to potentially cause disruptions and sow distrust during geopolitical crises. Microsoft's Threat Intelligence Center (MSTIC) was integral in publicly identifying this campaign in May 2023.[3]

In addition, Salt Typhoon was tracked by Microsoft since 2020. The attack reportedly infiltrated 9 major US internet service providers, raising concerns about access to sensitive law enforcement and intelligence data. Microsoft worked closely with the US government and our customers to detect, remediate, and coordinate responses to these threats. Both efforts demonstrate Microsoft's commitment to transparency, collaboration, and proactive defense in the face of sophisticated, nation-state cyber espionage campaigns.

With the digital landscape blinking red and nation-state adversaries targeting US critical infrastructure, using AI to improve cyber defense posture is necessary for all organizations.

Observations on malicious actors' use of AI & Microsoft's response

While we are not seeing threat actors' use of AI to create novel threats at scale, they are leveraging AI to increase productivity, automating the creation of phishing emails, generating deepfake content, and conducting large-scale social engineering campaigns. Just last week, our Digital

[2] Microsoft Digital Defense Report 2024

[3] Volt Typhoon targets US critical infrastructure with living-off-the-land techniques | Microsoft Security Blog

Crimes Unit (DCU) published a blog detailing the take-down of a global "cybercrime-as-a service" network, which impersonated Microsoft tech support targeting older Japanese individuals.[4]

To illustrate this example, through our investigation in partnership with officials in Japan and India, we learned these cybercriminals used generative AI to scale their operations by identifying potential victims, automating the creation of malicious pop–up windows, and performing language translations to target Japanese victims. AI-driven tools can also craft highly convincing phishing messages mimicking legitimate communications, increasing the likelihood of successful credential theft. We've also observed deepfake technology being used to impersonate executives and manipulate audio and video content, posing severe risks to organizational integrity and trust. We will continue to share insights into the evolving use of AI by threat actors and foster collaboration with industry and government partners to strengthen the broader cyber ecosystem.

SECURITY FROM AI – Advanced detection and response

To counter these AI-enabled threats, Microsoft has invested heavily in advanced detection and response capabilities. We employ machine learning algorithms to identify patterns and anomalies indicative of AI-generated attacks. Microsoft's Defender Threat Intelligence platform integrates these capabilities, providing real-time insights and automated defenses against AI-driven threats. By continuously analyzing vast amounts of data from its global network, Microsoft can swiftly detect and mitigate attempts to exploit AI for malicious purposes.

Over a year ago, we also implemented the AI Threat Actor policy[5] framework, which is designed to prevent the use of AI by the most advanced nation-state adversaries and cybercriminals.[6] Key areas of our policy include:

- Detection and disruption of AI use-even if innocuous-- by nation-state Advanced Persistent Threats (APTs), Advanced Persistent Manipulators (APMs,) and cybercriminal syndicates, including account termination and service restrictions.

- Cross-provider notification, where Microsoft alerts other AI service providers when threat actors misuse their platforms.

- Ecosystem collaboration to share intelligence and coordinate responses to AI abuse.

- Transparency reporting to inform the public and stakeholders about threat actor activity and Microsoft's mitigation actions.

Meaningful intelligence sharing and ecosystem collaboration are important measures for industry and the government to develop as AI technology becomes more integrated into systems and our lives. Examples of efforts that Microsoft participates in include:

- Microsoft partnered with OpenAI and published research on how threat actors are using AI products and services. Our analysis of the current use of large language model technology by state-affiliated threat actors revealed behaviors consistent with attackers using AI as another

[4] Cross-border collaboration: International law enforcement and Microsoft dismantle transnational scam network targeting older adults - Microsoft On the Issues.
[5] Staying ahead of threat actors in the age of AI | Microsoft Security Blog
[6] https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai/?msockid=3d87261edbdc6668281335f2da6b6786

productivity tool, querying open-source information, translating, finding coding errors, and running basic coding tasks.

- Microsoft shares countermeasures and insights with the wider ecosystem, via frameworks such as MITRE ATT&CK and helped launch MITRE ATLAS™, which maps Adversarial Threat Landscape for Artificial-Intelligence Systems.

- Through the Frontier Model Forum (FMF), Microsoft has entered into a first-of-its-kind partnership to facilitate information-sharing on threats, vulnerabilities, and capability advances unique to frontier AI. Since 2017, Microsoft has hosted the AI Red Team Colloquium, fostering peer-to-peer engagement across leading AI labs and security teams.

Strong government-industry partnerships and transparency about adversaries' use of AI will enhance our cyber defense and mitigate risk. This feedback loop will improve AI technology focused on cyber defense.

SECURITY WITH AI – How generative AI can help cyber defenders

Microsoft is making significant investments in AI innovation to provide cybersecurity defenders with an asymmetric advantage over increasingly sophisticated attackers. Lessons from defending Ukraine have highlighted how AI can dramatically enhance defensive capabilities, addressing long-standing challenges such as talent shortages, burnout, and the need for speed, scale, and precision in cyber response. Key areas where we see real-world examples of AI transforming cyber defense include:

- **Scaling the cyber workforce:** The cybersecurity talent shortage continues to challenge organizations, but Security AI tools offer a force multiplier by augmenting human capabilities and alleviating expertise bottlenecks. AI can support junior analysts, accelerate skill development, and enable teams to respond more effectively in a crisis. Specialized Security AI agents enable a scalable, digital cyber defense workforce that can be activated instantly during crises and scaled back during normal operations. This surge capability ensures organizations are not caught flat-footed, avoiding saturation in the face of large-scale attacks or simultaneous incidents. By combining human judgment with AI-driven scalability, we can build a more resilient, responsive, and adaptive cyber defense posture.

