Microsoft

Microsoft Digital Defense Report 2025
Governments and Policymakers Executive Summary

Lighting the path to a secure future

A Microsoft Threat Intelligence report

Introductory statement by Amy Hogan-Burney and Igor Tsyganskiy from the full report

Mobilizing for impact:

Cybersecurity leadership in a defining era

Amy Hogan-Burney
Corporate Vice President,
Customer Security & Trust

Igor Tsyganskiy
Corporate Vice President and
Chief Information Security Officer

We are living through a defining moment in cybersecurity. As digital transformation accelerates, supercharged by AI, cyber threats increasingly challenge economic stability and individual safety. Cyber threats are rapidly evolving from technical problems affecting business to events impacting all aspects of our society.

The pace of change in the threat landscape has pushed us to rethink traditional defenses. The growth and adoption of AI by both defenders and threat actors benefits both sides. AI in cybersecurity is already creating new challenges for security organizations as they rush to adapt systems, understand new threats, and equip their people with new knowledge to keep pace.

Cyber threats are also playing an increasingly significant role in geopolitical conflicts and criminal activities, creating both a wide and deep scope of responsibility for defenders. AI will play a critical role in helping security professionals productively address the growing threat landscape, but as an industry we must step into this new paradigm cautiously. With the increased speed of an AI-centric world, the impact of action–whether by security organizations, criminal actors, or nation states–will have faster and potentially greater second, third, or fourth-order effects. It is imperative that defenders consider these ripple effects as they implement new security controls, share security research, fix new security vulnerabilities, and collaborate with each other.

Adversaries, whether nation-states, criminal syndicates, or commercial cyber mercenaries, are leveraging emerging technologies to attack with both greater volume and more precision than ever before, often by exploiting the trust that underpins our digital lives. International collaboration among defenders will be critical to define new coordinated defenses and set new international norms that enforce consequences for cyberattacks targeting the global critical infrastructure or essential services.

For security leaders, the imperative is clear: cybersecurity must be a priority, embedded into the fabric of organizational strategy and addressed regularly as part of risk management. Global partnerships across industry peers and even competitors must be established to coordinate and collaborate on defenses against common adversaries. Traditional perimeter defenses are no longer sufficient. Resilience must be designed into systems, supply chains, processes, and governance. New types of threats will emerge with increasing frequency; being informed and prepared is critical.

What's new in this year's report

AI as both a defensive necessity and a target

We're witnessing adversaries deploy generative AI for a variety of activities, including scaling social engineering, automating lateral movement, engaging in vulnerability discovery, and even real-time evasion of security controls. Autonomous malware and AI-powered agents are now capable of adapting their tactics on the fly, challenging defenders to move beyond static detection and embrace behavior-based, anticipatory defense.

At the same time, AI systems themselves have become high-value targets, with adversaries amping up use of methods like prompt injection and data poisoning to attack both models and systems, which could lead to unauthorized actions, data leaks, theft, or reputational damage.

Diverse vectors for initial access

In today's world, campaigns rely on multi-stage attack chains that mix tactics and techniques such as social engineering and technical exploits. This year, we saw the widespread adoption of "ClickFix," a social engineering technique that tricks users into executing malicious code themselves, bypassing traditional phishing protections. We also saw the incorporation of new access methods like device code phishing by both cybercriminal and nation-state actors.

The pervasive threat of infostealers

Increasingly, adversaries aren't breaking in, they're logging in. In today's specialized cybercrime economy, access is essential, and infostealers are a way for operators to collect credentials and tokens for sale on the dark web. Follow-on activities by the buyers of compromised credentials can include ransomware, data exfiltration, and/or extortion. Overall, this means that organizations that experience an infostealer infection are at high risk of future breaches.

Nation-state actors expanding operations

Geopolitical objectives continue to drive a surge in state-sponsored cyber activity, with a notable expansion in targeting the communications, research, and academia sectors. These expansions are mostly within expected scope and volume, and primarily focused on using cyber espionage against typical targets to complement traditional intelligence operations. Building on a trend we first noted last year, nation states continue to accelerate AI use to evolve their cyber and influence operations, making them more scalable, advanced, and targeted.

We urge you to read this report with a bias toward action. It is not just a reflection of the challenges both past and future; it is a call to mobilize, prepare, and confront. Innovation, resilience, and partnership are the pillars of a secure digital future. By embracing these principles, we can navigate uncertainty and build a world where technology empowers and protects us against the rising tide of threats.

