Microsoft

Shaping Global Policy for a Secure Future

Secure Future Initiative

Introduction

Cybersecurity is foundational to global stability, economic growth, and public trust. Microsoft's Secure Future Initiative (SFI) is designed to embed security at every level of our operations, from product design to daily execution. Complementing this, our cybersecurity policy and diplomacy (CPD) efforts extend SFI's impact by engaging the multistakeholder community to make security a shared priority.

01.

Fostering a security-first culture in artificial intelligence (AI)

02.

Strengthening global cybersecurity and resilience

03.

Reinforcing international cybersecurity norms and accountability

This paper explores three core areas of focus. The first is fostering a security-first culture in artificial intelligence (AI). As AI reshapes the digital landscape, securing its development and use is critical. Microsoft's efforts span countering threat actors' malicious use of AI; leveraging AI for defenders; and ensuring the security of AI systems, models, and serving infrastructure. These initiatives include shaping global policy, sharing of tools and best practices and advancing diplomacy to ensure AI technologies are developed and deployed responsibly and securely.

The second area is strengthening global cybersecurity and resilience. Building resilience requires more than technology, it demands capacity, alignment, and foresight. This includes adopting emerging technologies to stay ahead of evolving threats, investing in strategic cybersecurity capacity building to equip nations and organizations with the skills and frameworks needed to protect critical infrastructure, and regulatory alignment to reduce complexity and deliver consistent protection across jurisdictions. Making AI security and quantum safety national cybersecurity priorities is essential for addressing emerging risks. By grounding these efforts in international risk-based standards and aligning with existing regulations, organizations can maximize the impact of cybersecurity talent and deliver stronger and more consistent defenses online.

The third focus is reinforcing international cybersecurity norms and accountability. Protecting civilians and critical infrastructure requires clear rules and mechanisms for enforcement. Through multistakeholder diplomacy and public-private partnerships, Microsoft is strengthening global rules, promoting transparency, and supporting mechanisms to identify violations and impose consequences. These efforts aim to reduce the risk of escalation and foster trust in the digital ecosystem.

As the threat landscape evolves, so too will cybersecurity policy and diplomacy. Geopolitical dynamics, technological innovation and rising policymaker expectations will continue to shape the agenda. Microsoft remains committed to championing with thought leadership, partnerships, and innovation — safeguarding the shared digital ecosystem for customers, communities and partners worldwide.

Promoting a security-first culture in AI

Microsoft's engineering teams are embedding security-first principles into every layer of our AI stack. In parallel, our AI security policy and diplomacy efforts center on collaborating with the multistakeholder community to ensure that AI is developed and deployed securely across sectors. Building on the foundation of Microsoft's SFI, we extend this commitment beyond our own operations to support governments, industry, and partners to strengthen defenses against emerging threats.

3 Policy Areas

The following section details Microsoft's approach to AI security across three policy areas:

(i) countering threat actors' malicious use of AI,
(ii) advancing AI for defenders, and
(iii) ensuring the security of AI.

A. Countering threat actors' malicious use of AI

The rapid evolution of AI brings both opportunities and risks. Threat actors, from opportunistic hackers to sophisticated state actors, are increasing the volume and sophistication of attacks using AI. Microsoft has observed AI being used for vulnerability research, refined operational command techniques, and detection evasion and social engineering.

To address this growing challenge, Microsoft has taken significant steps to prevent threat actors from misusing and accessing AI.

In partnership with OpenAI, we also adopted a principled approach to detect and disrupt threat actors using our AI models, systems, and technology. As part of that work, Microsoft has committed to alerting other AI providers when threat actors leverage their platforms and to sharing threat intelligence and countermeasures through frameworks such as MITRE ATT&CK and MITRE ATLAS™. To further advance security, Microsoft's AI Red Team has developed open-source toolkits and built the AI Red Teaming Agent to help organizations proactively identify and address risks in generative AI applications.

Secondly, we co-founded the Coalition for Secure AI, an open-source initiative that equips practitioners and developers with guidance and tools to build secure-by-design AI systems. We also joined other firms in the Frontier Model Forum to sign a first-of-its-kind agreement facilitating information sharing among industry, government, and civil society on vulnerabilities, threats, and capabilities unique to frontier AI.

Finally, during the Paris AI Action Summit, Microsoft announced its Frontier Governance Framework, designed to monitor emerging AI capabilities that could pose national security or large scale public safety risks. The framework establishes processes for assessing and mitigating these risks, so that AI models can be deployed in a secure and trustworthy way. Throughout this work, Microsoft works closely with governments worldwide to proactively assess the national security implications AI.

