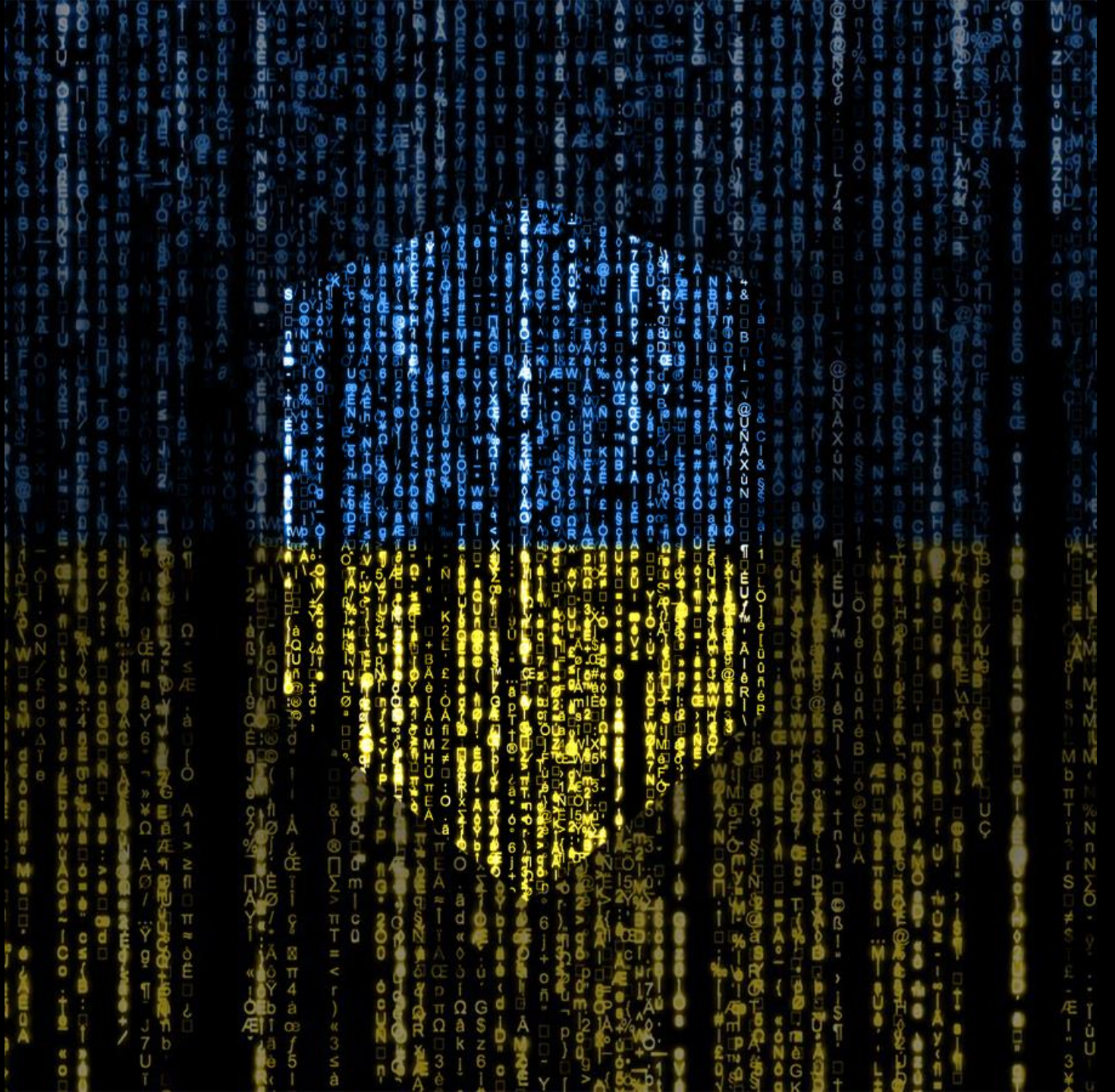
Cybersecurity

In a changing world



Microsoft

Sandra Barouta Elvin

National Security Officer for Microsoft Sweden since April 2020

- Spokesperson for security, compliance and data protection
- Government Security Program

Chairwoman for American Chamber of Commerce Security Working Committee in Sweden

20+ years in Information and IT Security.

5 years in Public Sector.

500+ C-level meetings on cyber security and risk management.

9 major cyber attacks managed.

1999
Software AG
Pre-sales consultant and XML developer

2002
Sundbybergs Stad
Support & System Team Manager +Information Security Responsible

2006
Nexus Technology
Information Security Consultant, Forensic Lead

2007
Ericsson
Head of Enterprise IT Infrastructure and various other roles

2017
H&M
Head of IT Security & IT Risk Management

Microsoft Security – how it started

Gates
sday, January 15, 2002 5:22
soft and Subsidiaries: All FTE
Trustworthy computing

ew years I have sent out a memo talking about the highest
rosoft. Two years ago, it was the kickoff of our .NET strate
was several memos about the importance of the Internet t
and the ways we could make the Internet truly useful for p
the last year it has become clear that ensuring .NET is a p
tworthy Computing is more important than any other part o
don't do this, people simply won't be willing -- or able -- to t
vantage of all the other great work we do. Trustworthy Com
ghest priority for all the work we are doing. We must lead th
hole new level of Trustworthiness in computing.

When we started work on Microsoft .NET more than two ye
a new direction for the company -- and articulated a new w
our software. Rather than developing standalone applicati
re moving towards smart clients with rich
ices. We're driving the XML We
dors can share in
or for

Government Security Program

The GSP is designed to provide participants with the confidential security information and resources they need to trust Microsoft's products and services.

Our purpose is to help governments protect themselves and their citizens by:

Enabling trust & transparency

Providing Access to security information about Microsoft products and services

Providing data to improve protection of government information technology against cyber threats

Fostering collaboration between Microsoft security teams and government cybersecurity experts

Microsoft security today

Our expansive, global reach and AI-driven security tools give us insight into key trends in cybersecurity that affect everyone from individuals to nations.

