ARMIS

THE STATE OF

CYBERWARFARE

THE 2025 ARMIS CYBERWARFARE REPORT

WARFARE WITHOUT BORDERS:

AI's Role in The New Age of Cyberwarfare

By ARMIS LABS

FOREWORD

By Nadir Izrael,
CTO and Co-Founder, Armis

Over the last three years since Armis published its first State of Cyberwarfare and Trends Report, we've seen monumental shifts in cyberwarfare, driven by tectonic tensions in geopolitical conflicts and exponential advancements in technology, namely Artificial Intelligence (AI).

We've all read the headlines about evolving global conflicts: Russia's invasion of Ukraine, pressure building between China and Taiwan, and suspicions that North Korea completed the largest crypto heist in history strictly as a means to fuel the country's nuclear weapons program. These events have only compounded month-over-month, fueling the fire that has exacerbated global chaos, while at the same time, advancements in AI and quantum computing fan the flames.

Now is not the time to become enthralled as bystanders who cannot look away. While it may seem as though these examples are ever-distant to many of us, the threat looms large and is much closer than most appreciate. It is up to us to answer this call to action to protect society as we know it from an impending attack. To successfully do this, it's essential we have a comprehensive understanding of the ever-expanding attack surface in order to manage cyber risk exposure in real-time. With this knowledge, we can take action – before it's too late.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

87% Over **87% of IT decision-makers** are concerned about the impact of cyberwarfare on their organizations

The lines between traditional warfare and cyber conflict have blurred. At the same time, AI-driven cyberattacks have evolved at a rapid-pace, growing more sophisticated each day. Entire organizations are vulnerable and nations are caught in a digital crossfire. Tensions between nations have escalated to unprecedented levels, and the threat of cyberwarfare is no longer a distant fear.

In this third edition of the *Armis State of Cyberwarfare and Trends Report*, we reveal a landscape transformed by AI-driven threats and an inability to keep up. Now, **over 87% of IT decision-makers are concerned about the impact of cyberwarfare on their organizations** – a monumental shift from previous reports. Last year, **almost half (46%) of IT leaders surveyed said they were unconcerned or indifferent about the impact of cyberwarfare**. So, what's changed?

A key factor is the rise in geopolitical uncertainty, fueled by armed conflicts and a seismic shift in the 2024 election cycle, where every governing party in a developed nation lost vote share. However, the most significant driver is AI, which is dramatically escalating the scale and sophistication of cyber threats, from large-scale ransomware attacks to full-on cyber-physical attacks impacting our critical infrastructure.

Almost **two-thirds (64%) of IT leaders agree that generative AI (GenAI) challenges the geopolitical status quo**, allowing smaller nations and non-state actors to emerge as near-peer cyber threats. Advanced Persistent Threat (APT) groups aligned with Russia, Iran, North Korea, and China are all using Large Language Models (LLMs) and OpenAI's systems to enhance their operations and erode trust in democratic institutions. Iranian-linked hackers 'CyberAv3ngers', for example, are using tools like ChatGPT to exploit weaknesses in water systems, energy grids, and manufacturing facilities across the globe.

This year's report highlights the ramifications of AI. **Almost half (48%) of IT leaders acknowledge that their organizations were previously hacked and have not managed to secure their ecosystem adequately.** In the food and beverage sector, this skyrockets to 62%. Yet, these challenges are not new. Last year's report underscored similar issues: overwhelmed teams, a deluge of data, and limited resources, leaving organizations struggling to close critical gaps. The difference now is that attackers are weaponizing AI at unprecedented levels, accelerating risks while organizations fall further behind in their ability to respond.

KEY FINDINGS

AI AS A DOUBLE-EDGED SWORD

AI continues to supercharge the cyber threat from nation states such as Russia, China, North Korea, Iran and their proxies. **Almost three-quarters (74%) of IT decision-makers agree that AI-powered attacks significantly threaten their organization's security**. Russia's integration of AI into its cyberwarfare strategies is raising fears, especially in the UK and Europe. Similarly, China's DeepSeek AI model has sparked privacy and security fears, leading to bans in Italy, Taiwan and across the U.S.

This is echoed by **73% of IT leaders specifically worried about nation-state actors using AI for cyberattacks.** The rise of AI-generated disinformation further underscores the broader challenge of defending against increasingly sophisticated AI-driven cyber operations. While **77% of IT decision-makers agree with the statement, *'My organization has implemented measures to detect and counter AI-powered attacks,'*** the ease with which attackers can exploit AI tools to manipulate narratives and clone voices poses a significant threat to organizations and individuals alike.

While AI is part of the threat, it's also the solution. AI-powered threat intelligence is transforming security, enabling proactive risk detection and mitigation for organizations to use AI to fight against AI, creating a high-speed "machine-

AI in Offensive Cyber Operations

Key Capabilities Observed by Armis Labs

Automated Malware Development:
AI-generated malicious code can dynamically alter itself to avoid detection.