B. Advancing AI for defenders

Defenders are increasingly leveraging generative AI to shift the balance in their favor— accelerating vulnerability discovery, prioritizing risk-based patching, and streamlining incident response through real-time analysis and automation. This is critical for operators of essential infrastructure and operational technology (OT) systems, where resources and cybersecurity expertise are often limited.

Across Europe, through Microsoft's European Security Program, we are expanding AI-based threat intelligence sharing to help governments stay ahead of emerging threats. However, technology alone is not enough. Persistent barriers to AI adoption for defenders include talent and skills gaps in cybersecurity. To address this, in July 2025, Microsoft launched Elevate, a global commitment to empower people by equipping them with the skills, knowledge, and tools needed to thrive with AI.

Microsoft also supports non-governmental organizations (NGOs) with nearly 100 Microsoft employees volunteering through the CyberPeace Institute (CPI) to defend the most vulnerable in cyberspace. AI helps close skills gaps by generating training content, upskilling new defenders, and freeing experienced analysts for higher-impact tasks.

To ensure responsible use of AI in defense, Microsoft co-launched the Roundtable for AI, Security, and Ethics (RAISE) with the United Nations Institute for Disarmament Research (UNIDIR) in 2024. Guided by the principles of compliance with international humanitarian law (IHL), international human rights law, and established norms of responsible state behavior in cyberspace, RAISE fosters inclusive, cross-regional dialogue and consensus-building around the responsible use of AI in security and defense. In April 2025, RAISE hosted the inaugural Global Conference on AI, Security, and Ethics at the United Nations influencing submissions to the UN Secretary-General's report on AI in the military domain.

C. Ensuring the security of AI

Microsoft's SFI emphasizes transparency, accountability, and human oversight in AI-driven security. By embedding these values into the design and deployment of AI for cyber defense, we can ensure that innovation in cybersecurity is both effective and trustworthy. This includes applying and extending security best practices to AI systems— such as secure-by-design and development, Zero Trust architecture, multi-factor authentication, and role-based access controls. We are also at the forefront of addressing emerging threats such as data poisoning and prompt injection attacks. Through initiatives like the GitHub Secure Open Source Fund, we support open-source projects that underpin the AI stack.

Mission-focused public-private partnerships remain pivotal. In the UK, Microsoft is collaborating with the Laboratory for AI Security Research (LASR) on a joint research program into AI-cybersecurity challenges, focusing on critical infrastructure and agentic AI security.

At its core, Microsoft's approach to AI security policy is rooted in proactive collaboration, innovation, and responsible stewardship -countering malicious use of AI, advancing AI-driven defenses, and ensuring the robust security of AI systems and serving infrastructure.

Enhancing global cybersecurity and resilience

In today's dynamic threat landscape, strengthening global cybersecurity and resilience requires bold action: embracing emerging technologies like post-quantum cryptography (PQC), scaling cybersecurity capacity building, and aligning cybersecurity regulations to support operational cyber defense.

This section highlights our advocacy efforts to transition to quantum-safe cryptography, expand capacity building in the Global South, and foster industry-wide engagements to better align existing and future cybersecurity regulations. It also explores innovative initiatives, such as the Digital Emblem, a machine-readable marker led by the International Committee of the Red Cross (ICRC) that designates medical and humanitarian systems as protected under international humanitarian law.

A. Transitioning to Post-Quantum Cryptography (PQC)

Quantum computing holds transformative potential across fields like medicine and material sciences, but it also introduces significant cybersecurity risks. As quantum capabilities advance, they threaten to undermine some of the current cryptographic systems, exposing sensitive data to compromise. A key concern is the "harvest now, decrypt later" tactic, where adversaries collect encrypted data today with the intent to decrypt it using quantum computers in the future. Although widespread quantum computing may not arrive until the 2030s, the urgency to transition to quantum-safe cryptography is immediate.

Transitioning the digital ecosystem requires collaboration on a global scale. Through partnerships, Microsoft contributes to multiple initiatives to facilitate the quantum-safe transition. These include the NIST Post-Quantum Cryptography Project, the National Cybersecurity Center of Excellence Migration to Post-Quantum Cryptography, the Internet Engineering Task Force (IETF), the Open Quantum Safe (OQS) project, and MITRE's Post-Quantum Cryptography Coalition. Through these efforts, we are helping develop quantum-safe algorithms, supporting their adoption in standards like TLS and X.509, and advocating for accelerated adoption across commercial and open-source technologies.