78T

Trillion security signals per day inform our insights

34K

Full-time dedicated security engineers

15K

Partners with specialized security expertise

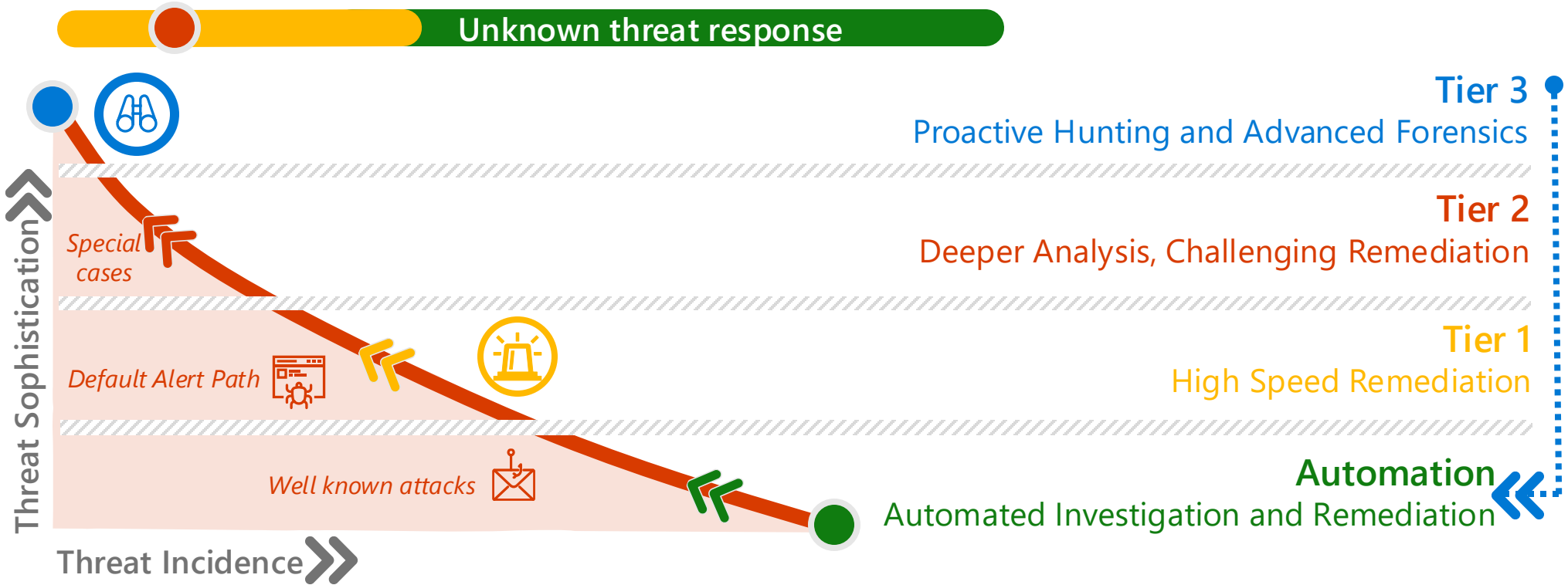
Why TI & threat hunting?

Traditional cybersecurity is *reactive*

SOCs can be classified into a three-tier model when it comes to addressing unknown threats. Most organizations' responses operates in reactive tiers - automation, tier 1, and tier 2.

Threat Hunting is *proactive*

Threat hunting allows organizations to *proactively* mitigate threats. Analysts leverage specialized data and platforms to hunt a threat in totality. This process enriches lower response tiers, while reducing future incidents and breaches[1].



Digitalization complicating security operations

IT Security

- Protecting information technology
- Focusing on technical security

Malware

Network intrusion

Unauthorized system access

Phishing

DoS/DDoS

Digital security

- Protecting against digital threats
- Focusing on securing digital information and processes

Cybercrime/ fraud

Data breach

Identity theft

Privacy breach

Cyber espionage

Disinformation

Microsoft Threat Intelligence collaboration

MICROSOFT THREAT ANALYSIS CENTER (MTAC)

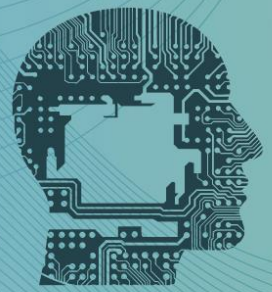
Influence operation (IO) detection and analysis

•

Cyber-enabled IO

Cyber threat intelligence & cyber-enabled IO detection

MICROSOFT THREAT INTELLIGENCE CENTER (MSTIC)



AI and data science applied to influence operation analysis and assessment

AI FOR GOOD LAB (AI4G)

The new cyber threat landscape

- Increased sophistication of attacks
- Blurring lines between nation-state and cybercriminal activity
- Growing impact of AI on both attack and defense

Our presence in the digital ecosystem positions us to observe key trends in cybersecurity. Microsoft's perspectives on cybersecurity are framed through **50 years of experience and insight.**

Society | Microsoft stakeholders | Microsoft Customers

Microsoft's unique vantage point

Billions of customers globally, from a broad and diverse spectrum of organizations, and consumers.

78 trillion security signals per day

1,500 unique threat groups tracked

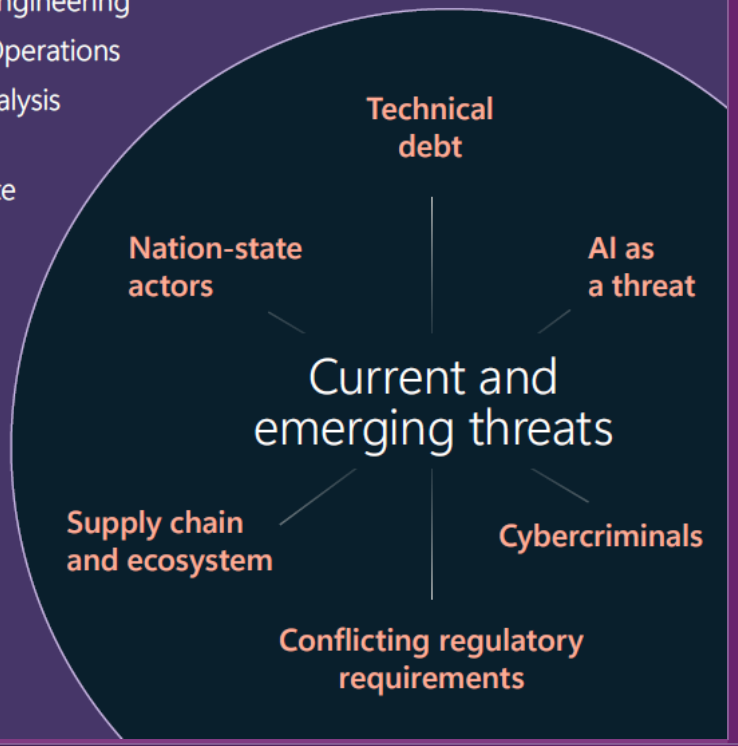
Microsoft's cybersecurity approach

Microsoft security investments

- AI Red Teams
- Defending Democracy
- Detection and Response
- Digital Crimes
- Digital Safety
- Incident Response
- National Security
- Physical Security
- Public Awareness and Education
- Responsible AI
- Security Engineering
- Security Operations
- Threat Analysis
- Threat Intelligence

34,000 dedicated security engineers

focused full-time on the largest cybersecurity engineering project in the history of digital technology.



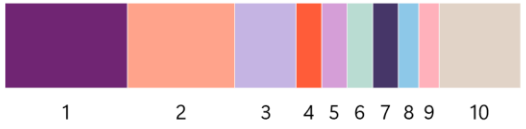
The evolving cyber threat landscape

- Blurred Lines Between Nation-States and Cybercrime
- International Law and Influence Operations
- Election Influence Operations
- Escalating cyber aggression
- AI-Enhanced Threats
- Hybrid Warfare and Cyberattacks
- Global AI Security Partnerships
- AI for Defense

Threat actors and motivations

- Nation-state threat actors are increasingly engaging in financially motivated cyber operations, blurring the lines between nation-state activity and cybercrime. This includes utilizing ransomware, offering stolen data for profit, and potentially collaborating with cybercriminal groups.
- Top Targeted Sectors Worldwide: IT (24%) Education & Research (21%) Government (12%)
- Emerging Techniques
- Education & Research: Increasingly targeted as testing grounds for advanced attacks, including QR code phishing.
- AI Threats: Nation-state actors are adopting AI tools for influence operations, making detection more challenging for defenders.