AI-Driven Phishing:
Machine-generated messages enhance the effectiveness of social engineering attacks.

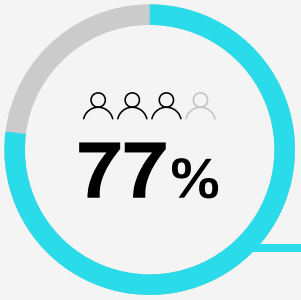
Deepfake Disinformation:
AI-generated media manipulates public perception and undermines trust in digital communication.

Autonomous Network Attacks:
AI-powered tools continuously scan for vulnerabilities and execute attacks without human intervention.

AI Attack Recommendation:
AI-powered tools to identify the most ikely areas to attack that won't have detection in place.

versus-machine" dynamic where AI systems are constantly engaged in an escalating battle of innovation. Predictive AI models help neutralize threats preemptively, while AI-driven solutions monitor both surface and dark web activity for early warning signs. The combination of surface and dark web monitoring, purpose-configured honeypots, and human intelligence provides a crucial edge, helping security teams stay ahead of emerging threats. Yet, almost half (49%) say their organization lacks the budget and resources to invest in AI-powered security solutions. A further 50% of IT leaders acknowledge that their organization lacks the necessary expertise to implement and manage AI-driven cybersecurity tools.

GLOBAL TENSIONS FURTHER FUEL INSTABILITY



of IT decision-makers agree that geopolitical tensions globally have created a greater threat of cyberwarfare

Alongside AI's role, over **three-quarters (77%) of IT decision-makers agree that geopolitical tensions globally have created a greater threat of cyberwarfare**, a stark increase from 41% in the previous year. France, in particular, is acutely aware of this risk, with 85% of respondents reporting a greater threat after a year of political and social turmoil. Even after successfully repelling countless cyberattacks during the 2024 Olympics, France was targeted by disinformation campaigns seeking to erode trust in its ability

AI in Defensive Cyber Operations

Key Capabilities Identified by Armis Labs

Behavioral Analysis:
AI detects deviations from normal user activity, identifying potential intrusions.

Automated Threat Hunting:
AI continuously scans for new attack vectors, indicators of offensive actions and indicators of compromise.

Adaptive Defense Mechanisms:
AI enables real-time reconfiguration of security settings in response to emerging threats.

Exploitation Detection:
Machine learning models identify exploitation of vulnerabilities in software.

TTP Detection:
Machine learning models identify variations in typical CLI and system components acting outside of normal functions.

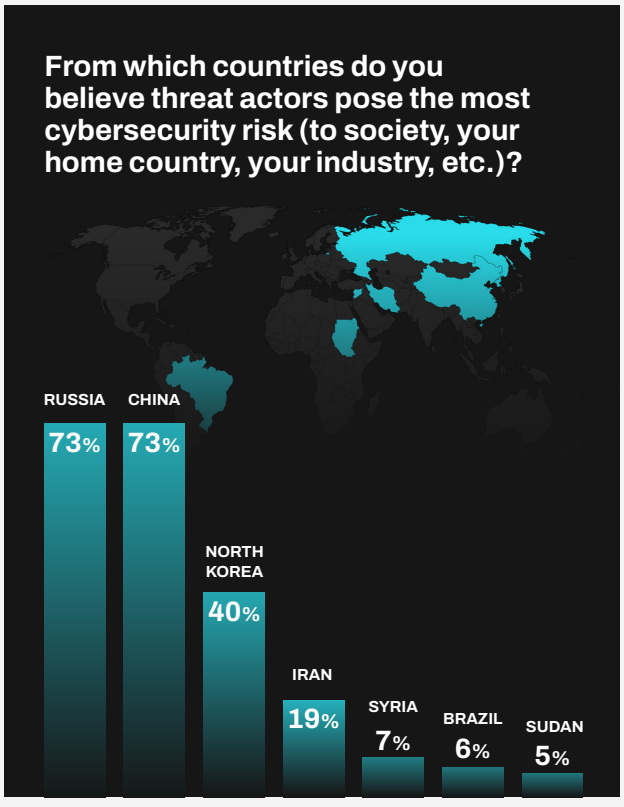
New System Detection:
Machine learning models identify when new OT, IOT and applications come online in a vulnerable state.

Visibility Gap Analysis:
Find assets that are not sufficiently protected with poor visibility.

Defensive Recommendation:
Identification of a threat and mitigation plan based upon relevant defensive capabilities.

to safeguard critical infrastructure. Furthermore, allegations of Russian-linked election interference exacerbated the nation's fragile political and economic situation.

These incidents are not isolated events. Across the globe, **IT decision-makers consistently point to three dominant state-sponsored threats: Russia (73%), China (73%), and North Korea (40%).** Regional perspectives vary *(Fig. 1)*; however, when asked whether "*China is more of a threat to security than Russia*," over half (51%) agreed. This has increased from 44% from last year. Moreover, 72% of IT leaders believe that the cyber capabilities of nation-state actors have the potential to trigger a full-scale cyberwar, with devastating consequences for global critical infrastructure.