AE HoganBurney

Amy Hogan-Burney
Corporate Vice President,
Customer Security & Trust

Igor Tsyganskiy

Igor Tsyganskiy
Corporate Vice President and
Chief Information Security Officer

Visit **microsoft.com/mddr**
for the full report

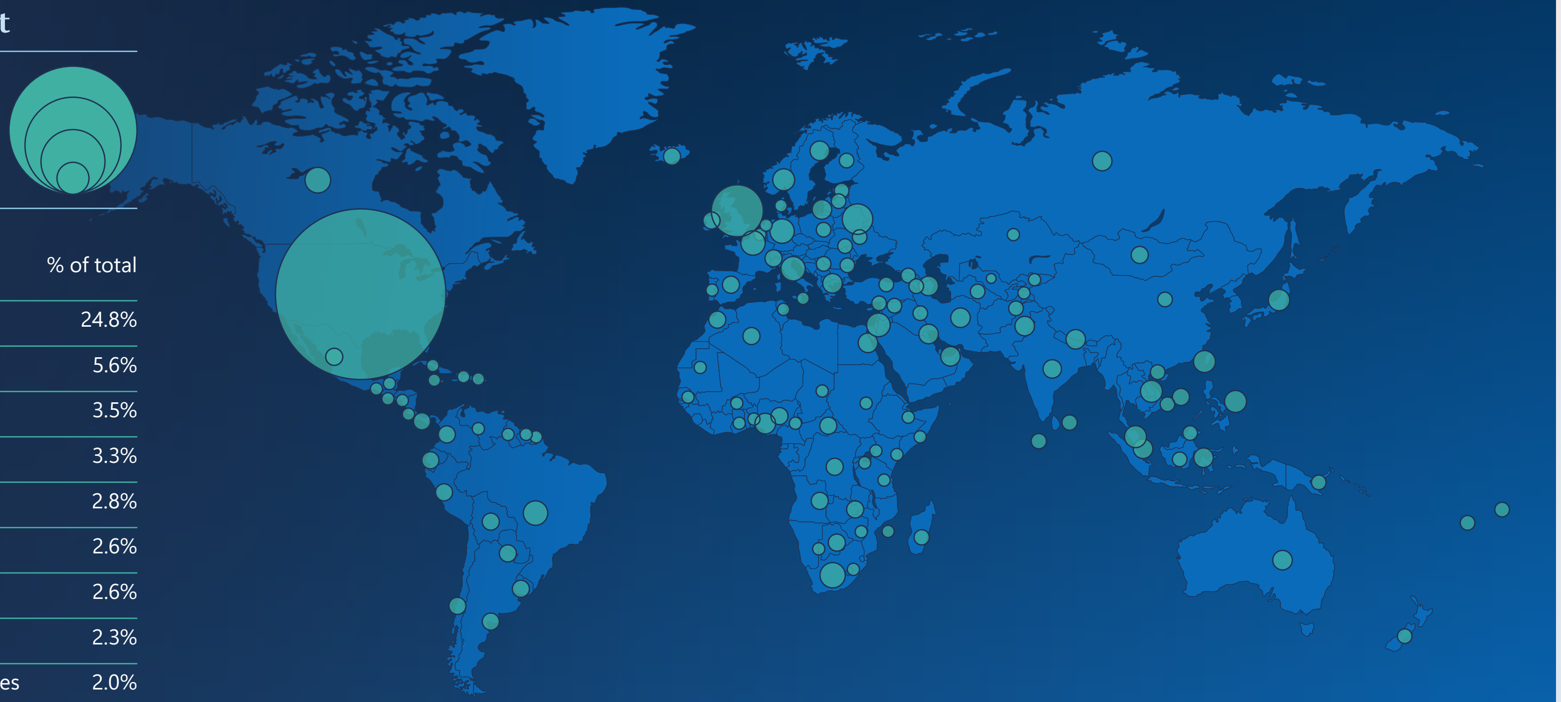
How threat actors are shaping the cyber risk environment

2025 marks a turning point in the cyber threat world. Attacks are increasingly defined by speed, scale, and sophistication.

Looking back over the past year, we've continued to see actors accelerate their development of new and novel techniques to challenge the defenses organizations are implementing to detect and prevent them. However, the daily threats organizations face largely remain the same: attacks by opportunistic threat actors targeting known security gaps. While users globally are at risk, we've observed most attacks in the last six months focused on the United States, the United Kingdom, Israel, and Germany.

For an interactive map with additional details visit **microsoft.com/mddr**

Countries where customers are most frequently impacted by cyber threats (January-June 2025)



Scale of impact

Most impacted

Least impacted

		% of total
1	United States	24.8%
2	United Kingdom	5.6%
3	Israel	3.5%
4	Germany	3.3%
5	Ukraine	2.8%
6	Canada	2.6%
7	Japan	2.6%
8	India	2.3%
9	United Arab Emirates	2.0%
10	Australia / Taiwan	1.8%

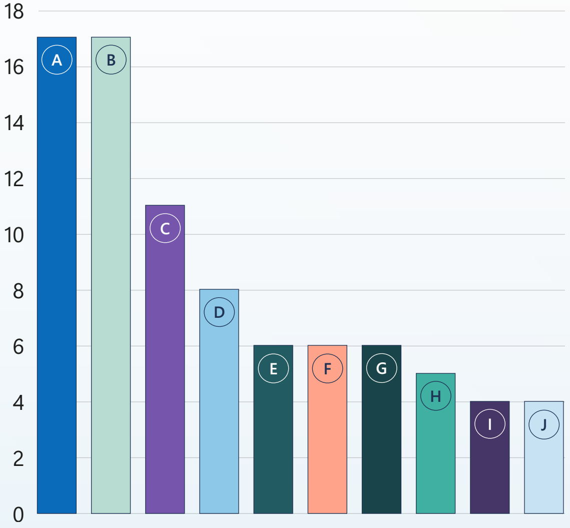
Source: Microsoft Threat Intelligence

Adversaries are targeting entities for data

Government organizations, IT companies, and research and academia were the sectors most impacted by cyber threats this year, as they were last year. These organizations manage critical public services and store vast amounts of sensitive data, including personally identifiable information (PII) and authentication tokens, which can enable future attacks.