Top 10 targeted sectors worldwide



	Sector	Percentage
1	IT	24%
2	Education and Research	21%
3	Government	12%
4	Think tanks and NGOs	5%
5	Transportation	5%
6	Consumer Retail	5%
7	Finance	5%
8	Manufacturing	4%
9	Communications	4%
10	All others	16%

Threat actors from Russia, China, Iran, and North Korea pursued access to IT products and services, in part to conduct supply chain attacks against government and other sensitive organizations.

Source: Microsoft Threat Intelligence, nation-state notification data

Ransomware trends and insights

2.75x

Increase year over year in human-operated ransom-linked encounters

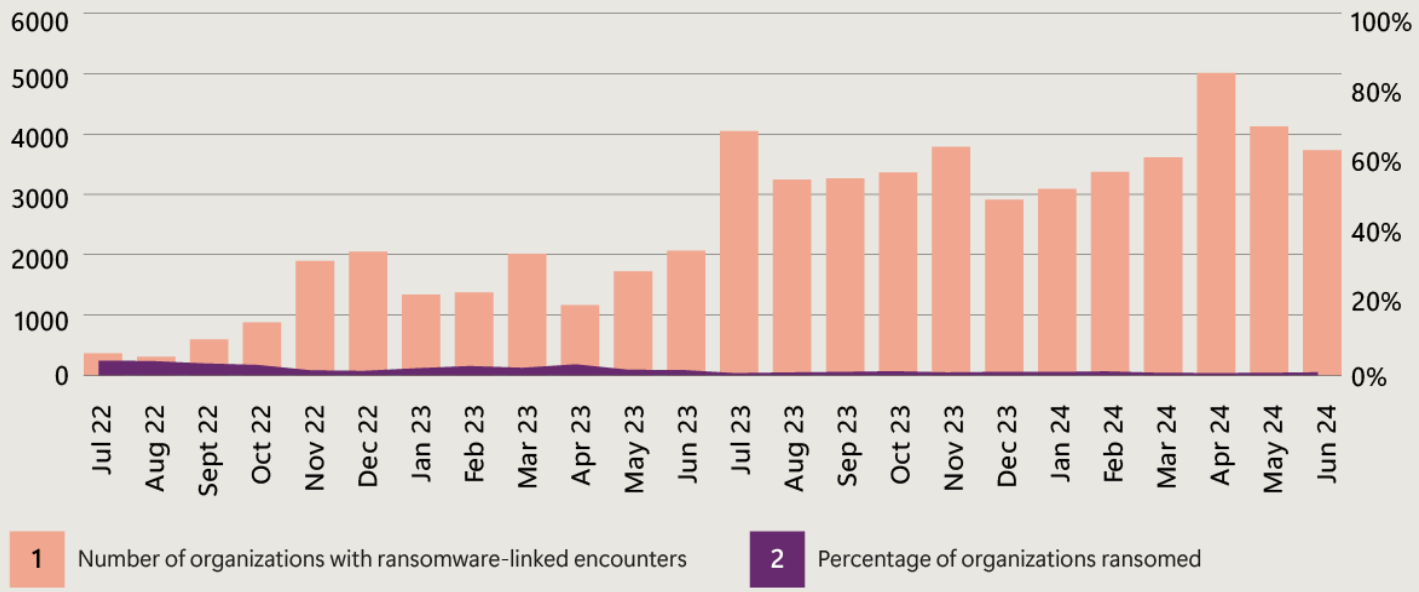
92%

Of successful ransom attacks leveraged an unmanaged device in the network

3x

Threefold decrease in ransom Attacks reaching encryption stage over the past two years

Organizations with ransom-linked encounters continues to increase while the percentage of those ransomed is decreasing (July 2022–June 2024)



Although organizations with ransom-linked encounters continues to increase, the percentage that are ultimately ransomed (reaching encryption stage) decreased more than threefold over the same time period.

Source: Microsoft Defender for Endpoint

Identity attacks in perspective

More than 99% of identity attacks are password attacks

Breach replay

Password spray

Phishing

Rely on predictable human behaviors such as selecting easy passwords, reusing them on multiple websites, and fall prey to phishing attacks

Password-based attacks continue to dominate, but can be thwarted by using strong authentication methods.