(Fig. 1) Top threat actors per country

Modern warfare has evolved to incorporate digital attacks alongside drones and sophisticated missile systems. Global hotspots illustrate how easily digital conflict can ignite broader instability. Latin American governments are being targeted by Russian and North Korean disinformation campaigns, largely due to economic and political ties to the U.S. Escalating tensions in the Middle East further disrupt the regional balance. In Eastern Europe, the Russia-Ukraine war has intensified, and Southeast Asia faces mounting uncertainty as China increases military exercises near Taiwan. Each conflict brings with it economic and geopolitical ramifications.

The renewed focus of global leaders on foreign policy and countering China's influence could serve as a flashpoint for new geopolitical tensions. Potential shifts in NATO commitments and trade relations may inadvertently create vulnerabilities, both physical and cyber, that adversaries are poised to exploit.

Despite these looming threats, over half (53%) of IT decision-makers now express confidence in their government's ability to defend against cyberwarfare, up dramatically from last year's report. This optimism likely stems from greater awareness of nation-state threats and the visibility of countermeasures, such as the U.S. and Japan's joint investment in AI-driven cyber defense research. While these initiatives are positive, their ability to keep pace with emerging threats remains uncertain.

Nation-State AI Cyber Capabilities

Reported by Armis Labs

United States - The U.S. invests heavily in AI for cyber defense, leveraging machine learning for various offensive and defensive operations. Government agencies collaborate with private-sector cybersecurity firms to enhance AI-powered security solutions. AI-driven Security Operations Centers (SOCs) provide real-time automated response to cyber threats. Intelligence agencies have been using AI extensively for developing analytical capabilities.

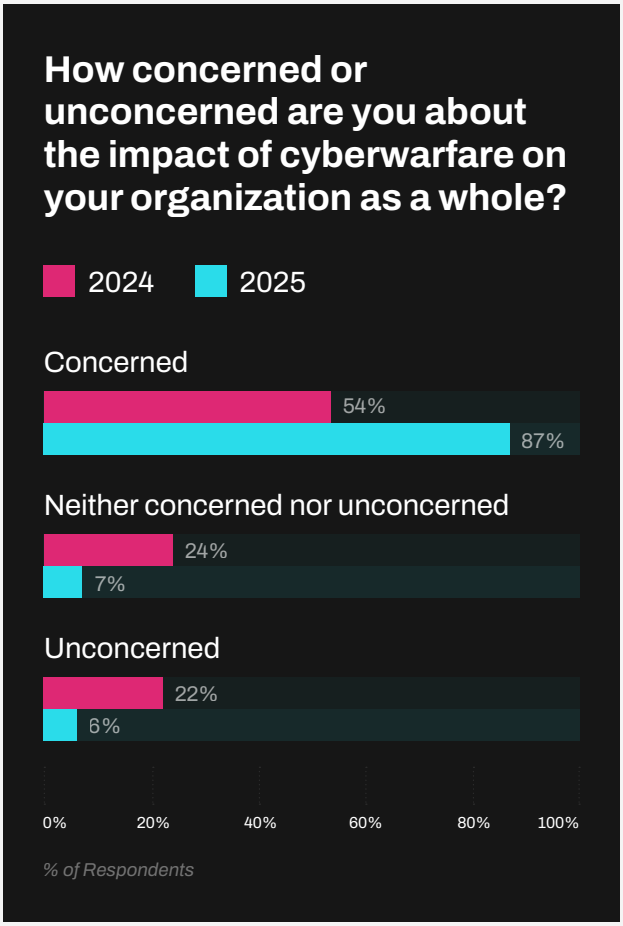
China - China incorporates AI into cyber espionage and influence operations. Chinese APT groups utilize AI for vulnerability discovery, data analysis, and disinformation campaigns. AI-enhanced big data analytics improve intelligence-gathering capabilities, while automated influence campaigns leverage AI-generated content to manipulate public opinion.

Russia - Russia employs AI for large-scale disinformation campaigns and cyber espionage. AI-powered bot networks amplify propaganda, while AI-generated fake news and deepfakes influence geopolitical events. Russian cyber units experiment with AI-enhanced malware obfuscation to evade detection.

Iran & North Korea - Iranian and North Korean cyber actors use AI to optimize phishing attacks, conduct financial cybercrimes, and analyze stolen data for intelligence purposes. North Korea employs AI-assisted reconnaissance to enhance cryptocurrency theft operations that fund its military programs.