Additionally, many government, non-governmental organizations (NGO), and research and academia institutions operate on legacy systems that are difficult to patch and secure, and have small IT teams with limited incident response capabilities. This makes them high-value targets for both nation-state actors and financially motivated cybercriminals. Given adversaries' desire for data, it is no surprise that in the past year, Microsoft Incident Response, the Detection and Response Team (DART) observed attackers performed data collection in 79.5% of reactive engagements.

Ten global sectors most impacted by threat actors (January-June 2025)



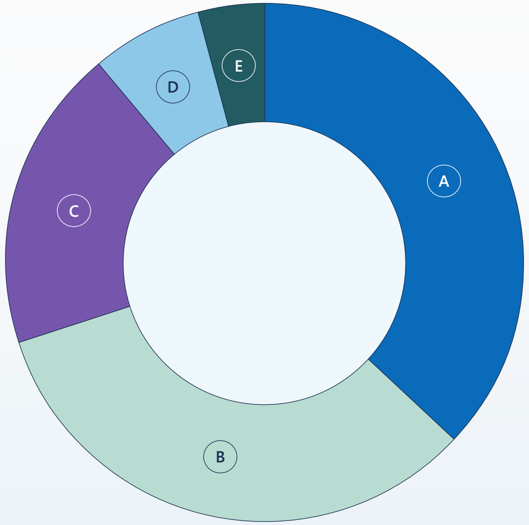
	%
A. Government agencies and services	17
B. Information technology	17
C. Research and academia	11
D. Non-governmental organizations	8
E. Critical manufacturing	6
F. Transportation systems	6
G. Consumer retail	6
H. Communications infrastructure	5
I. Financial services	4
J. Healthcare and public health	4

Source: Microsoft Threat Intelligence

Most attacks are for money

The vast majority of attacks are conducted by cybercriminals, not nation-state threat actors. 33% of the incidents DART investigated this year involved extortion, compared to only 4% motivated by espionage. Ransomware or destructive activity was noted in 19% of incidents. Notably, 7% of organizations were impacted by infrastructure building. This means threat actors might be taking advantage of organizations' unmanaged digital assets to stage attacks against other third-party targets downstream.

Identified motivations in incident response engagements



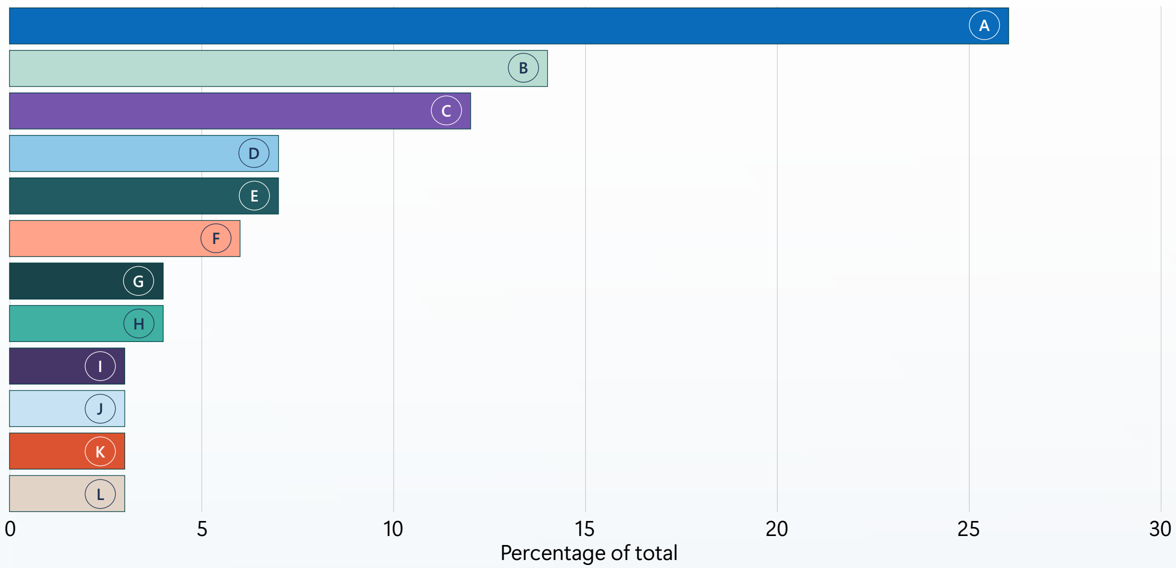
	%
A. Data theft	37
B. Extortion	33
C. Destruction/human-operated ransomware	19
D. Infrastructure building	7
E. Espionage	4

Source: Microsoft Incident Response, Detection and Response Team

Nation-state actors are expanding their operations, but are still espionage focused

Nation-states have expanded their targeting both by volume and geographic reach, with most activity focused on using cyber espionage to complement traditional intelligence operations.