<1%

of attacks

MFA attacks

- SIM swapping
- MFA fatigue
- AitM

Post-authentication attacks

- Token theft
- Consent phishing

Infrastructure compromise

7,000

Password attacks per second

39,000

Token theft incidents per day

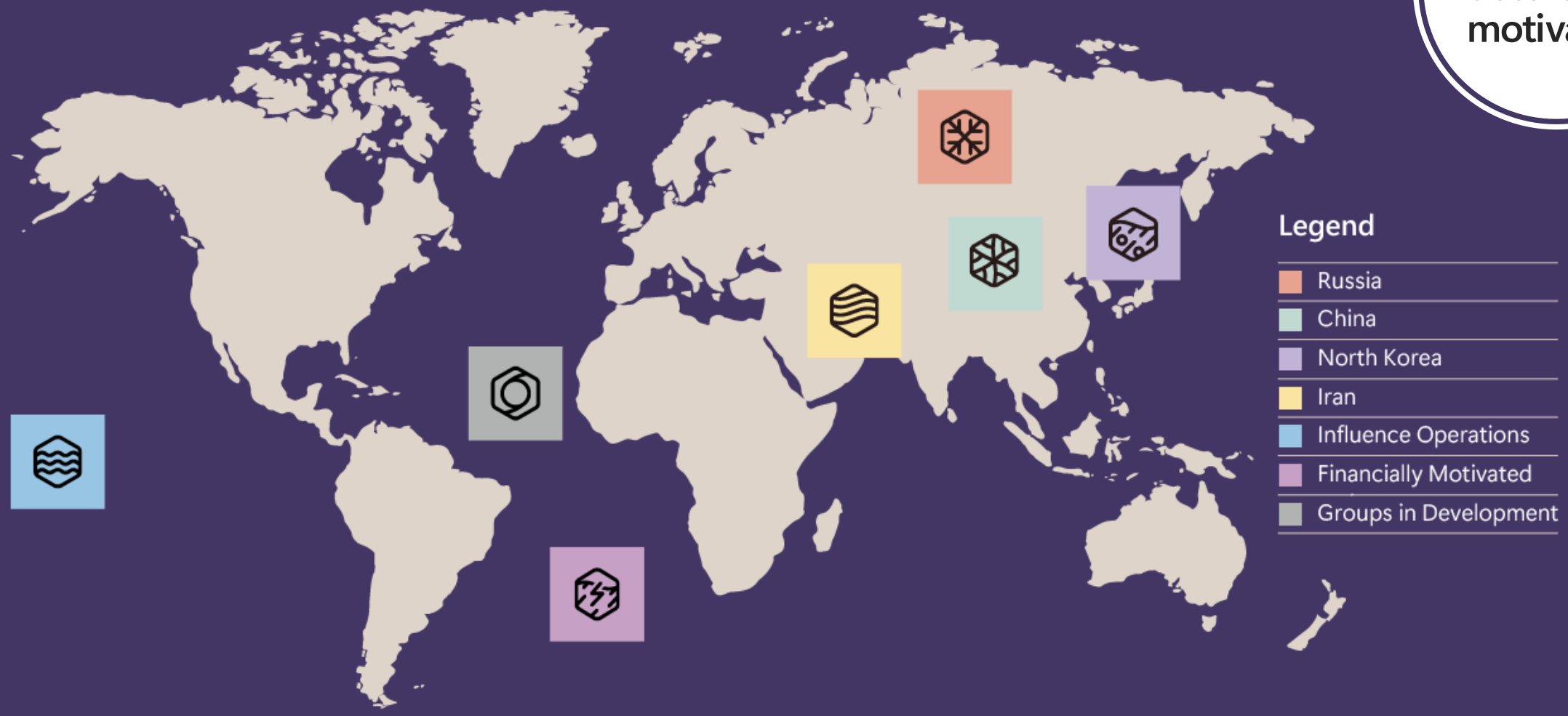
146%

Rise in AiTM phishing attacks

Source: Microsoft Threat Intelligence

Monitoring more than 600 nation-state groups

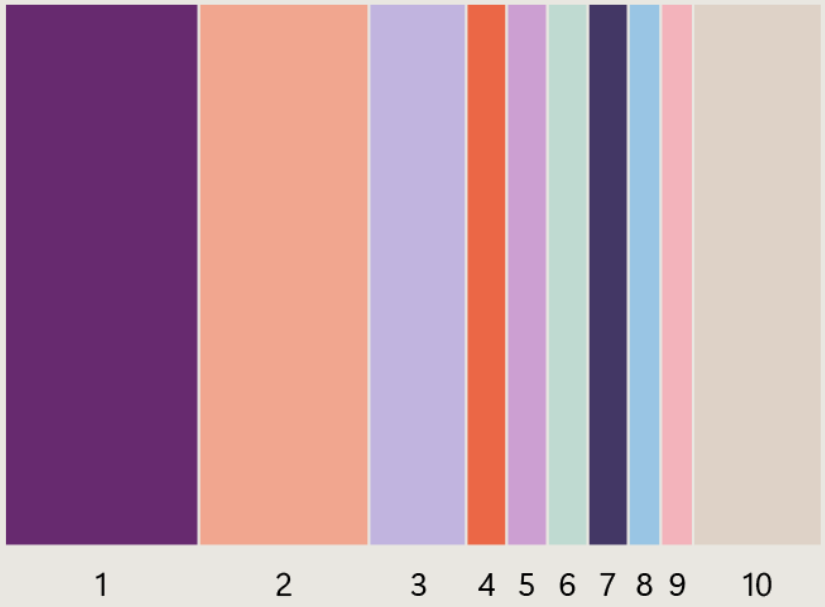
Threat actors and motivation



Nation-state threat activity by the numbers

- State-affiliated threat actors played a persistent supporting role in broader geopolitical conflicts.
- The Education and Research sector became the second most targeted by nation-state threat actors.

Top 10 targeted sectors worldwide



	Sector	Percentage
1	IT	24%
2	Education and Research	21%
3	Government	12%
4	Think tanks and NGOs	5%
5	Transportation	5%
6	Consumer Retail	5%
7	Finance	5%
8	Manufacturing	4%
9	Communications	4%
10	All others	16%

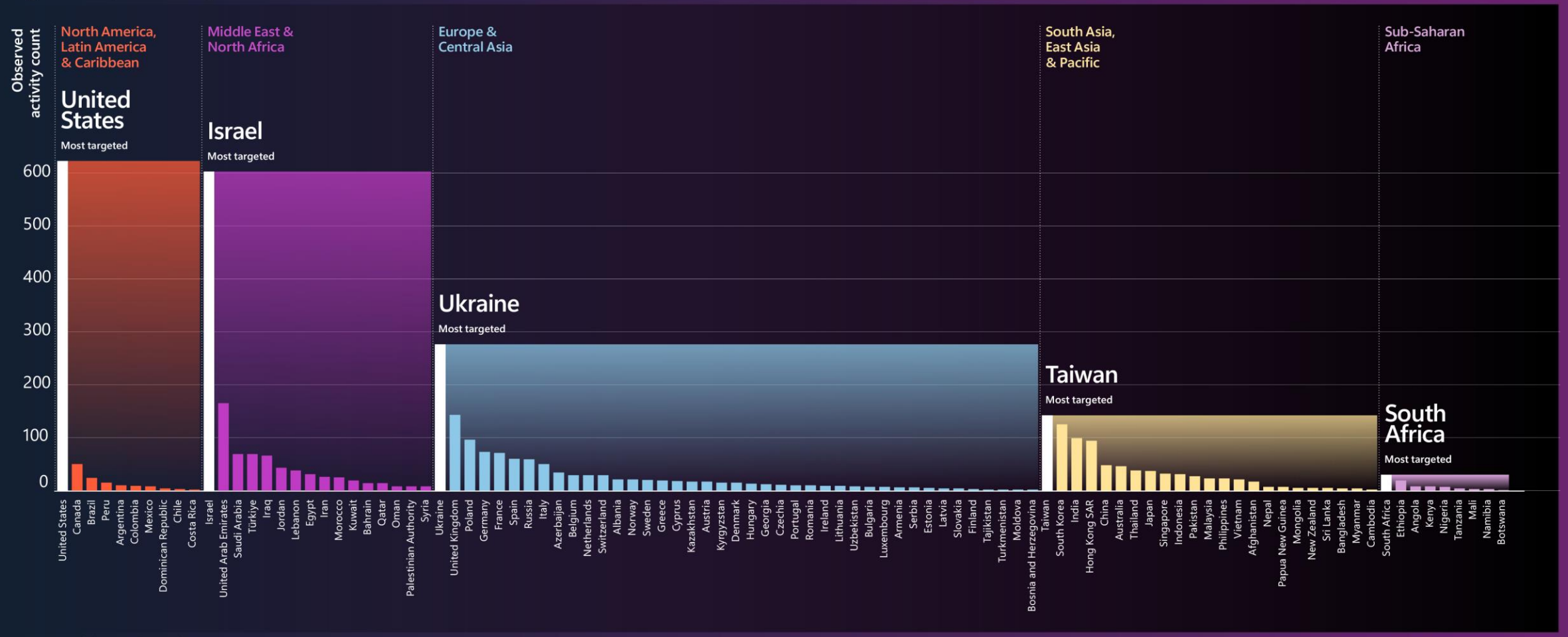
Threat actors from Russia, China, Iran, and North Korea pursued access to IT products and services, in part to conduct supply chain attacks against government and other sensitive organizations.

Source: Microsoft Threat Intelligence, nation-state notification data

Source: Microsoft Threat Intelligence

Nation-state threat actor targeting

Regional sample of activity levels observed



Source: Microsoft Threat Intelligence data

Nation-state threat activity by the numbers

Russia

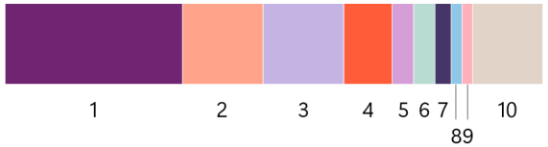
Nation-state threat actor activity

Targeting by region

	Sector	Percentage
1	Europe & Central Asia	68%
2	North America	20%
3	Middle East & North Africa	5%
4	East Asia & Pacific	3%
5	Latin America & Caribbean	3%
6	South Asia	1%
7	Sub-Saharan Africa	1%

Approximately 75% of targets were in Ukraine or a NATO member state, as Moscow seeks to collect intelligence on the West's policies on the war. Ukraine remains the country most targeted by Russian actors.

