ARMIS®

THE STATE OF

CYBERWARFARE

THE INVISIBLE FRONT LINE: AI-POWERED CYBER THREATS ILLUMINATE THE DARK SIDE

THE 2024 ARMIS
CYBERWARFARE REPORT

TABLE OF CONTENTS

INTRODUCTION

Make no mistake, the world is at war. A new axis has arisen. Democratic and freedom-oriented sovereign states around the globe are now under constant attack from bad actors and Eastern axis enemies.

The digital realm has become the front line of a once silent conflict that rages between nations and rogue factions across the globe. Bad actors are relentless, the damage and scale widespread, and the feeling of vulnerability is undeniable. Artificial Intelligence (AI) has brought this war to a new level, one that was widely predicted, but not expected to happen so soon.

In the second edition of the Armis Cyberwarfare Report, we expose a sobering truth: the paradigm has shifted dramatically over the last 12 months and most are woefully unprepared. So much so that many even believe their own governments can't protect them from the negative impacts of cyberwarfare. Put simply, many of us are on our own in this battle and likely to fall victim sooner rather than later. It's time to get ready before it's too late.

Stuxnet – the first publicly known very sophisticated, targeted nation-state cyberweapon – shattered the illusion of digital safety way back in 2010. Since then, the barrage has been relentless: the Chinese government hacking systems belonging to U.S. companies and military contractors, Ukrainian critical infrastructure and government systems under fire for years by Russian cyberweapons, cyberwarfare raging across the Middle East, and North Korea stealing $3bn to fund its nuclear weapons program; to mention only a few of the well-cataloged incidents. These are only the 'tip of the iceberg' when it comes to the state of modern-day AI-fueled cyberwarfare.

Now, with the widespread adoption of AI, everyone from the European Parliament to the Cybersecurity and Infrastructure Security Agency (CISA) are trying to protect networks and critical infrastructure from the risks of AI-related cyberattacks. Nation-states are weaponizing AI and amplifying their ability to cause harm, with global attack attempts more than doubling in 2023, increasing 104%. Put simply, cyberwarfare has evolved into an intelligence arms race.

Such attacks are not just about data breaches or financial gains; it's a calculated assault on public trust, destabilizing elections, economies, crippling entire commercial and societal systems and manipulating populaces at large. The recent wave of ransomware attacks on Sweden's government services and critical infrastructure by Russian threat actors – with the country on the verge of joining NATO – says it all.

And 2024 adds a terrifying new dimension: half of the global population will head to the polls across 76 nations this year. And **39%** of those surveyed believe cyberwarfare could affect the integrity of an electoral process. The very foundations of democracy are at risk. Chinese-linked cyber actors even made a desperate last-minute push to derail Taiwan's elections in January 2024, just falling short in attempts to distort the democratic process.

Armis now revisits its findings from the 2022-2023 State of Cyberwarfare and Trends Report, analyzing how known attacks, methodologies, and sentiment towards cyberwarfare has evolved. This latest study surveyed over 2,600 IT decision-makers globally across the United States (U.S.), the United Kingdom (UK), France, Germany, Canada, and Singapore (*see Methodology for more details*) to provide the latest comprehensive picture of the current crisis.

KEY FINDINGS

ENEMIES AT THE GATE: A GLOBAL SNAPSHOT

Forty-one percent of IT leaders say the cyberwarfare threat has increased due to geopolitical tensions with China, Russia and their proxies. Previous Armis research observed an increase in cyberattacks originating from Chinese (.cn) and Russian (.ru) domains. Manufacturing saw .cn and .ru domains contributing to an average of 30% of monthly attack attempts. These targeted attacks suggest a deliberate strategy to disrupt the way we live, cripple crucial manufacturing processes, take life-giving systems offline and to destabilize entire economies.

What's more shocking is an erosion of trust in traditional defenses. **Forty-six percent believe** their nation's governments are incapable of protecting citizens and organizations from cyberwarfare threats. **Nearly half of respondents think we're on our own.** And yet, the war is raging on all around us.

In response to the statement, *"China's state-sponsored cyber operations pose a greater threat to global security than those of Russia,"* **44% agreed**, highlighting concerns about China's advanced offensive capabilities.