- **Secure code development**: AI can potentially assist developers in writing more secure code by providing real-time feedback and vulnerability detection or reduce false positives created by traditional code analysis tools. AI-powered tools can also help developers adhere to best practices and coding standards, and in time will be able to reliably reduce the likelihood of introducing security flaws.
    - In the next five years, up to 95% of software code written by software developers will be done with the assistance of AI. This trend provides an opportunity to prevent vulnerabilities altogether by centralizing efforts for secure by design with a tested and vetted list of high-quality AI code generators.

- **Improving baseline security posture**: AI can continuously monitor an environment and recommend adjustments, helping close gaps that security teams might miss in fast-changing conditions, closing common gaps that can go unnoticed or take time for security teams to identify in a rapidly changing environment.

- For example, the Conditional Access Optimization Agent in Microsoft Entra monitors for new users or apps not covered by existing policies, identifies necessary updates to close security gaps, and recommends quick fixes for identity teams to apply with a single click.
- Similarly, the Vulnerability Remediation Agent for Intune identifies, evaluates, and prioritizes vulnerabilities. It continuously monitors newly published threats, assesses their risk levels, and offers clear, actionable recommendations for remediation.

- **Novel Threat Detection**: AI based threat detection is capable of detecting threats that haven't been seen before and is much more resilient to changes in threat actors tactics and objectives. More capable detections that are harder to evade impose an increased cost on attackers.

As the above examples show, generative AI can significantly enhance cyber defense by streamlining the patching process, creating a scalable cyber defense workforce, strengthening secure code development and active threat detection. Accelerating the use of these technologies across organizations will have a positive impact on the cyber ecosystem and help defenders regain the advantage.

SECURITY OF AI – Engendering trust in AI technology through security protocols

For generative AI to be embraced and its adoption accelerated across organizations, it must be trusted—and that trust must be earned through demonstrable security protocols. At Microsoft, we are committed to AI that is secure by design and default by seeking to embed guardrails at every layer of the AI stack: from infrastructure and platforms to models, systems, and the applications that rely on them. SFI underscores Microsoft's commitment to build AI systems with rigorous threat modeling, secure open-source software practices, and US and international standards in mind.

While many traditional software security practices remain relevant, AI systems also introduce unique challenges—such as safeguarding model weights and mitigating prompt injection attacks—that also demand more specialized approaches such as content safety filters and prompt shields. That's why we apply both internal and third-party AI attack taxonomies at all layers of the stack, conduct red teaming and adversarial testing, and empower customers with tools that perform risk analysis on AI systems, like PyRIT and AI-specific monitoring across hybrid and multi-cloud environments. Our AI Red Team regularly probes models and high-risk systems, and we incentivize external research through AI bug bounty programs. We also advance transparency through Coordinated Vulnerability Disclosure and structured patch management. Importantly, we recognize that securing AI is not a one-time event but an iterative and continuous process—one that evolves with emerging threats and technologies. [7]

In addition to our layered security approach to the AI technology stack, we actively collaborate with government partners like NIST (and its Secure Software Design Framework Profile for Generative AI) and through forums like the Frontier Model Forum and the Coalition for Secure AI (CoSAI) to share best practices. These efforts collectively underscore our commitment to fostering a secure and resilient AI ecosystem for the future.

[7] For more on our approach to AI policy and practices: Responsible AI: Ethical policies and practices | Microsoft AI.

Policy recommendations to enable use of AI for cyber defense

Given the strategic importance of AI in achieving asymmetric advantage and prevailing across the digital landscape —especially for the US Government – I offer the following policy suggestions for the Subcommittee's consideration:

- **Federal workforce readiness**: Education and awareness of AI capabilities is one of the largest impediments to adoption. Lack of access to AI platforms and significant compute capacity is leading many federal data scientists to move to the private sector. The US government needs to be a leader in AI investment and education in order to be a leader in the adoption of AI. Congress should consider ways in which it helps facilitate awareness of AI capabilities within the government and additional downstream efforts to inform critical infrastructure owners and operators around the country.

- **Cyber deterrence**: Finding ways to impose sufficient costs to deter adversaries from conducting cyber operations against the US government and US critical infrastructure is an important aspect of addressing cyberspace as a highly-contested environment. Even with an accelerated adoption of the most advanced defensive AI capabilities, nation state rivals like China are unlikely to be dissuaded from further investing in offensive cyber capabilities to compromise any vulnerable systems in the US. We encourage Congress to assess whether additional steps are needed to strengthen counter-measures against nation state cyber threat actors to discourage this behavior. Possible ideas for consideration include examining whether the targeting of US critical infrastructure with offensive cyber operations and/or prepositioning of malware for disruptive or destructive cyber attacks should be declared off-limits by the US government – as violations of international norms and laws – and examining improvements to public attribution of cyber attacks for greater deterrent impact. The US government should also consider framing a hierarchy of deterrence consequences with an all-tools approach and not constrain itself to only a cyber response.

- **Reforming traditional acquisition models to meet the AI moment**: Traditional IT acquisition often overlooks AI integration in cybersecurity. As Congress considers expanding AI use across agencies and critical infrastructure, it may want to explore centralized acquisition models that accelerate adoption and enhance security agility.

In conclusion, the integration of AI into cybersecurity strategies is not just a technological advancement but a necessity for staying ahead of increasingly sophisticated cyber threats. By prioritizing AI-driven innovation, transparency, and collaboration with industry peers, government agencies, and technology providers, we can build a resilient cyber defense ecosystem. This collective effort will ensure that we are better equipped to safeguard our digital infrastructure, protect sensitive data, and maintain trust in our technological advancements.

Cybersecurity stands as one of the most impactful—and lowest-risk—applications of artificial intelligence. In the face of increasingly sophisticated and large-scale threats, the only certainty is that inaction will lead to failure.