Most-targeted sectors by nation-state actors



	% of total
A. IT	26
B. Research and academia	14
C. Government	12
D. Think tanks/NGOs	7
E. Consumer retail	7
F. Manufacturing	6

	% of total
G. Transportation	4
H. Communications	4
I. Finance	3
J. Health	3
K. Defense	3
L. Energy	3

Source: Microsoft Threat Intelligence nation-state notification data

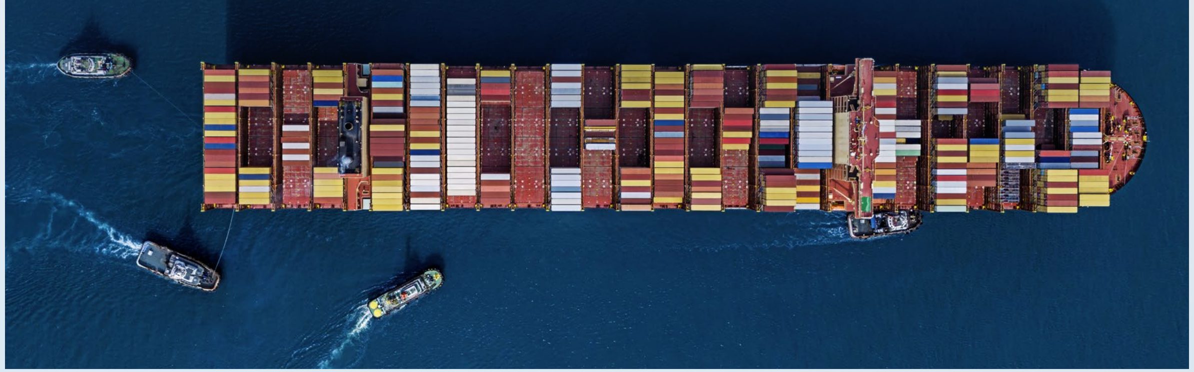
A ransomware attack with potential global impact stopped in under two minutes

In February 2025, the global economy narrowly averted catastrophe after a global shipping company experienced a ransomware attack. Had the company's systems been taken offline for even a few hours, the cascading effect would have impacted trade and industry around the world. Prolonged downtime would have ground maritime commerce to a crawl.

The attack epitomizes the risk of our interconnected world: a ransomware attack against just one private company can have global implications. Supply chains—both physical and digital—increase our attack surface, and organizations and industries halfway around the world can feel the knock-on effects of a single successful compromise. Malicious cyberactivity is not just a problem for individual victims to handle, but a whole-of-society problem.

As daunting as today's cyber threat landscape feels, this is a success story—proof that investing in cybersecurity pays off. Because the shipping company committed to protecting its digital assets, the attack was quickly stopped. **The time from observation to disruption was a mere 14 minutes, with encryption stopped one minute and eight seconds after it began.**

If the right protections are enabled, ransomware attacks can be contained at the onset of the attack, with no encryption at all.



Nation-state highlights

China

China is continuing its broad push across industries to conduct espionage and steal sensitive data. State-affiliated actors are increasingly relying on partnerships with non-governmental organizations (NGOs) to expand their capabilities and are using covert networks and vulnerable internet-facing devices to gain entry and avoid detection. They have also become faster at operationalizing newly disclosed vulnerabilities.

Top three sectors most targeted by Chinese threat actors (% of total): IT (23%), Government (10%), Think tanks/NGO (9%), Manufacturing (9%)

Top three regions most targeted by Chinese threat actors (% of total): United States (35%), Thailand (14%), Taiwan (12%)

Russia

Russia remains focused on Ukraine but has broadened its targets to small businesses in countries supporting Ukraine, possibly using them pivot points to reach larger organizations. Outside Ukraine, the top ten affected nations are all NATO members—a 25% increase from last year. Russian actors are also increasingly tapping into the cybercriminal ecosystem.

Top three sectors most targeted by Russian threat actors (% of total): Government (25%), Research and academia (13%), Think tank/NGOs (13%)

Top three regions most targeted by Russian threat actors (% of total): United States (20%), United Kingdom (12%), Ukraine (11%)

Iran

Iran is going after a wider range of targets than ever before, from the Middle East to North America, as part of broadening espionage operations. Recently, three Iranian state-affiliated actors attacked shipping and logistics firms in Europe and the Persian Gulf to gain ongoing access to sensitive commercial data, raising the possibility that Iran may be pre-positioning to have the ability to interfere with commercial shipping operations.

Top three sectors most targeted by Iranian threat actors (% of total): IT (21%), Research and academia (15%), Government (8%)

Top three regions most targeted by Iranian threat actors (% of total): Israel (64%), United States (6%), United Arab Emirates (5%)

North Korea

North Korea remains focused on revenue generation and espionage. In a trend that has gained significant attention, thousands of state-affiliated North Korean remote IT workers have applied for jobs with companies around the world, sending their salaries back to the government as remittances. When discovered, some of these workers have turned to extortion as another approach to bringing in money for the regime.