Most targeted sectors



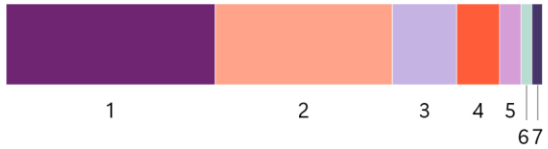
	Sector	Percentage
1	Government	33%
2	IT	15%
3	Think tanks and NGOs	15%
4	Education and Research	9%
5	Inter-governmental organization	4%
6	Defense Industry	4%
7	Transportation	3%
8	Energy	2%
9	Media	2%
10	All others	13%

Russian actors focused their targeting against European and North American government agencies and think tanks, likely for intelligence collection related to the war in Ukraine. Actors like Midnight Blizzard also targeted the IT sector, suggesting it was in part planning supply-chain attacks to gain access to these companies' client's networks for follow-on operations.

China

Nation-state threat actor activity

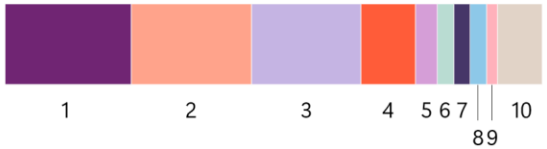
Targeting by region



	Sector	Percentage
1	East Asia & Pacific	39%
2	North America	33%
3	Europe & Central Asia	12%
4	Latin America & Caribbean	8%
5	South Asia	4%
6	Middle East & North Africa	2%
7	Sub-Saharan Africa	2%

Chinese threat actors' targeting efforts remain similar to the last few years in terms of geographies targeted and intensity of targeting per location. While numerous threat actors target the United States across a wide variety of sectors, targeting in Taiwan is largely limited to one threat actor, Flax Typhoon.

Most targeted sectors



	Sector	Percentage
1	IT	24%
2	Education and Research	22%
3	Government	20%
4	Think tanks and NGOs	10%
5	Manufacturing	4%
6	Defense Industry	3%
7	Communications	3%
8	Finance	3%
9	Transportation	2%
10	All others	9%

Most Chinese threat activity is for intelligence collection purposes and was especially prevalent in ASEAN countries around the South China Sea. Granite Typhoon and Raspberry Typhoon were the most active in the region, while Nylon Typhoon continued to target government and foreign affairs entities globally.

Source: Microsoft Threat Intelligence

Nation-state threat activity by the numbers

Iran

Nation-state threat actor activity

Targeting by region

	Sector	Percentage
1	Middle East & North Africa	53%
2	North America	23%
3	Europe & Central Asia	12%
4	South Asia	6%
5	East Asia & Pacific	3%
6	Latin America & Caribbean	2%
7	Sub-Saharan Africa	1%

Iran placed significant focus on Israel, especially after the outbreak of the Israel-Hamas war. Iranian actors continued to target the US and Gulf countries, including the UAE and Bahrain, in part because of their normalization of ties with Israel and Tehran's perception that they are both enabling Israel's war efforts.

Most targeted sectors

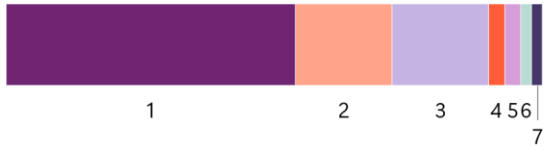
	Sector	Percentage
1	Education and Research	19%
2	IT	11%
3	Government	7%
4	Transportation	6%
5	Finance	4%
6	Communications	4%
7	Energy	3%
8	Commercial Facilities	3%
9	Manufacturing	3%
10	All others	42%

Iranian targeting focused on education, IT, and government as part of strategic intelligence collection. Iranian actors often target the IT sector to gain access to downstream customers, including those in government and the defense industrial base (DIB). "Other" includes media and think tanks or NGOs, which Iran often targets to gain insights into dissidents, activists, and persons who can impact policymaking.

North Korea

Nation-state threat actor activity

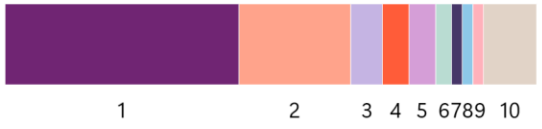
Targeting by region



	Sector	Percentage
1	North America	54%
2	East Asia & Pacific	18%
3	Europe & Central Asia	18%
4	Latin America & Caribbean	3%
5	Middle East & North Africa	3%
6	South Asia	2%
7	Sub-Saharan Africa	2%

The United States remained the most heavily targeted country by North Korean threat actors, but the United Kingdom rose up the ranks this year to second place. The "Other" category comprised 44 other countries targeted by North Korean threat actors.

Most targeted sectors



	Sector	Percentage
1	IT	44%
2	Education and Research	21%
3	Manufacturing	6%
4	Consumer Retail	5%
5	Finance	5%
6	Think tanks and NGOs	3%
7	Communications	2%
8	Government	2%
9	Health	2%
10	All others	10%

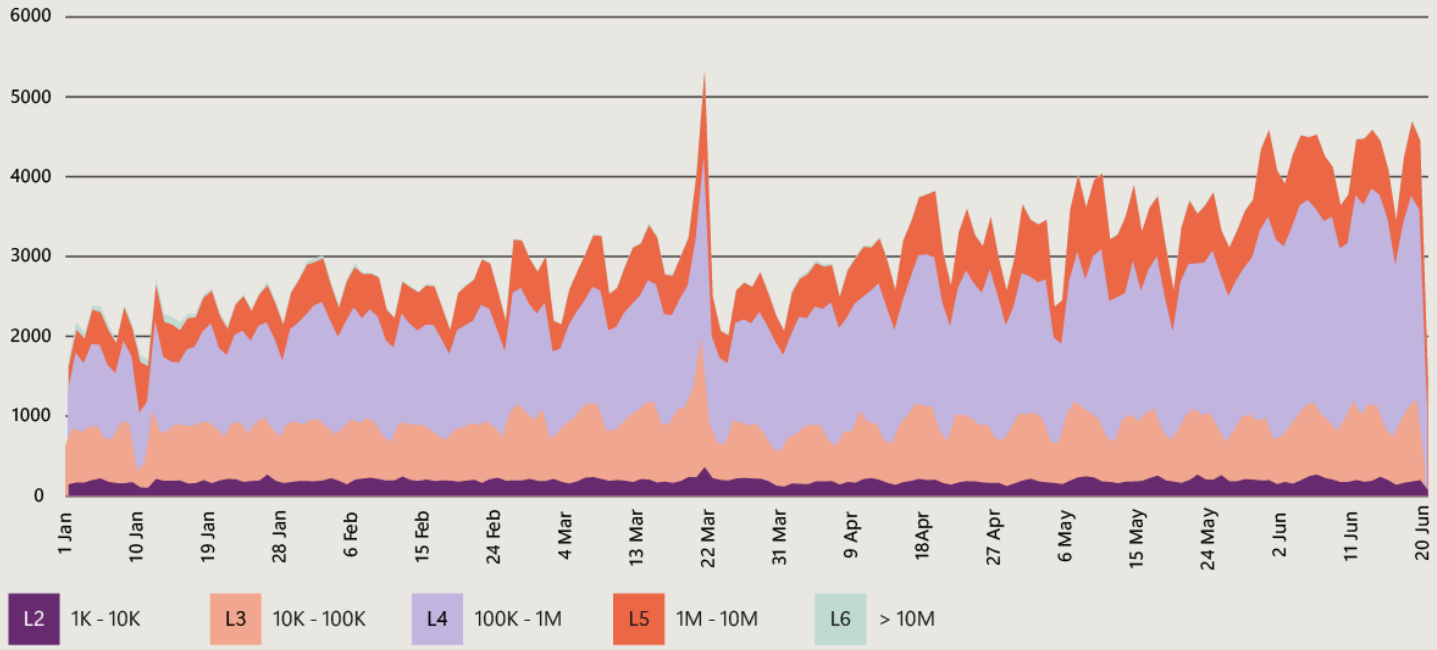
North Korean threat actors targeted the IT sector the most, particularly to conduct increasingly sophisticated software supply chain attacks. They also continued to heavily target experts in the education sector for intelligence collection. The "Other" category comprised seven other sectors.