Thirty-nine percent remained unsure, acknowledging Russia's destructive potential. North Korea also emerges as another threat, with **44% believing** its cyber capabilities have the potential to instigate a full-scale cyberwar that could cripple critical infrastructure.

However, it's not just about cyber espionage; it's about how much more vulnerable the West is to disruption of our lifestyle than the East. Simple things like the interruption of streaming, social media, or internet services can severely damage the way we live and be used to exploit public opinion over prolonged periods of time.

And what better year than 2024 to try and sway public opinion, with a record number of elections happening worldwide. From the U.S. presidential race to elections in Europe and India, the democratic process is under threat, with bad actors attempting to sow discord and destabilize the integrity of the political process. We've seen it already with AI deepfakes affecting the elections in Slovakia, Nigeria, and recent impersonations of U.S. President Joe Biden.

The UK has already been warned of Russian groups like Star Blizzard's cyber campaigns against democracy, causing doubts about the legitimacy of an election result. In the U.S., however, officials are confident the 2024

election will be the 'most secure' in history. Yet, previous Russian interference in the 2016 election – combined with the current lack of faith in governments – only further strengthens the seeds of discord that have already been planted.

AI IS SUPERCHARGING CYBERWARFARE

AI is swiftly becoming the driving force behind cyberattacks. From being used on the frontlines of the Russia-Ukraine cyberwar to Iran-backed hackers interrupting UAE, UK, and Canadian programming with fake news and an AI-generated anchor, AI is being weaponized to manipulate information on a massive scale. This is before we discuss the black market commercial applications of these tools. If you thought Ransomware as a Service (RaaS) was bad, wait until you see what happens next.

Disinformation campaigns that disrupt and destabilize economies will escalate with the rise of Large Language Models (LLMs), deep fakes, sophisticated voice replication and social media technologies. Deepfakes disguised as top journalists' reports are spreading like wildfire online, raising concerns about manipulated media as a major threat in this critical election year. **Globally, 42%** of IT leaders already believe cyberwarfare could target the media, while **19% remain unsure.**

Armis Labs further identified several threat actors using AI for advanced cyber capabilities:

> **Forest Blizzard (APT28):** This Russian-affiliated group has used AI services to augment its cyber espionage capabilities on sensitive technologies such as satellite communication protocols and radar imaging.

> **Emerald Sleet (Kimusky):** North Korean hackers are using generative AI to conduct sophisticated cyberattacks to circumvent traditional security measures and infiltrate sensitive networks with alarming precision.

> **Crimson Sandstorm (Imperial Kitten):** Iranian threat actors are using AI to streamline their offensive operations, ranging from generating code snippets for malware development to creating deceptive phishing emails.

> **Charcoal Typhoon (Aquatic Panda) and Salmon Typhoon (Maverick Panda):** Chinese state-affiliated groups are using LLMs as an intelligence tool and have employed AI for many purposes, including vulnerability research, script generation and linguistic analysis, conducting large-scale cyber reconnaissance and sophisticated attacks.

The use of AI underscores the evolving threat landscape and highlights how it will continue to supercharge the volume and impact of cyberwarfare. Reinforcing again, why the importance of protecting your entire attack surface is critical.

TIP OF THE ICEBERG: A THREAT FAR GREATER THAN WE THINK

Last year's Armis State of Cyberwarfare and Trends Report revealed IT and security professionals disclosed one or more cybersecurity breaches. This trend has not stopped. Now, organizations have been breached an average of **2.14 times in the past year.** Nearly **half (48%) globally** have experienced one or two breaches, while **22% admit** to having suffered more than two. Many still under-report attacks for a variety of reasons.

Larger organizations with more complex networks appear to be prime targets, as **32% of organizations with 1,750-1,999 employees** report experiencing more than two breaches, compared to **19% for smaller companies with 1,000-1,249 staff.** Certain sectors are worse off than others:

- **Financial services:** 41% report over two breaches.
- **Medical/healthcare/pharmaceutical:** 37% report over two breaches.
- **Government/public sector:** 30% report over two breaches.

The harsh reality? It's probably much worse than the leading professionals consider because so many organizations are blind to their own vulnerabilities. **Less than half (49%)** of organizations claim complete visibility of all network-connected assets. Research highlights that if an organization's attack surface is not being fully monitored it introduces significant exposures and unseen cybersecurity risks.