Top three sectors most targeted by North Korean threat actors (% of total): IT (33%), Research and academia (15%), Think tank/NGOs (8%)

Top three regions most targeted by North Korean threat actors (% of total): United States (50%), Italy (13%), Australia (5%)

Regional sample of nation-state activity levels observed

Observed event activity count per country

- 🟥 Over 200 events
- 🟪 100—200
- 🟦 50—100
- 🟦 0—50

Americas

Top activity levels	
United States	623
Canada	51
Brazil	24
Peru	16
Argentina	11
Colombia	10
Mexico	9
Dominican Republic	5
Chile	4
Costa Rica	3

Asia & Pacific

Top activity levels	
Taiwan	143
Korea	126
India	100
Hong Kong SAR	95
China	49
Australia	47
Thailand	39
Japan	38
Singapore	33
Indonesia	32

Europe

Top activity levels	
Ukraine	277
United Kingdom	144
Poland	97
Germany	74
France	72
Spain	61
Russia	60
Italy	51
Azerbaijan	35
Belgium	30

Middle East & Africa

Top activity levels			
Israel	603	Kenya	9
United Arab Emirates	166	Nigeria	8
Saudi Arabia	70	Tanzania	5
Türkiye	70	Mali	4
Iraq	67	Namibia	4
Jordan	44	Botswana	2
Lebanon	39		
Egypt	32		
Iran	27		
Morocco	26		
South Africa	31		
Ethiopia	20		
Angola	9		

AI: Both a solution and vulnerability

As adversaries begin to leverage the capabilities of AI, so too must defenders. While AI is still new, its impact is already significant: thanks to AI-based protections, providers report automatically neutralizing the vast majority of identity attacks. With the assistance of AI, security teams can remediate threats before they cause damage, with minimal false alarms or missed detections, making defenses both faster and smarter.

AI's defensive applications are broad: it can be used to conduct threat analytics, identify detection gaps and vulnerabilities, validate detections, identify homoglyph phishing, automate remediation and patching, and shield vulnerable users. AI agents, specifically, can help in threat mitigation and incident response by automatically responding to threats—for example by suspending suspicious accounts and initiating a password reset, containing a breach before an attacker can conduct further malicious activities. Agents can also enforce policies, monitor credentials and app permissions and behaviors, and control employee accesses.

AI use, however, comes with vulnerabilities and risks. These include both threats to AI systems and their users and threats enabled by AI.

Threats from AI cyberattack augmentation

Malicious use of AI has always been inevitable, but for the first time, we're witnessing adversaries deploy generative AI to enhance a broad spectrum of activities, including scaling social engineering, data analysis, and even real-time evasion of security controls. Autonomous malware and AI-powered agents are now capable of adapting their tactics in real life, challenging defenders to move beyond static detection and embrace behavior-based, anticipatory defense.

In the past six months, AI in influence operations has picked up aggressively. In addition, we've seen the emergence of AI-first actors—including nation-state entities—that prioritize AI-generated content and tools over traditional methods and manipulations.

*

In this AI-first era, defending AI with AI is not just a security necessity —it's a strategic advantage.

Storm-2139: A tale of AI exploit and abuse

Microsoft and global AI providers are advancing innovation while upholding core principles. The Digital Crimes Unit (DCU) action against Storm-2139 shows how public-private collaboration can shape responsible AI and disrupt cybercriminal abuse.

In July 2024, Microsoft uncovered a global network exploiting stolen API keys to bypass AI safety measures of various popular AI services, including Azure OpenAI. The developers were using and selling their nefarious tools, which were used to create thousands of abusive AI-generated images including celebrity deepfakes, sexually explicit imagery, and misogynistic, violent, or hateful synthetic content. By using content provenance tools and open-source intelligence, DCU was able to trace the origins of this malicious behavior. The network we uncovered included creators who developed software designed to bypass AI safety measures and generate offensive and harmful content, providers who customized and distributed the software, and end users who deployed these tools to create synthetic content.

To disrupt the network, the DCU implemented a two-phase approach. In December 2024, the DCU filed a civil complaint to seize and sinkhole the primary domain used by Storm-2139 to communicate and collaborate. This action allowed the DCU to uncover additional evidence, leading to an amended complaint in February 2025 that named the key developers and providers behind the tools. In March 2025, Microsoft provided extensive criminal referrals to the US Department Justice (DOJ), Federal Bureau of Investigation (FBI), UK's National Crime Agency (NCA), and Europol's European Crime Center (EC3).

Lessons from this operation for Policymakers:

- AI abuse is real and global
- Generative AI is being weaponized—governments must act now through regulations.
- Legal disruption works
- Civil litigation can effectively dismantle cybercriminal infrastructure.
- Cross-border collaboration is vital
- International referrals show the need for joint task forces and shared intelligence.
- Provenance and open-source intelligence (OSINT) matter
- Tracing AI-generated abuse requires investment in detection and attribution tools.
- Policy must cover the full abuse chain
- From developers to users—regulate creation, distribution, and use of malicious AI tools.
- Public-private partnerships are essential
- Coordinated efforts between industry and government are key to tackling AI threats.

The DCU's work with international law enforcement and others shows how private sector expertise can enhance public sector enforcement. Governments should formalize and expand these partnerships, especially in emerging areas like AI abuse and synthetic media.