Source: Microsoft Threat Intelligence

DDoS: Stealthier threats emerge

The increased focus of DDoS attacks on the application layer has created a greater risk of impact on business availability.

Number of network DDoS attacks (January-June 2024)



The number of DDoS attacks mitigated continues to increase, with a notable surge layer 4 (L4, application layer) attacks. Application layer attacks are more stealthy, sophisticated, and difficult to mitigate than network-level attacks. Layers in the key are in "packets per second (pps)".

Source: Microsoft Global DDoS Mitigation Operations

Microsoft Security

Threat landscape: Communications infrastructure sector

Q4 2024

Microsoft Threat Intelligence

Activity overview

Trends	Nation state threat actors	Tools and techniques	Financially motivated threats	Vulnerabilities	OSINT
Threat landscape for information technology sector in 2024	Storm-2372 Storm-1660 Storm-1830 Red Sandstorm Mint Sandstorm Zigzag Hail Sapphire Sleet Emerald Sleet Seashell Blizzard subgroup Forest Blizzard	FusionDrive GoldBackdoor Code injection attacks using publicly disclosed ASP.NET machine keys	IronSentry PhaaS Malvertising campaign leads to info stealers hosted on GitHub Phishing campaign impersonates Booking.com	CVE-2025-21419 CVE-2025-21420 CVE-2025-21391 CVE-2025-21333 CVE-2024-43583	Lumma Stealer deepseeek, and deepseekai Bybit hack

Microsoft Security

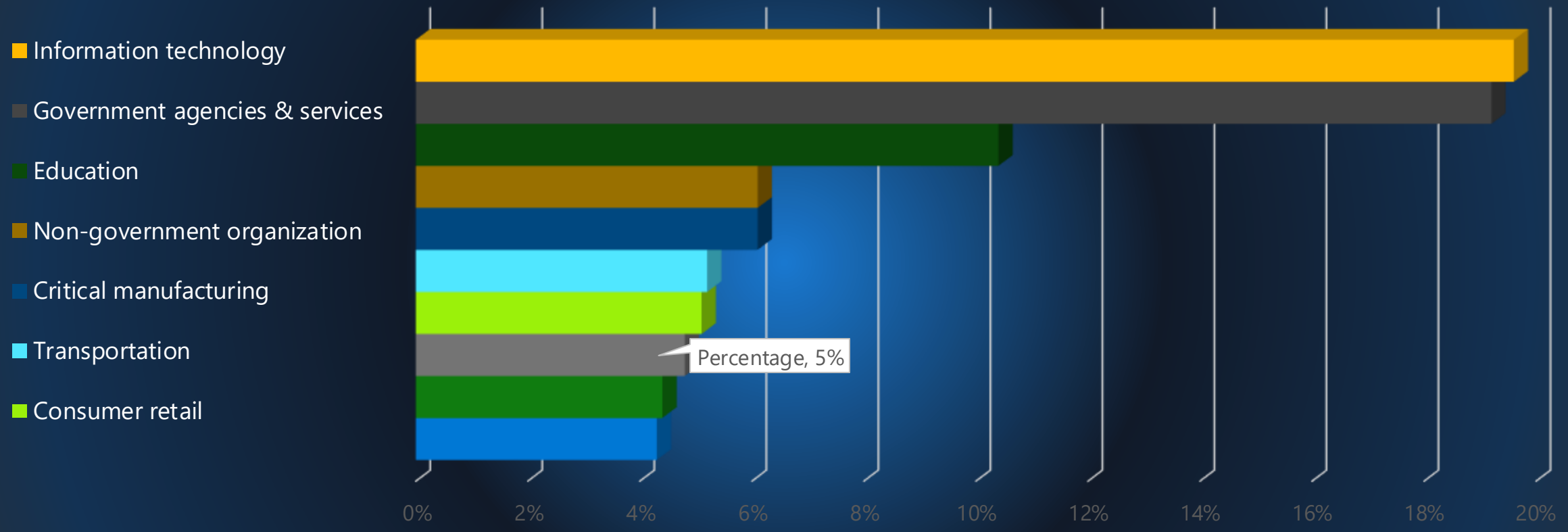
Threat landscape: Communications infrastructure sector

Q4 2024

Microsoft Threat Intelligence

Communications infrastructure ranking

Communications infrastructure is the 8th most commonly observed industry impacted in Q4 2024 analyzed events



Communications infrastructure also accounted for ~5% of the total number of Microsoft Defender for Endpoint malware-related alerts in the quarter