Armis Labs has also seen an **increase in the combination of weaponized vulnerabilities** being used by threat actors in a single attack. Before the recent international task force cracked down via Operation Cronos, ransomware group Lockbit used a ProxyShell exploit chain (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207), the PaperCut exploit (CVE-2023-27350) and the Citrix Bleed vulnerability (CVE-2023-4966). Threat actor group Akira still uses a combination of Cisco ASA vulnerabilities, VPN vulnerabilities and remote access vulnerabilities (ConnectWise), sometimes going unnoticed.

Bring Your Own Device (BYOD) and Shadow IT also expand the attack surface further, often going unnoticed by security teams because they're overwhelmed by a deluge of data. Bad actors are exploiting that. The frequent breaches we witness are often avoidable, but in the chaos of a cyberwar, prioritizing resources remains a complex challenge for many. More organizations will regrettably fall victim.

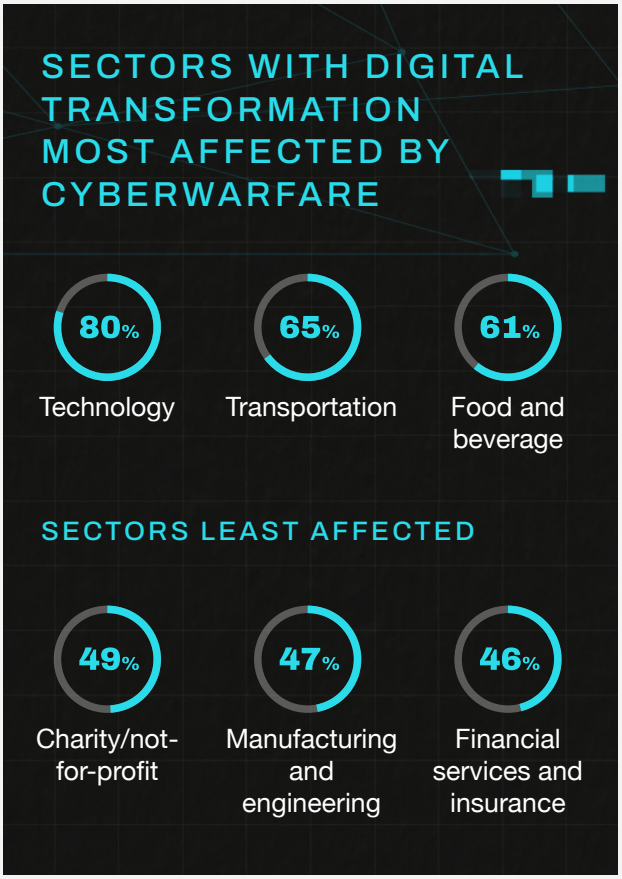
THE CRIPPLING IMPACT OF CYBERWARFARE: INNOVATION STALLED, ECONOMIES DISRUPTED

Since our previous report, the economic impact of such attacks has become far worse. The impact of cyberwarfare extends beyond stolen data and disrupted operations and is stifling innovation, putting critical infrastructure at risk as well as hindering economic growth across the globe. Is it any wonder why some economies are struggling to grow sufficiently?

60% of IT leaders report that digital transformation projects have stalled or been scrapped entirely due to cyberwarfare risks. This marks an increase from 55%, highlighting the escalating threat and its stranglehold on innovation.

A predicted $3.4 trillion will be spent annually on digital transformation by 2026. Cyberwarfare threatens to grind this to a halt, as the fast array of programs in play today, did not consider 'cybersecurity' to be a key driver. Over half of respondents across the globe report it has already stopped their digital transformation projects:

- Singapore: 71%
- France: 65%
- UK: 64%
- US: 54%
- Germany: 50%



The technology sector, unsurprisingly, bears the brunt of this attack, with **80% of IT leaders** reporting stalled digital transformation projects. With cyberattack examples such as those on a software company in Germany; to a ransomware attack on a technology company in Singapore, these incidents over the last twelve months all translate to stifled innovation, hampered efficiency, and, ultimately, a stagnating global economy.

Worryingly, Armis Labs recently found threat actors like the **Houthi-linked OilAlpha group** combining social engineering and malicious mobile apps for disguised espionage attacks across the Arabian Peninsula. While innovation

may be stalling for many of us, bad actors continue to increase their innovation and technological prowess. There is no stagnation happening in the dark world of cybercrime and cyberwar.