CYBERWARFARE TAKES CENTER STAGE

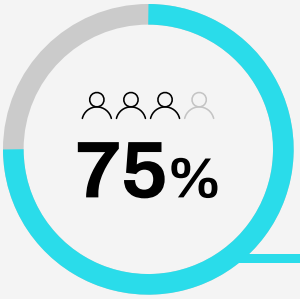
This year's report highlights how cyberwarfare has emerged as a central issue for organizations worldwide *(Fig. 2)* due to the increasing frequency and sophistication of attacks, coupled with escalating global tensions.



(Fig. 2) Timeline of concern around the impact of cyberwarfare.

A third (33%) of IT decision-makers strongly agree that their organization is prepared to handle a cyberwarfare attack; however, the relentless evolution of cyber threats continues to expose critical vulnerabilities in modern network ecosystems *(Fig 3)*, forcing businesses to continuously rethink their priorities. Yet,

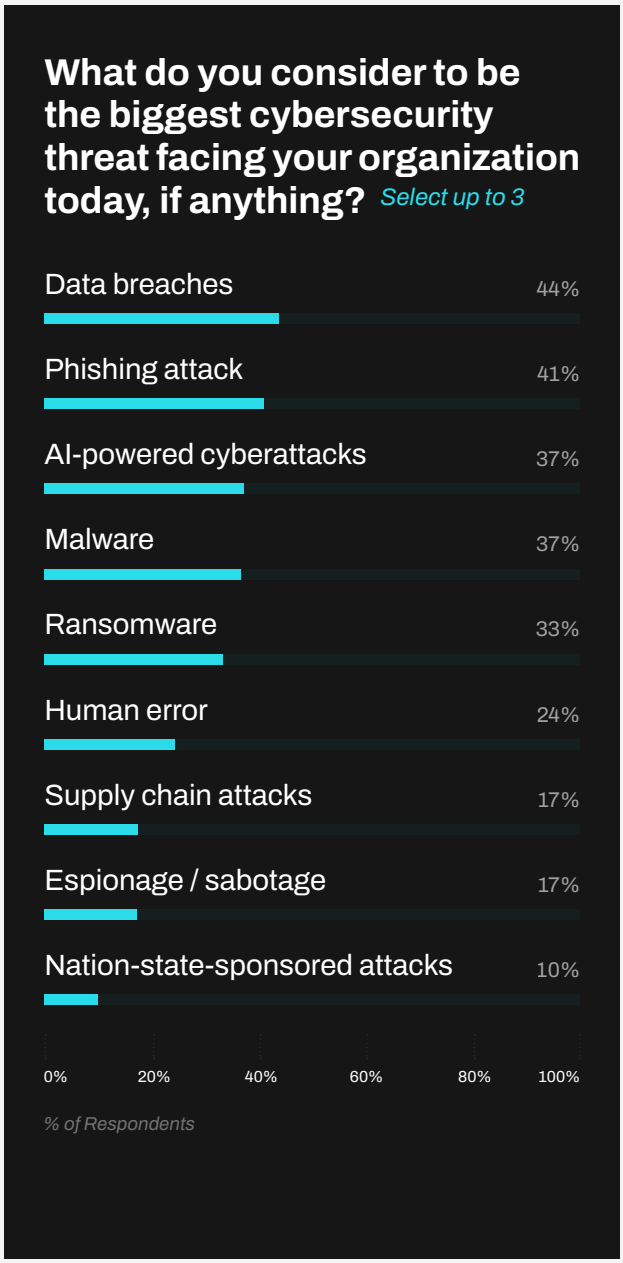
cybersecurity funding remains inadequate. Less than 35% of IT leaders strongly agree that their company has allocated a sufficient budget for cybersecurity programs, including people and processes, with only 25% of medical, healthcare, and pharmaceutical respondents feeling adequately funded. The government and public sector fares even worse at just 20%.



of IT decision-makers believe cyberwarfare attacks will increasingly target institutions representing free press and independent thought

Cyberwarfare is no longer confined to traditional military targets, either. **Three-quarters (75%) of IT decision-makers believe cyberwarfare attacks will increasingly target institutions representing free press and independent thought** – a sharp rise from last year's 42%. This is already playing out, APT groups like China's Salt Typhoon are persistently targeting critical U.S. infrastructure such as telecommunications providers Verizon and T-Mobile.

IT decision-makers are four times more likely to report increased threat activity on their networks in the past six months compared to the six months prior (40%). This is double the rate reported last year (19%). Thankfully, 81% of respondents agree that shifting to a more proactive cybersecurity posture that helps prevent breaches is a top goal of their organization in the year ahead.



(Fig. 3) Top five biggest cybersecurity threats.

Emerging AI-Driven Cyber Threats

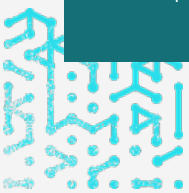
Identified by Armis Labs

Adversarial Machine Learning Attacks: Attackers manipulate AI models to misclassify threats, evade detection, or disrupt defensive AI systems.

AI-Powered Social Engineering: AI-generated voice and video deepfakes deceive targets into revealing sensitive information.