Communications infrastructure regional impact

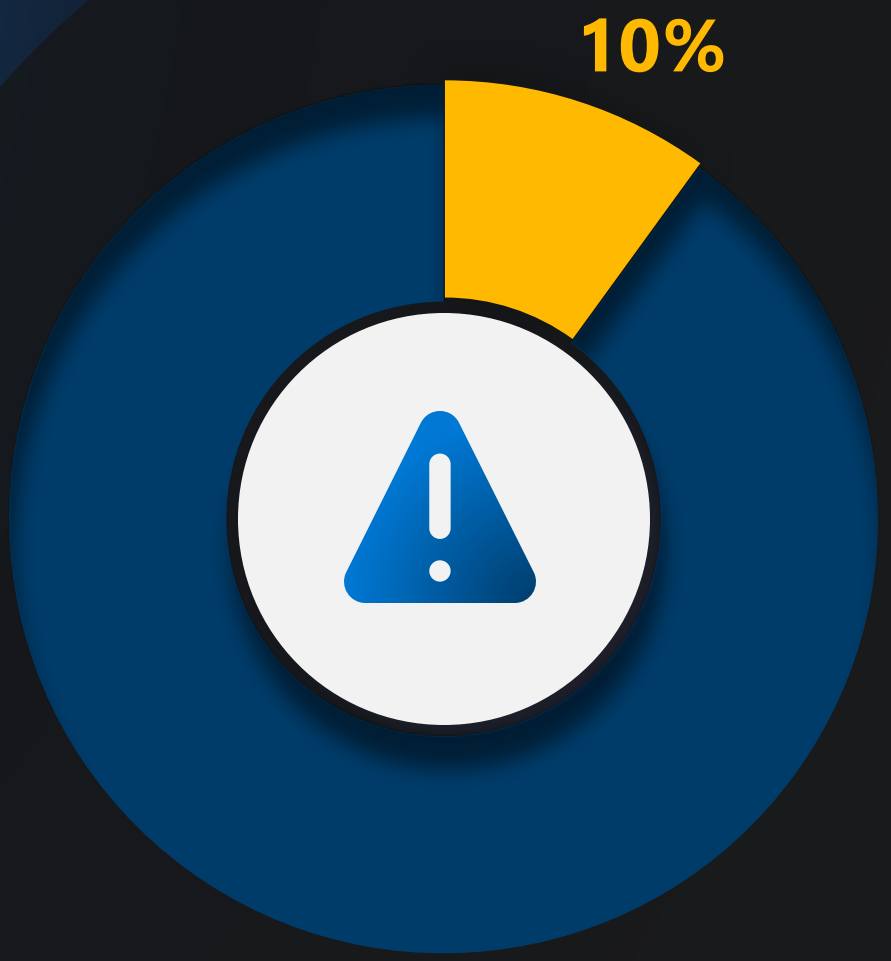
These regions were **most frequently impacted by cyber threats impacting the communications infrastructure sector** in Q4 2024

The top three countries facing **events impacting communications infrastructure** in Q4 2024 were:

- United States
- Israel
- Germany

Ransomware deployment
Q4 2024

About 1 in 10 threat actors impacting the communications infrastructure sector include ransomware deployment in their arsenal



Most active threat actors

Q4 2024

Sangria Tempest

Ukraine

Mango Sandstorm

Iran

Storm-0861

Iran

CVEs impacting communications infrastructure

Most exploited

Microsoft Office CVE-2017-11882	**Microsoft Windows CryptoAPI** CVE-2020-0601	**Microsoft Internet Explorer** CVE-2020-0674	**Apache Log4j2** CVE-2021-44228	**Polkit pkexec** CVE-2021-4034
Zoho ManageEngine CVE-2022-47966	**Linux Kernel** CVE-2016-5195	**Linux Kernel** CVE-2022-1043	**Microsoft SMBv3** CVE-2020-0796	**Microsoft Win32k** CVE-2020-1054
Linux Netfilter CVE-2021-22555	**pfSense pfBlockerNG** CVE-2022-31814	**Apple OS** CVE-2020-9839	**Linux eBPF** CVE-2021-3490	**Linux Kernel** CVE-2017-7308
Linux Kernel CVE-2017-16995	**Microsoft Win32k** CVE-2022-21882	**Linux Kernel** CVE-2022-0995	**GNU Bash** CVE-2014-6271	**Apple OS** CVE-2022-46689

Least exploited

How can we protect against 99% of attacks?

How effective is MFA at deterring cyberattacks? A recent study based on real-world attack data from Microsoft Entra found that MFA reduces the risk of compromise by 99.2 percent.[1]

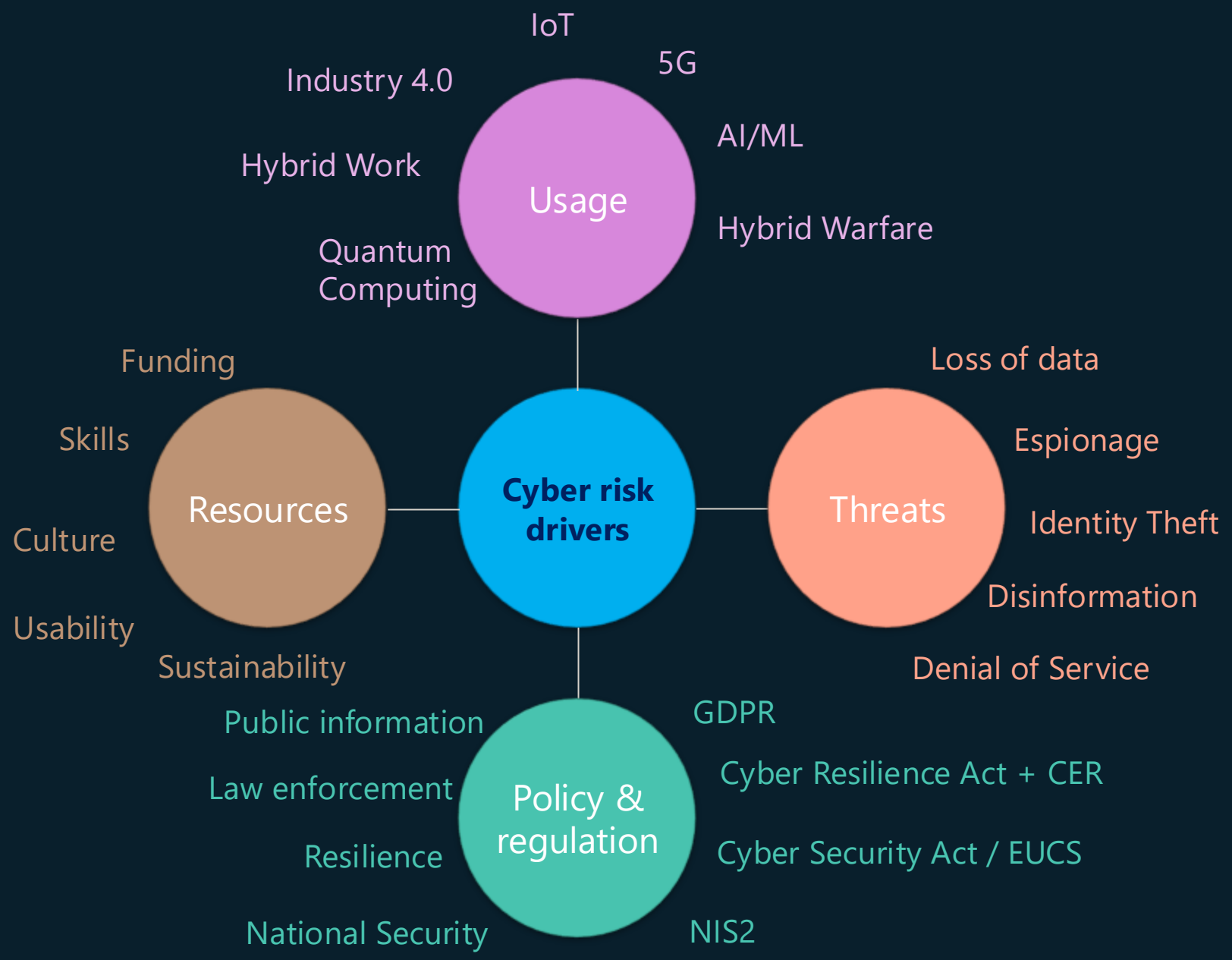
Fundamentals of cyber hygiene

99%

Basic security hygiene still protects against 99% of attacks.