HEALTHCARE IN THE CROSSHAIRS

Out of all sectors, healthcare has found itself on the front lines (once again), with threats jeopardizing patient safety and disrupting the provision of vital care. In 2023, healthcare organizations saw a consistent month-over-month increase in attack attempts of 13%. Internet of Medical Things (IoMT) devices like imaging workstations witnessed increased risks in 2023 while nurse call systems remained one of the riskiest medical and IoT devices in clinical environments. And it's a sector that still relies on legacy technology, with 12% of the industry still using End-of-Support (EoS) Operating Systems (OS).

Attacks are only going to escalate for this sector, with various nation-state threat actors making a habit of going after healthcare providers looking to steal sensitive data or cause maximum disruption. After all, malicious actors know the sector is woefully under-staffed and under-resourced and primed for nation-state disruption.

ZOOMING IN

44% of healthcare organizations are worried about the impact of cyberwarfare.

Over 51% already report experiencing a cyberwarfare incident.

37% have suffered more than two attacks.

26% experienced increased threat activity in the past six months.

35% don't think their organization has allocated sufficient budget to aspects of cybersecurity.

Despite this knowledge, preparedness remains ineffective. **Only 30%** report dedicating **16-20% of their IT budget to cybersecurity**, potentially leaving them vulnerable.

"While legacy systems remain part of the threat, it's not always so simple to upgrade. Medical devices are intricate parts of a larger system and it isn't as simple as replacing an MRI machine or CT scanner, particularly for a sector that constantly faces budget cuts. Therefore, attack surface visibility is a foundational element for strong hygiene practices. Security controls such as segmentation remain critical not only for individual assets, but also for securing entire patient care delivery systems to effectively minimize cyberattacks and care disruptions."

Mohammad Waqas,
CTO of Healthcare at Armis

Armis Labs further reported a **notable uptick in successful cyberattacks** targeting companies that use Operational Technology (OT) and Internet of Things (IoT) devices, like those in healthcare and public health. These disruptions highlight the escalating vulnerability to public safety and national security. Other sectors were also affected, such as manufacturing, critical infrastructure and information technology, emphasizing that no one is safe.

BOARDROOMS ARE STRUGGLING WITH HOW TO RESPOND TO THE PROBLEM

Amidst all this, there's another more distressing trend: complacency at the very top. Previously, 76% of IT leaders reported boards were actively instilling a culture of awareness and preparedness for cyberwarfare. Now, that number has **dropped significantly to 51%** - a dangerous regression in leadership focus – when the opposite is needed now more than ever before.

This lack of boardroom engagement is particularly concerning in Germany, where **31% of respondents disagreed** with the following question: *"The board of directors are changing the organization's culture towards cyber security in response to the threat from cyberwar."* And yet, Germany remains under siege by Russian propaganda while also failing to protect critical infrastructure from countless cyberattacks by suspected state-backed actors.

The lack of a "culture of cybersecurity" across many organizations is a recipe for disaster. In the face of such existential threats, this knee-jerk reaction puts entire organizations at risk.

IT LEADERS ARE AT A CYBERSECURITY CROSSROADS

"Would you consider your organization prepared to handle cyberwarfare and respond to related threats?" In all sectors surveyed, at least **94% of IT leaders** agreed, and those in Germany expressed **100% confidence**. While many express unwavering certainty in their organizations' preparedness, the data says otherwise. Is this delusion or simply optimistic thinking?

- **More than one in 20 (6%)** IT leaders admit they're either in the process of developing a cyberwarfare plan or don't have one at all.
- Response strategies are patchy at best, with **only 52%** having any form of a contingency plan.
- This drops even lower in crucial sectors like **financial services and insurance (38%)** and **telecoms (37%).**

Just **13% of IT leaders** worldwide report having a validated, proportionate plan in place to deal with cyberwarfare. Whereas **34% admit** the plan is communicated but has not been validated and **12% reveal** a plan is in place but has not yet been practiced. Put simply, organizations are only setting themselves up for failure.