Exploitation of AI Vulnerabilities: Attackers target AI-based security tools to manipulate or disable cyber defenses.

Autonomous Cyber Weapons: AI-driven malware operates independently, adapting to security measures in real-time.



THE COST OF CYBERWARFARE

The financial and operational toll of cyberwarfare is escalating at an alarming rate. In 2024, the global average cost of a data breach was $4.88M USD, up 10% when compared to 2023 and the highest total ever. This is disrupting industries and crippling business operations, as just **over two-thirds (67%) of IT decision-makers report that their company has experienced a cybersecurity breach at least once**. While not every breach results in a financial payout, the impact can range from data theft and operational downtime to large-scale ransomware extortion.

The third edition of the *Armis State of Cyberwarfare and Trends Report* highlights how ransomware payouts have now risen following previous research. **The average ransomware payout in the UK is £5.6 million**, with 1 in 8 companies (12%) paying between £3.95 million and £7.9 million. The situation is even more severe **in Europe, where the average payout rises to €8.5 million**, with over half (51%) of EU companies surveyed having had to make a ransomware payout. **The U.S. and Australia top the list, with an average payout of $10.1 million**, with 1 in 10 companies (10%) reporting payments exceeding $10 million (Fig. 4).

When making a ransomware payout, how much does your company pay on average?

Europe

Under €475,000, *please specify in € (range 1-474999)*	1%
€475,000 - €950,000	8%
Over €950,000 - €1.9M	9%
Over €1.9M - €4.75M	8%
Over €4.75M - €9.5M	14%
Over €9.5M - €28.5M	7%
Over €28.5M - €47.5M	4%
Over €47.5M, *please specify in € millions (range 47.6+)*	0.17%

United States

Under $500,000, *please specify in $*	1%
$500,000 - $1M	11%
Over $1M - $2M	11%
Over $2M - $5M	9%
Over $5M - $10M	10%
Over $10M - $30M	10%
Over $30M - $50M	8%
Over $50M, *please specify in $ millions*	0.2%

Australia

Under $500,000, *please specify in $*	4%
$500,000 - $1M	11%
Over $1M - $2M	10%
Over $2M - $5M	9%
Over $5M - $10M	9%
Over $10M - $30M	10%
Over $30M - $50M	4%
Over $50M, *please specify in $ millions*	0.5%

United Kingdom

Under £395,000, *please specify in £*	1%
£395,000 - £790,000	7%
Over £790,000 - £1.58M	10%
Over £1.58M - £3.95M	8%
Over £3.95M - £7.9M	12%
Over £7.9M - £23.7M	6%
Over £23.7M - £39.5M	5%
Over £39.5M, *please specify in £ millions*	0.2%

% of Respondents

(Fig. 4) The average cost of a ransomware payment (regional).

These figures reveal a troubling trend: cybercriminals are growing bolder, targeting high-value sectors where disruption can be used for maximum financial gain. The automotive industry has been hit the hardest, with EU companies making an average payout of €12.8 million while UK businesses pay an average of £13.9 million.

Although 75% of IT decision-makers see increased cybersecurity prioritization from their boards and C-suites, this represents only a partial rebound after last year's significant decline in executive-level focus (from 76% in 2022/23 to 51% in 2023/24). The cost is now more than just financial. It puts individuals and their most sensitive information at risk. Take the 2024 Change Healthcare ransomware attack, the largest U.S. healthcare data breach in history, which compromised the data of 190 million Americans. Those organizations that fail to take proactive measures are not only risking their bottom line but also the trust and safety of the people they serve.

CLOSING THE CYBERSECURITY GAP

It's clear that defensive measures are still lacking. **58% of organizations only respond as an attack occurs or after the damage has already been done** *(Fig 5)*. Such a reactive approach invites AI-driven cyberattacks that can cripple operations before defenses can even react. This lack of preparedness means that organizations that stay the course will always be left chasing their tails – to the detriment of society.

Key gaps include: securing remote or hybrid work environments (31%), insufficient budget to scale cybersecurity operations (24%), and inadequate threat intelligence to identify and prioritize risks effectively (23%).