Microsoft is also engaging policymakers worldwide to prioritize the transition to quantum-safe cryptography as a national cybersecurity priority. Grounded in the principle of "security above all else," we actively work with governments to align strategies across jurisdictions, adopt international standards to avoid fragmentation, and promote adoption of transparent transition plans for government systems. Early and progressive timelines are critical to avoid delays and maintain trust in the digital infrastructure underpinning modern society.

B. Capacity building in the Global South

Cybersecurity capacity building equips nations and organizations with the expertise, frameworks, and operational readiness to counter increasingly sophisticated cyber threats. To advance this work, Microsoft launched the Advancing Regional Cybersecurity (ARC) Initiative, a partnership between Microsoft and Kenya's National Computer and Cybercrime Coordination Committee (NC4). This initiative aims to strengthen incident response and recovery through cross-sector collaboration— facilitating a stakeholder roundtable, a tabletop exercise, and producing an adaptable toolkit to enhance cybersecurity preparedness.

Beyond ARC, Microsoft supports the development and improvement of national cybersecurity strategies and contributes to resources such as the International Telecommunication Union's (ITU) Guide to Developing a National Cybersecurity Strategy. These efforts enable governments, particularly in the Global South, to strengthen their cyber defenses, align with international best practices, and build resilient digital infrastructures essential for sustainable growth and security. By investing in scalable, locally driven solutions, we empower governments in the Global South to defend against cyber threats and foster long-term security and prosperity.

C. Advancing cybersecurity regulatory alignment

The proliferation of fragmented cybersecurity regulations worldwide creates operation friction and diverts resources from effective cyber defense, for governments and industry. While regulation is essential for resilience, inconsistent definitions, reporting thresholds, and security requirements hinder effective collaboration, especially for organizations operating across multiple jurisdictions or with constrained capacity. Recognizing this, and rooted in SFI's vision of security first, Microsoft encouraged regulatory alignment and reciprocity, advocating for high-level commitments and international dialogue through forums such as the Organisation for Economic Co-Operation and Development (OECD). In April 2025, Microsoft joined a coalition of over 50 Chief Information Security Officers (CISOs) urging governments to strengthen alignment.

A landmark is the 2024 European Union (EU) Cyber Resilience Act (CRA), which sets baseline requirements for products with digital elements across the EU. Microsoft actively participates in the CRA Expert Group, which provides expertise and assistance to the Commission as it prepares additional supporting legislation and guidance. Microsoft also contributes in CRA standardization processes to ensure practical, effective, and globally interoperable standards. Implementation will nevertheless remain complex, requiring harmonization across the CRA poses challenges, particularly in coordinating the EU's independent conformity assessment bodies and market surveillance authorities. The European Commission is expected to clarify implementation guidance through implementing acts by December 2025, with significant work to continue in 2026. Our engagement reflects a commitment to fostering innovation, strengthening resilience, and delivering consistent protection for users and organizations worldwide.

D. Digital Emblem

In modern conflicts, humanitarian and medical networks are often indistinguishable from the broader internet, leaving them exposed to cyber operations. Led by the ICRC, the Digital Emblem is a machine-readable, globally recognizable marker, analogous to the Red Cross, Red Crescent, and Red Crystal, that designates these systems as protected under international humanitarian law. Advancing as a standard in the Internet Engineering Task Force (IETF), the Emblem enables verified operators to tag specific domains, internet protocol (IP) ranges, and workloads so that platforms and defenders can recognize and prioritize their protection.

Built-in safeguards, such as verification of eligibility, anti-abuse controls, and privacy-preserving design ensure accountability and prevent misuse. The Emblem turns norms into operational reality: a standardized signal that products can enforce by default; automation that elevates protection; and multistakeholder implementation that is tested and refined and then scaled. Microsoft has supported the Emblem from its inceptions and continues to contribute to standards, reference implementations, and operationalization to better protect civilians and the essential services they rely on.

Reinforcing international cyber norms

Cyber threats, particularly those conducted by nation states, are escalating in scale and sophistication. This reality underscores the urgent need for the international community to define and uphold what constitutes responsible behavior in cyberspace. Recent developments, such as the conclusion of the UN Open Ended Working Group (OEWG) on Information and Communication Technologies (ICTs) security and the launch of the New Global Mechanism come at a critical time. While the OEWG demonstrated that consensus remains possible, even in a polarised geopolitical climate, the international law and stakeholder provisions remain weak. Unless these provisions are significantly strengthened, the new mechanism risks losing legitimacy and effectiveness. In an era of deep geopolitical and technological tensions, multistakeholder diplomacy— bringing together governments, industry and civil society— is more important than ever.