Strengthening global cyber resilience through regulation and collaboration

In a world where breaches are a matter of when, not if, resilience and recovery are of paramount importance. As digital systems increasingly interface with bureaucratic, governmental, and critical infrastructure systems, both nationally and internationally, resilience also means ensuring societal functions can be maintained in the face of disruption.

Resilience requires a holistic approach: protecting infrastructure, managing crises regardless of their cause and origin, and ensuring continuity across business, governmental, and societal domains.

Resilience must be established at multiple levels, including national and international, to align capabilities, share intelligence, and coordinate responses. Only through integrated and proactive collaboration can we build systems that are not only secure but also capable of adapting, absorbing shocks, and continuing to deliver essential services.

Governments around the world are moving quickly to enact new policies, laws, and regulations to help mitigate cyber risk and promote resilience. In the last year, three major themes have emerged in government priorities: regulatory expansion and enforcement, supply chain security, and evolving international cooperation.

1. **Regulatory expansion and enforcement:** Governments have advanced and/or implemented comprehensive cybersecurity regulations that emphasize accountability, risk management, and timely incident reporting. These regulations often include mandatory compliance measures, governance requirements, and oversight mechanisms, continuing a trend of shifting from voluntary guidelines to enforceable standards.
2. **Securing the digital supply chain:** Governments also focused on driving cybersecurity requirements to improve supply chain security across the lifecycle of digital technologies. New regulations are mandating secure-by-design principles, transparency through software bills of materials (SBOMs), and robust post-market monitoring.
3. **Evolving international regulatory cooperation:** Where countries once relied primarily on ad hoc partnerships and information sharing, the first instance of a formal mutual recognition of cybersecurity requirements advanced during the last year. This evolution reflects a growing recognition that cyber threats transcend borders and require harmonized responses.

At the same time, while these actions can improve cyber defenses, they may also lead to inconsistent requirements across jurisdictions, increasing complexity and costs while actually reducing security. With this in mind, governments seeking to reduce cyber risk and encourage resiliency should focus on standards setting and rulemaking that promotes iterative learning and global interoperability alongside strong accountability. Furthermore, they should use iterative approaches to regulations that are risk-based and outcome- or process-oriented.

Advancing multistakeholder efforts for peace and security online

Rising cyber conflict has sparked global cooperation, with countries engaging through the United Nations (UN) and other forums to build and uphold a shared rules-based framework for responsible behavior online. The success of these government-led dialogues also requires the participation of key nongovernmental partners from industry and civil society to share technological insights and to underscore the risk and human impact of offensive nation-state cyber operations.

Unlike traditional domains of interstate conflict and cooperation – such as arms control or maritime law – cyberspace is largely owned, operated, and innovated by the private sector. It is also constantly evolving. Effective international frameworks for peace and stability online must reflect this reality by ensuring that those who build and maintain cyberspace can inform discussions around responsible state behavior online. This past summer marked the end of the UN's Open Ended Working Group on cybersecurity (OEWG), and there is a critical opportunity now to reimagine participation models for the next generation of cybersecurity dialogues that are as dynamic as the domain they aim to govern. To this end, Microsoft believes it is important to:

Establish a permanent, more action-oriented, cybersecurity mechanism at the UN: Successive UN working groups have provided a forum for dialogue on responsible state behavior in cyberspace for over two decades, but future progress requires a more agile and enduring framework within the UN that does not rely on the consensus of every UN member state before it can issue guidance. A mechanism anchored in clear norms, technical expertise, and which meaningfully includes non-governmental stakeholders to ensure practical and beneficial outcomes.

Build on existing rules and expand as needed: Efforts like the International Criminal Court's draft policy on cyber-enabled crimes and the Digital Emblem of the Red Cross show that existing mandates of international law already apply in digital contexts. But ensuring they are applied depends largely on political will, institutional clarity, and operational capacity. Similarly, the 11 UN norms for responsible state behavior online provide important baseline guardrails that must be applied and upheld. While their implementation remains crucial, additional norms should be continuously explored and developed to keep pace with a constantly changing digital domain.

Things like commercial cloud services have become so important to daily life that they should be recognized as international critical infrastructure and off-limits to targeting by nation state cyber operations.

Institutionalize multistakeholder dialogue on AI, security, and ethics: The Roundtable for AI Security and Ethics (RAISE), led by UNIDIR with support from Microsoft and other partners, is an ongoing workshop series that highlights the value of sustained, cross-sector dialogue on AI risks in security contexts. UN bodies could replicate and support such initiatives to align technical capabilities with policy development and promote responsible innovation through inclusive collaboration.

Deterrence in action: Building consequences for nation-state actors

As infrastructure essential to daily life—including water, food, healthcare, communications, and transportation systems—becomes increasingly dependent on digital technology, nation-state cyber operations targeting these systems cannot be permissible; in particular those prepositioning for disruptive or destructive cyberattacks in case of future conflicts.

Defensive actions alone to protect critical infrastructure are unlikely to deter nation-state adversaries. These are politically motivated activities that must be addressed with political solutions as well. To protect critical infrastructure, political institutions, and civilian systems, governments must build frameworks that signal credible and proportionate consequences for malicious activity that violate international rules.