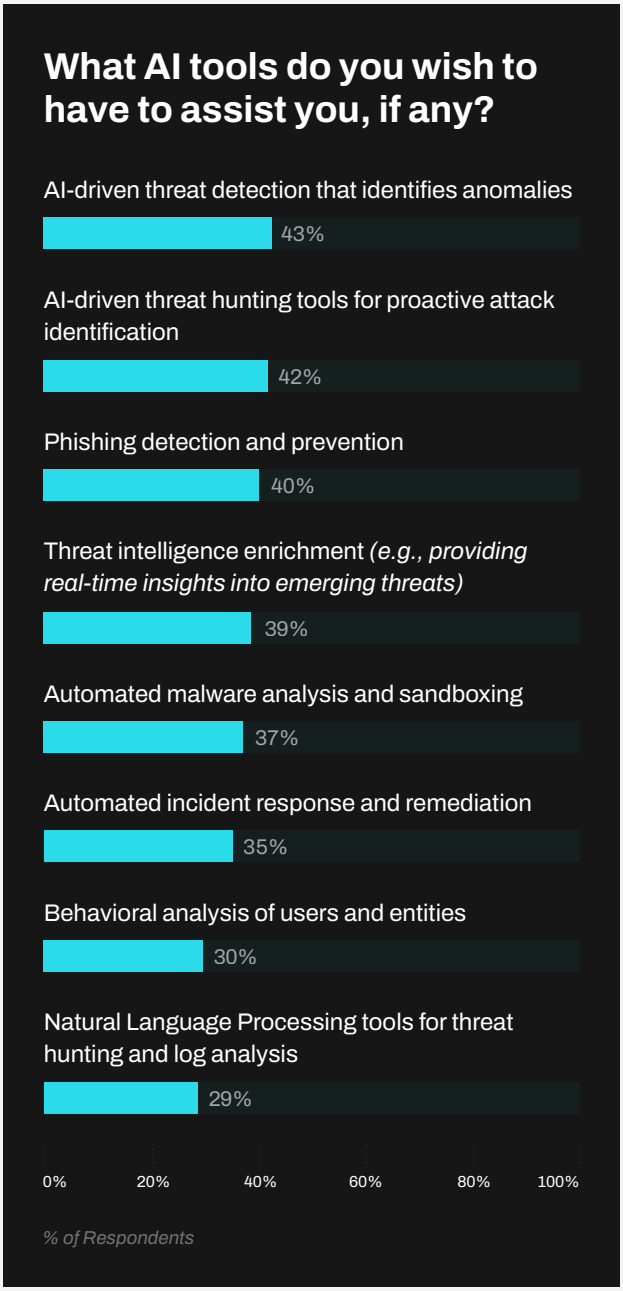
(Fig. 5) How quickly organizations detect and respond to a cyberattack

Additionally, 4 in 5 (85%) IT decision-makers surveyed report that offensive techniques regularly bypass security tools, showcasing how traditional methods are not enough. The nature of these attacks varies by region: IT leaders in France (39%), the U.S. (34%), and Italy (29%) most frequently cite phishing and spear-phishing attacks as the techniques that regularly evade

security tools, whereas in Germany, credential theft and abuse, through brute force or password spraying (31%), are the most commonly observed techniques bypassing security measures.

Common security strategies include using multi-factor authentication (MFA) (58%) and enforcing strong password policies (56%), while deploying AI-powered security tools (46%) to fight back effectively is noticeably lower. While a solid foundation, these measures fail to address the evolving nature of AI-driven cyberattacks. At least 42% of IT leaders said their organization is limiting user privileges to better address the increasing sophistication of cyberattacks, particularly those using AI.

Many recognize AI's potential to strengthen their defenses, with 94% of IT decision-makers wishing they had AI tools to assist them *(Fig. 6)*. And AI is already proving its worth. The U.S. Treasury, for instance, has recovered over $4 billion in improper payments, with $1 billion a direct result of AI. Yet, without proper support, the gap between AI's offensive and defensive capabilities will widen, leaving organizations vulnerable. Addressing this requires strategic investment and a shift to proactive, AI-driven security.



(Fig. 6) What AI tools do you wish to have to assist you, if any?

AI-powered Technological Countermeasures

Recommended by Armis Labs

Large Language Models (LLMs)

- Adversarial Fine-Tuning & Alignment
- Robust Training Data & Poison Mitigation
- API Security & Model Extraction Defenses
- Red-Teaming and Continuous Monitoring

RAG (Retrieval-Augmented Generation) Frameworks

- Input Segmentation (“Spotlighting”)
- Dynamic Content Filtering
- State Delta Monitoring (TaskTracker)
- Robust Aggregation of Retrieved Results
- Secure Retriever & Index Management

MCP (Model Context Protocol) Servers

- Strong Authentication & Isolation
- Model Provenance & Signing
- Confidential Model Serving Environments
- Continuous Monitoring & Throttling
- End-to-End MLOps Security

By combining classic cybersecurity methods (e.g., encryption, access control, auditing) with AI-specific defenses (e.g., adversarial training, prompt safeguards, robust aggregation), organizations are striving to keep AI systems secure and trustworthy under malicious pressure. Multiple layers of defense ensure that evolving threats are continually addressed, maintaining security for LLMs, autonomous systems, RAG frameworks, and MCP servers well into 2025 and beyond.

WHO HAS IT WORSE?

Medical, healthcare, pharmaceutical

75% of respondents from the medical, healthcare and pharmaceutical industries **believe that AI-powered attacks pose a significant threat** to their organization’s security.

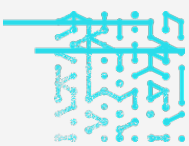
Half (50%) of respondents within the sector state that their organization lacks the necessary budget and resources to invest in AI-powered security solutions.