A. Promoting responsible behavior in cyberspace

This section outlines Microsoft's collaborative diplomacy efforts with industry partners and beyond to reinforce international cyber norms. Our work includes advancing accountability and responsible state behavior through initiatives such as the Cybersecurity Tech Accord, which unites over 160 global technology companies around shared commitments to protect users and promote responsible conduct. Since its inception, the Cybersecurity Tech Accord has played a pivotal role in shaping international cybersecurity dialogues, including through active engagement in the OEWG. These efforts push back against authoritarian models of internet governance and advocate for an open, interoperable, and rules-based digital environment.

Yet, even with agreed norms, the boundaries of acceptable behavior remain contested, particularly in the murky space between legitimate intelligence gathering and destabilizing cyberespionage. To address this, Microsoft has partnered with American University (AU) to convene a series of roundtables focused on the real-world costs of cyberespionage. Insights from these discussions will inform a forthcoming policy paper with recommendations for clearer boundaries and stronger norms to prevent escalation, expected to be published this fall.

B. Cyber deterrence

Beyond norm-setting, deterrence is essential. Calling out violations and attributing malicious activity is an important first step, but it must be paired with sufficient consequences, including political pressure, to uphold international expectations.

In 2025 Microsoft publicly attributed several cyber operations to nation state threat actors. This included activity conducted by Russian (Void Blizzard) and Chinese (Silk Typhoon) nation state groups. The North Atlantic Treaty Organization (NATO) statement of solidarity and condemnation was encouraging, but more must be done to impose cost to violators. This is why Microsoft is supporting new research, led by the Royal United Services Institute (RUSI), to explore innovative approaches for effective cyber deterrence.

C. Cyber mercenaries

We are also addressing the growing threat of cyber mercenaries— private sector actors developing and selling commercial cyber intrusion capabilities, sometimes based on zero-day exploits. Valued at least $12 billion, this market fuels escalation and proliferation and presents grave risks to national security and human rights. Microsoft is tackling this challenge through technical and legal disruption of malicious use of zero-day exploits against our customers.

We are complementing these approaches by encouraging the development of responsible approaches of the use of these technologies. For example, Microsoft recently partnered with Foreign Policy on a pioneering report highlighting the scope of the problem and has been a strong advocate for the continued adoption of the Pall Mall Code of Practice, now endorsed by 27 governments.

D. Ransomware

Finally, ransomware remains one of the most persistent threats, particularly to critical sectors, such as healthcare. Attacks have surged nearly fivefold in the past five years, according to research from our partners at Foreign Policy Analytics. Their research also highlighted that ransomware actors continue to thrive, in part because they operate with impunity from jurisdictions that serve as de facto "safe havens". Microsoft is advocating for greater accountability for those states, including treating ransomware attacks on civilian infrastructure as potential crimes against humanity, when they result in severe harm, including loss of life. These efforts, grounded in international law and due diligence principles, aim to close the enforcement gap and strengthen global resilience.

Through these combined actions— advancing norms, promoting accountability, and driving deterrence— Microsoft is reinforcing the vision of the SFI for a safer, more predictable cyberspace where collective defense is possible and trust underpins technological progress.

Conclusion

In today's rapidly evolving digital landscape, cybersecurity policy and diplomacy must be proactive, adaptable, and rooted in collaboration. As threats grow in complexity— fueled by advances in AI— political and diplomatic leadership is essential for global alignment, fostering meaningful multistakeholder partnerships, and reinforcing trust in the digital ecosystem.

Driving progress requires prioritizing regulatory interoperability, strengthening international norms, promoting responsible behavior in cyberspace by all actors, and investing in capacity building. These measures empower organizations and governments alike to strengthen resilience and ensure accountability across borders.

These efforts complement Microsoft's SFI, which focuses on improving Microsoft's own security posture, embedding robust protections across all our products and services, and equipping customers with guidance and tools they need to defend against evolving threats. Together, these initiatives reflect a broader commitment to making security a shared responsibility across industry, government, and civil society.

Ultimately, collective action, grounded in the key areas outlined in this paper, are essential to safeguarding the digital ecosystem and ensuring that security remains at the heart of technological progress.


Microsoft