- Enable multifactor authentication (MFA)
- Apply Zero Trust principles
- Use extended detection and response (XDR) and antimalware
- Keep up to date
- Protect data

Outlier attacks on the bell curve make up just 1%


IoT
5G
Industry 4.0
AI/ML
Hybrid Work
Usage
Hybrid Warfare
Quantum Computing
Funding
Loss of data
Skills
Espionage
Resources
Cyber risk drivers
Threats
Identity Theft
Culture
Disinformation
Usability
Sustainability
Denial of Service
Public information
GDPR
Law enforcement
Policy & regulation
Cyber Resilience Act + CER
Resilience
Cyber Security Act / EUCS
National Security
NIS2

The risk management matrix

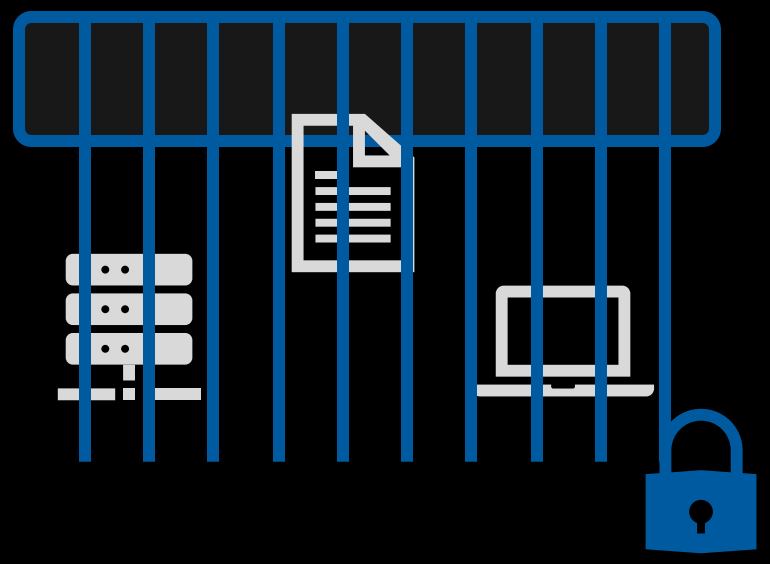
	On-Prem	IaaS	PaaS	SaaS
Users/processes	Customers	Customers	Customers	Customers
Data classification	Customers	Customers	Customers	Customers
Client protection	Customers	Customers	Customers	Suppliers
Identity & access protection	Customers	Customers	Suppliers	Suppliers
Application controls	Customers	Customers	Suppliers	Suppliers
Network protection	Customers	Suppliers	Suppliers	Suppliers
Server security	Customers	Suppliers	Suppliers	Suppliers
Physical security	Customers	Suppliers	Suppliers	Suppliers

Suppliers

Customers

Zero Trusts secures assets where they are

enabling secure freedom instead of locking them up in a "secure" network



Classic Approach – Restrict everything to a 'secure' network

Zero Trust – Protect assets anywhere with central policy

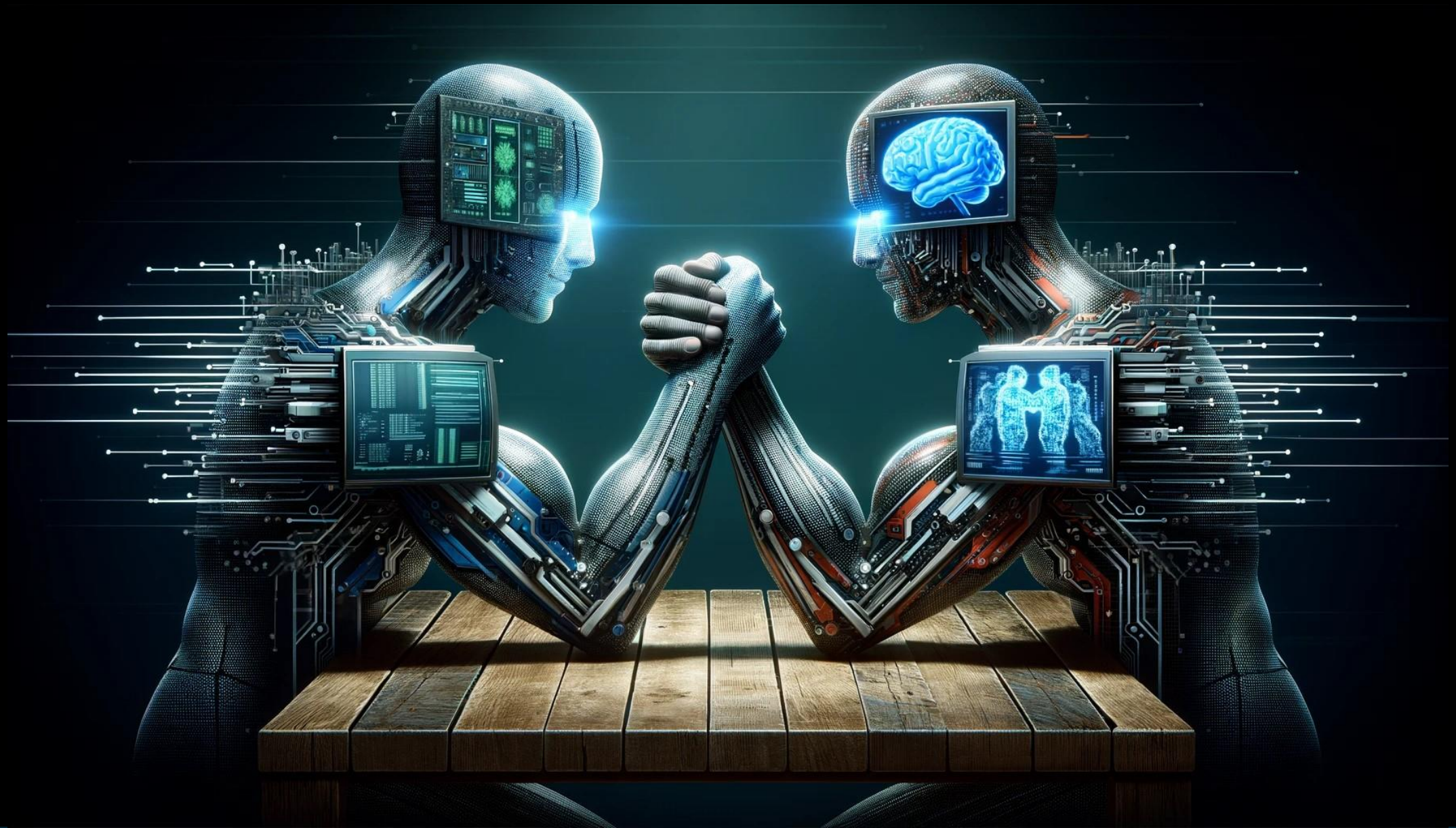
Secure Future Initiative

Secure by design | Secure by default | Secure operations

Security culture and governance

- Protect identities and secrets
- Protect tenants and isolate production systems
- Protect network
- Protect engineering systems
- Monitor and detect threats
- Accelerate response and remediation

AI - attackers vs. defenders



Microsoft

Thank you!

sandra.elvin@microsoft.com

@sandrabarouta

linkedin.com/in/sandrabaroutaelvin/