43% of respondents agree that their organization typically detects and responds to a significant cyberattack as it occurs and not before.

Financial services and insurance

76% of respondents from financial services and insurance **believe the cyber capabilities of nation-state actors have the potential to instigate a full-scale cyberwar** that could cripple critical infrastructure worldwide.

When making a ransomware payout, financial services and insurance companies based in the EU pay, on average €10,156,617. Whereas for those companies based in the U.S., the average rises to $15,372,747.



Manufacturing and engineering

80% of respondents from manufacturing and engineering **agree that geopolitical tensions globally have created a greater threat of cyberwarfare.**

Over 78% working within the sector are concerned about the potential for nation-state actors to use AI to develop more sophisticated and targeted cyberattacks.

32% of IT decision-makers surveyed in the sector identified challenges in securing remote or hybrid working environments as the top gap in their security operations.

Utilities: energy and water

When making a ransomware payout, utility companies in the U.S. and Australia pay on average €10,156,617.

80% of respondents from the utilities: energy and water sector **believe that AI-powered attacks significantly threaten their organization's security.**

40% of respondents within the sector state that their organization lacks the necessary budget and resources to invest in AI-powered security solutions.

Additional findings from Armis Labs

Healthcare:
Continues to be the worst impacted with the highest number of confirmed breaches and severe high-profile incidents (e.g., UnitedHealth Group attack).

Telecommunications:
Significantly impacted by the Salt Typhoon incident, which dramatically worsened its cyber attack exposure.

Education and Research:
Experienced dramatic spikes in attacks during Q2 and Q3 2024, though overall annual figures are less than healthcare's impact.

Information and Communication:
Notable for high breach rates in the UK, with 72% of businesses reporting incidents, but with lower global figures than the top sectors.

Retail/Manufacturing:
Faced breaches, often linked to credential theft and legacy vulnerabilities, but overall impact remained lower compared to the sectors above.

Special note: We expect to see an increase in supply chain attacks. Particularly in open source tools.

Food and beverage

When making a ransomware payout, IT decision-makers working in food and beverage companies in the UK pay on average £6,940,714. Whereas for those companies based in the EU, the average rises to €9,120,000.

76% of those surveyed from the food and beverage industry **say their organization lacks the necessary expertise to implement and manage AI-powered security solutions.**

Over 62% say their organization was hacked previously and has not managed to adequately secure its ecosystem since.

Transportation

79% of respondents in the transportation industry **believe that geopolitical tensions globally have created a greater threat of cyberwarfare.**

35% of respondents from this sector agree that their organization typically detects and responds to a significant cyberattack as it occurs and not before.

27% of respondents identified challenges in securing remote or hybrid work environments and difficulty identifying and managing shadow IT or ephemeral assets as the top gaps in their security operations.

KEY REGIONAL FINDINGS

UNITED STATES

80% | **of U.S. respondents believe** that AI-powered attacks pose a significant threat to their organization's security.

79% | **of U.S. IT decision-makers** believe China poses the most cybersecurity risk.

77% | **believe** the cyber capabilities of nation-state actors have the potential to instigate a full-scale cyberwar that could cripple critical infrastructure worldwide.

57% | **of respondents from the U.S. say** their organization lacks the necessary expertise to implement and manage AI-powered security solutions.

UNITED KINGDOM

73% | **of UK respondents believe** the cyber capabilities of nation-state actors have the potential to instigate a full-scale cyberwar that could cripple critical infrastructure worldwide.

66% | **believe** GenAI is challenging the geopolitical status quo by enabling smaller nations to emerge as near-peer cyber threats.

45% | **of UK IT leaders** believe China now poses more of a threat to security than Russia.

32% | **of those surveyed** in the UK identified challenges in securing remote or hybrid working environments as the top gap in their security operations.

GERMANY

79% | **of IT decision-makers based in Germany** believe Russia poses the most cybersecurity risk.

69% | **of IT leaders** based in Germany are reconsidering suppliers and increasing cybersecurity investments due to geopolitical tensions.

52% | **Over half of respondents in Germany** consider AI-powered cyberattacks the biggest cybersecurity threat facing their organization today.

57% | **believe** that nation-states would target their organization.

FRANCE

86% | **of IT decision-makers based in France** believe Russia poses the most cybersecurity risk.

85% | **believe** that geopolitical tensions globally have created a greater threat of cyberwarfare.

45% | **surveyed** in France said the top AI tool they wish they had to assist them is AI-driven threat detection that identifies anomalies.

45% | Yet, **45% more** say their organization lacks the necessary expertise to implement and manage AI-powered security solutions.

ITALY

74% | **of respondents based in Italy believe** that geopolitical tensions globally have created a greater threat of cyberwarfare.

47% | **Almost half** of those surveyed in Italy consider the biggest threat facing their organization to be malware.

40% | **of IT leaders** in Italy have experienced more threat activity on their network in the past six months than in the six months prior.