Over the past year, there has been a marked increase in recognition of the need for such cyber deterrence, with governments and industry aligning more closely to response to malicious activity. For example:

- **NATO** has advanced coalition-based attribution frameworks and is exploring collective countermeasures in response to cyberattacks. In July, the alliance released a statement recognizing and condemning malicious cyber activities attributed to Russia by member states.
- The **US** administration has issued strong public statements and indictments tied to cyber operations and has publicly attributed cyberattacks in coordination with allies and partners.
- The **EU** is increasingly leveraging its Cyber Diplomacy Toolbox and sanctions regime to hold bad actors accountable, though implementation remains uneven.

Looking ahead, these are important foundations to build upon. To further strengthen a cyber deterrence framework, like-minded governments should work to:

- **Regularize public attributions.** States should more consistently issue public attribution statements, leveraging insights from other governments and partners in the private sector and establishing a more uniform process for doing so. Such statements should always indicate if international laws or norms were violated during a cyber incident.
- **Signal red lines**. States should make clear they will impose increasingly severe consequences in response to a spectrum of malicious nation-state cyber activity, ranging from espionage to prepositioning to disruptive and/or destructive cyber operations.
- **Impose diverse consequences**. Responses to nation-state cyberattacks should not be constrained to the cyber domain or prescribed in a one-size-fits-all model. Different threat actors will be deterred by different consequences. These could include economic measures, diplomatic sanctions, naming and shaming, posturing, or targeted declassification.
- **Prohibit private sector retaliations.** Private companies are not in the position to independently hack back against malicious nation-state actors, and doing so can risk unintended escalation and harm. While industry can support attributions and partner with government to take action, imposing consequences for internationally wrongful behavior by states will always need to be led by governments.

A viable model for cyber deterrence is a necessity for the stability of the online world and will require innovations in statecraft and diplomacy in the years ahead. This is why Microsoft is supporting ongoing research by the Royal United Services Institute (RUSI) to explore novel approaches to deterring malicious activity online.

Addressing the geopolitical enablers of ransomware operations

Many of the most prolific ransomware groups avoid consequences by targeting victims in other countries while their own governments turn a blind eye.

Whether they are state-affiliated groups or their government simply ignores their activity, the result is the existence of "safe haven" states that enable ransomware attacks abroad and violate international norms of due diligence which oblige governments to take action to prevent illegal cyber activity within their borders.

As a result, addressing ransomware operations requires a more coordinated international effort and political pressure that holds governments accountable for both direct and indirect support of ransomware attacks. Designating state sponsors of ransomware, for example, similar to state sponsors of terror, with associated stigmas and penalties, is one way to incentivize states to confront ransomware groups operating within their borders.

Other approaches to address escalating ransomware include:

- **Legal action:** Ransomware is a form of extortion which, in most cases, violates existing laws. These should be applied whenever possible. By designating state sponsors of ransomware, civilians might be able to take further legal action against those governments following ransomware attacks to seek damages in civil courts.
- **Public-private partnerships:** Encourage industry partnerships with law enforcement to improve cooperation against cybercrime. Examples include the International Counter Ransomware Initiative (CRI) and the Institute for Security and Technology (IST) Ransomware Task Force.
- **Deterrent consequences:** Governments should set clear expectations around what is responsible state behavior, reinforced by escalating consequences across domains sufficient to deter state-sponsored, or enabled, ransomware attacks.

Combating cyber mercenaries: Closing the gaps in global regulation

Cyber mercenaries, private firms that sell offensive cyber capabilities, operate in legal gray zones, often across borders. Their cross-jurisdictional nature and a lack of oversight make them difficult to trace or prosecute, allowing them to act with near impunity. Many also rebrand frequently, shift operations across jurisdictions, and use complex financial networks to further evade detection and regulation.

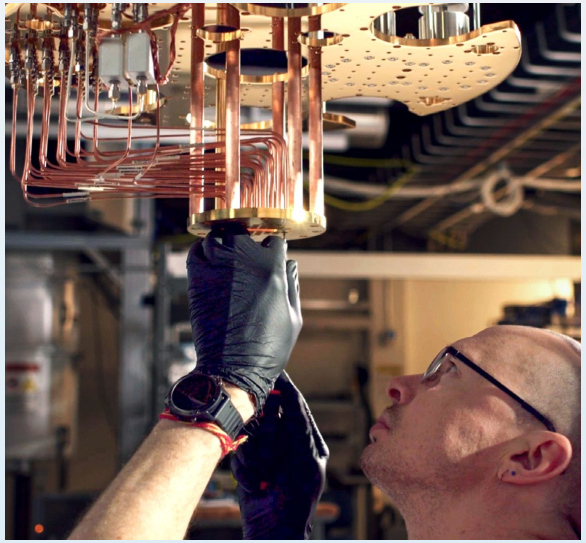
To counter this growing threat, governments and industry must collaborate further to disrupt the enabling market through intelligence sharing, coordinated responses, and regulation. International norms should also prohibit the use of cyber mercenaries and close legal loopholes that allow them to persist. Governments need to put in place severe limitations—or outright bans—on the cyber mercenary market to ensure their products, including spyware, cannot be used in violation of domestic or international law, human rights, or to significantly undermine product security.