This lack of practical preparedness extends to reporting procedures too, with nearly a **fifth (19%)** unsure of who to contact in the event of an attack. Barely **half of IT leaders (49%)** believe employees of their organization would know who to speak to if they noticed suspicious online activity, with **25% certain** their colleagues are unaware of the reporting process.

Beneath this facade of confidence lies a fragile security posture. Almost **half (46%) of IT leaders** say they're unconcerned or indifferent about the impact of cyberwarfare; a **13% increase** from the previous survey, when only 33% gave the same response.

Yet it is our belief, it's not indifference but rather a result of being overwhelmed. A lack of automation has left 29% of cybersecurity teams feeling overwhelmed, hindering security and IT professionals from effectively remediating or prioritizing threats. Many remain unaware of the help that is available to them.

Faced with a deluge of information, the mounting pressure to maintain constant vigilance and limited resources, it's easy to understand why some IT leaders are overloaded and share that they are indifferent.

However, this is not an excuse for inaction. The risks associated with cyberwarfare, as acknowledged by the very same IT leaders who highlight their vulnerabilities, necessitate a swift and decisive response. Particularly when asked: "***What is most at risk in the event of a cyberwarfare attack on your organization?***"

"The sheer volume of data breaches, coupled with the difficulty of proactively identifying and prioritizing the right efforts in prevention of the next likely attack can create a sense of fatigue and helplessness among technology leaders. They're bombarded with information on threats, vulnerabilities and potential solutions, making it difficult to prioritize and implement effective defenses if they do not have the right solutions in place."

Curtis Simpson,
CISO and CAO at Armis

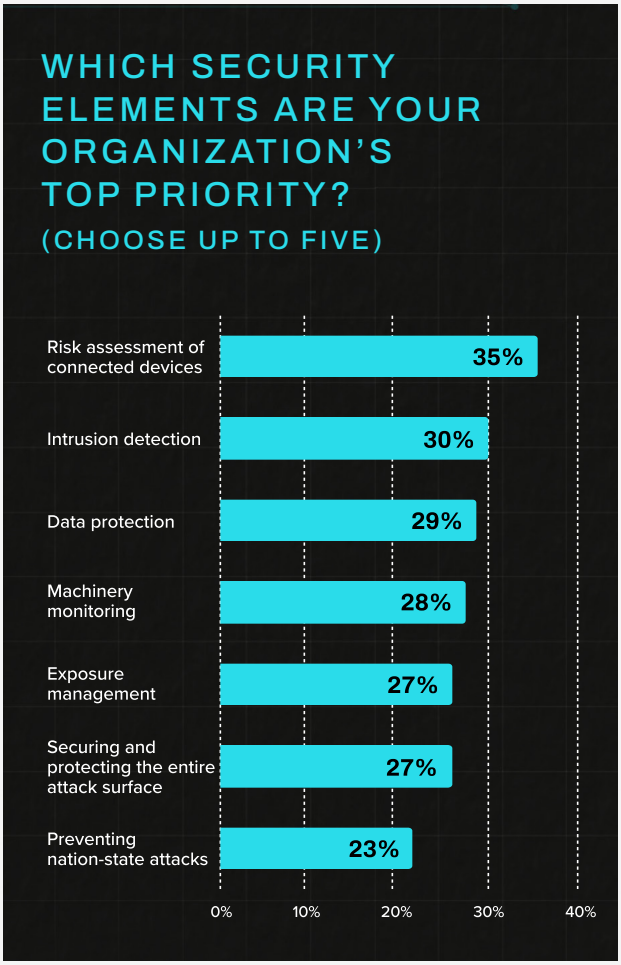
- Databases/personally identifiable information (PII): 54%
- Intellectual property: 51%
- Connected hardware and software: 47%
- Operational downtime: 24%
- Critical infrastructure: 19%

CYBER DEFENSES ARE BEING STARVED

The state of cybersecurity funding globally can be summed up in one word: inadequate. The triad of effective cybersecurity – people, programs, and processes – remains underfunded across the board, with only **53%** believing their organizations allocate sufficient budget to these critical areas.

Almost a **quarter (22%)** say this isn't the case. The figure worsens in **France to 30%**, despite industrial cyber espionage being a major concern for France's National Cybersecurity Agency (ANSSI) ahead of the Paris 2024 Olympics, a perfect opportunity to destabilize and wreak havoc on a global stage.