29% | Yet, **only 29% agree** that the threat is imminent.

AUSTRALIA

85% | **of those surveyed in Australia** agree that their organization is actively investing in security tools to stay ahead of emerging AI-powered threats.

71% | **believe** GenAI is challenging the geopolitical status quo by enabling smaller nations to emerge as near-peer cyber threats.

56% | **Over half say** their organization was hacked previously and has not managed to adequately secure its ecosystem since.

57% | **A further 57%** say their organization lacks the necessary expertise to implement and manage AI-powered security solutions.

PROACTIVELY NAVIGATING THE AI-DRIVEN THREAT LANDSCAPE

As the world moves deeper into the era of cyberwarfare, every organization is at risk. The reality is that cyberwarfare is one of the cheapest and most efficient ways to engage in war. With AI, the ability for bad actors to strike from a distance amplifies this further. Traditional security tools and manual oversight are ill-equipped to secure a landscape where vulnerabilities multiply faster than defenders can respond. But it's also the key to fighting back. The only way to counter AI-driven threats is with AI-powered defense.

With 50 billion connected assets expected in 2025, organizations cannot afford to rely on outdated, siloed security strategies. Instead, they must embrace comprehensive, real-time cyber exposure management to safeguard their infrastructure, operations, and data. After all, information is the ultimate weapon in cyberwarfare. It's time for organizations to flip the script and use the information they have available to them.

Armis, the cyber exposure management & security company, provides organizations with the visibility, security, and risk management capabilities necessary to navigate this evolving threat landscape. With its AI-powered Armis Centrix™ platform, Armis enables organizations with one comprehensive solution to address every facet of cyber exposure management – from asset discovery and management through to vulnerability discovery, prioritization and remediation. Through the use of AI-driven early warning insights, Armis Centrix™ also provides early warning intelligence, empowering organizations to anticipate and mitigate cyber threats before they have any impact on their environment. Armis ensures that organizations have real-time situational awareness of their entire attack surface – closing security gaps before they can be exploited and protecting every link in the digital chain.

The reality of modern cyberwarfare means that defending an organization's infrastructure is now a societal and economic imperative. Financial services, energy grids, healthcare systems, and supply chains are increasingly in the crosshairs of cyber adversaries. A successful attack on these sectors can disrupt economies, endanger lives, and compromise national security. Organizations must prioritize cybersecurity resilience, implementing proactive threat detection, robust risk management, and collaborative defense strategies to safeguard essential infrastructure and maintain public trust. It's time to fight back. Armis is at the forefront of this battle, providing organizations with the tools and intelligence needed to see, protect and manage their entire digital ecosystem in real-time.

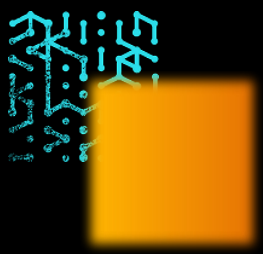
As the next twelve months unfold, state-sponsored chaos, AI-driven weaponry, and the blurred lines between civilian and military targets will define the cyber domain. To defend against these rising threats, we must adopt holistic security strategies, moving from a reactive to a proactive security posture.

ABOUT ARMIS LABS

Armis Labs, a division of Armis, is a team of seasoned security professionals dedicated to staying ahead of the ever-evolving cybersecurity landscape. With a deep understanding of emerging threats and cutting-edge methodologies, Armis Labs empowers organizations with unparalleled visibility and expertise to protect against the threats that matter most, right now.

Armis Labs is more than just a cybersecurity division; it's a thought leader in the field, constantly pushing the boundaries of knowledge and innovation. Through active participation in industry conferences, publication of research papers and contribution to industry-wide projects, Armis Labs shapes the discourse around emerging cyber threats and mitigation strategies.

At the heart of Armis Labs lies a formidable research powerhouse, where experts investigate the latest trends and tactics employed by cyber adversaries. Armed with state-of-the-art tools and methodologies, the team at Armis Labs conducts in-depth analyses of evolving threats both in the pre-emergence stage and "in the wild" stage of an attack.



METHODOLOGY

Armis revisits its findings, analyzing how known attacks, methodologies, and sentiment towards cyberwarfare have evolved. This latest study, conducted by Censuswide, surveyed over 1,800+ IT decision-makers in companies with 1,000+ employees in the U.S., UK, Italy, France, Australia, and Germany to provide the latest comprehensive picture of the growing crisis.

Over the past three years, Armis has surveyed 10,427 respondents as part of this cyberware report series. This year's report, as well as past reports (2024, 2023), also includes Armis proprietary data from Armis Labs, Armis Centrix™ for Early Warning and the Armis Asset Intelligence Engine.

This year's data was collected in December 2024. Censuswide abides by and employs members of the Market Research Society and follows the MRS code of conduct and ESOMAR principles. Censuswide is also a member of the British Polling Council.

Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011

ARMIS