Examples already exist of states taking effective action. The US has placed restrictions on when federal agencies can solicit the services of cyber mercenaries and banned firms that operate irresponsibly, meaningfully impacting the bottom lines of some cyber mercenary firms. Meanwhile, the UK and France have made strides over the past year in their stewardship of the Pall Mall Process, an international multistakeholder dialogue that includes more than 20 government participants and which seeks to regulate Commercial Cyber Intrusion Capabilities (CCIC) with shared frameworks. In April 2025, the Pall Mall Process produced a first-of-its-kind Code of Practice for governments to follow in order to limit harmful impacts of CCICs.

Transparency is key. Governments should expose vendors and intermediaries, enforce sanctions, and lead by example by refraining from using cyber mercenaries themselves. Meanwhile, industry must enhance platform security, monitor abuse, and act swiftly to disrupt cyber mercenary operations. Through due diligence and collaboration, both sectors can help shrink the space in which cyber mercenaries operate—protecting national security, human rights, and global digital stability.

Quantum technologies: Strategic priority in a new era of competition

Quantum technologies—computing, communications, and sensing—are foundational to future economic and national security.



Quantum technologies' potential to accelerate scientific discovery, enable breakthroughs in secure communications, and disrupt encryption have made this technology a high-priority area. Indeed, governments have identified quantum technology as a national imperative. Allies and adversaries alike are pursuing quantum capabilities through new national research and development (R&D) programs, as well as investments to cultivate their own academic and private sector ecosystems.

Commercial companies are driving a significant amount of current quantum R&D and private enterprise now sits at the epicenter of the global race to develop quantum technologies. Some adversaries might also leverage including the possible targeting of corporate R&D programs, startups, and academic spin-offs. It is therefore imperative to establish robust safeguards and strategic preparedness now, before quantum technology becomes widely operational. The stakes are hard to overstate: leadership in quantum could determine not just competitive advantage but the future integrity of secure communications and the global digital economy.

The implications of the race to quantum advantage are sweeping:

- **Industrial scientific leadership:** Quantum technologies could drive a new wave of innovation across chemistry and material science.
- **Impact to cryptography:** A sufficiently powerful quantum computer could break widely used public key algorithms, undermining the security of digital communications and data.
- **Sensor superiority:** Quantum sensors could detect stealth air or naval assets, eroding strategic deterrence recommendations

Governments play a critical role in enabling a quantum-safe future through strong collaboration with industry and effective policies. To accelerate readiness, we recommend governments take the following actions:

- **Establish quantum safety as a national cybersecurity priority.** Position quantum-safe cryptography as a strategic imperative and embed it into national cybersecurity frameworks.
- **Align quantum-safe strategies across jurisdictions.** Harmonize public policies, standards, and transition timelines. The G7 should lead by expanding its financial sector post-quantum cryptography workstream to align G7 members' broader quantum-safe strategies.
- **Adopt international standards.** Support global standards development and avoid fragmented, region-specific approaches that hinder interoperability, innovation, and security.
- **Set early and progressive timelines.** Drive action well before 2030. For instance, the US Committee on National Security Systems Policy 15 (CNSSP -15) mandates quantum-safe algorithms in all new products and services for national security systems by January 2027.
- **Lead by example with transparent transition plans.** Publish and regularly update government transition roadmaps—including timelines, milestones, and budgets—to foster knowledge sharing and best practices.
- **Raise awareness and build workforce capacity.** Educate the public and critical infrastructure sectors on quantum risks and readiness. Invest in skilling programs to equip the workforce for a quantum safe transition.
- **Modernize through cloud adoption.** Promote cloud migration as a strategic enabler. Cloud platforms can streamline the transition by embedding quantum-safe capabilities, reducing the burden on individual organizations.

Closing

As global regulatory frameworks evolve and legislative trends reshape the cybersecurity landscape, one truth remains constant: security is a shared responsibility.

Governments, industry leaders, civil society, and individual users each play a vital role in shaping a resilient digital ecosystem. The insights and data presented throughout this report underscore the urgency of collaboration—not only across borders but across sectors and disciplines.

Our commitment to lighting the path to a secure future is more than a campaign theme—it is a call to action. We believe that transparency, interoperability, and harmonized standards are foundational to progress. Whether through our threat intelligence, policy advocacy, or engineering innovations, we aim to empower defenders and decision-makers alike.

Thank you for reading this year's Microsoft Digital Defense Report. We invite you to explore our companion resources, share your feedback, and join us in building a secure, more trustworthy digital world.

Microsoft

Microsoft Digital Defense Report 2025

Lighting the path to a secure future

For more news on cybersecurity, visit:
microsoft.com/corporate-responsibility/cybersecurity

For more report insights, visit:
microsoft.com/mddr

For more news on cybersecurity policy, follow us on LinkedIn:
aka.ms/MOILinkedin

For insights and trends for security leaders, visit:
www.microsoft.com/security/security-insider

A Microsoft Threat Intelligence report
October 2025