But the problem goes beyond underfunding. Organizations struggle with prioritization, spreading themselves too thin across various security elements with no clear focus, weakening their overall cybersecurity posture.



Despite being a critical security measure, preventing cyberwarfare attacks ranks low on the priority list. It was chosen by fewer than a **quarter of respondents (23%)**. In the U.S., this **drops further to 18%**, in spite of growing threats like the Iran-backed CyberAv3ngers escalating campaigns against U.S. critical infrastructure or China's cyber-espionage capabilities being referred to as "the 'defining threat' of our time" by top U.S. cybersecurity officials. This lack of prioritization, coupled with insufficient funding, creates a dangerous situation for organizations across the globe. It also creates the perfect environment for bad actors and rogue nations to wage war.

READY TO FIGHT BACK

Despite this, there's a recognition of the need to fight back. **Forty-two percent of respondents** acknowledge the prevalence of preemptive cyber strikes against potential adversaries as a legitimate form of defense in the digital age.

With this in mind, IT leaders are also increasingly seeking external support for defense. **Almost 79% plan** to contract external cybersecurity providers within the next two years, compared to the **51% who currently** rely on such expertise. This signifies a growing recognition of the need for professional guidance in navigating the complex world of cyber defense.

Perhaps a growing realization that you should not try to go it alone is emerging.

KEY REGIONAL FINDINGS

While the global picture may seem clear, there are some key differences between regions. Here's a country-by-country snapshot of these findings.

UNITED STATES

33% of IT leaders say the cyberwarfare threat has increased due to geopolitical tensions with China and Russia.

53% of organizations say China poses a greater threat to global security compared to Russia.

40% believe a cyberwar could affect the integrity of an electoral process.

52% say that North Korea's cyber capabilities have the potential to instigate a full-scale cyberwar.

UNITED KINGDOM

90% believe their organization is prepared to handle cyberwarfare and respond to related threats.

16%, however, say their organization has suffered more than two cybersecurity breaches.

45% of organizations say Russia poses a greater threat to global security compared to China.

52% of IT leaders in the UK believe their nation's government can't protect citizens and organizations from cyberwarfare.

FRANCE

32% of IT leaders say their organization has suffered more than two cybersecurity breaches.

65% of IT decision-makers claim their organization's digital transformation projects have been paused or pulled due to the threat of cyberwarfare.

33% think a cyberwar could affect the integrity of an electoral process.

30% say their organization does not allocate sufficient budget to cybersecurity.

GERMANY

100% of IT leaders believe their organization is prepared to handle cyberwarfare and respond to related threats.

Yet, **only 46% of German businesses** say their organization has a contingency plan in place if cyberwarfare is detected across their network.

50% of IT decision-makers claim digital transformation projects have been paused or pulled due to the threat of cyberwarfare.

48% of organizations say Russia poses a greater threat to global security compared to China.

SINGAPORE

51% of IT decision-makers in Singapore believe cyberwarfare could target the media (national TV channels, radio stations, and publications).

43% of IT leaders believe their nation's government cannot protect citizens and organizations from cyberwarfare.

Almost half (49%) believe cyberwarfare could affect the integrity of an electoral process.

Yet, **55% say** they are unconcerned or indifferent about the impact of cyberwarfare.

CANADA

41% of organizations say China poses a greater threat to global security compared to Russia.

42% of businesses say that North Korea has the potential to instigate a full-scale cyberwar.

24% believe the use of cyberattacks by Iran is a justified response to perceived aggression from Western nations.

37% of IT leaders believe preemptive cyber strikes are a legitimate defense for companies and governments.

SWITCHING TO A COMPREHENSIVE SECURITY POSTURE WITH ARMIS

Cyberwarfare causes significant damage to both critical infrastructure and other unsuspecting organizations whilst also destabilizing vital processes and economies worldwide. In this kind of cyberwarfare, no organization is off the potential target list. Cyberwarfare attacks are easy to plan, often easy to execute, and can cause major damage; more than many forms of conventional warfare. That's what makes this such an effective form of warfare.

Information has become the ultimate weapon in cyberwarfare. With tens of thousands of physical and virtual assets connected to any organization's networks on an average day, and over 40% remaining unmonitored, it's time organizations start defending against current threats while also positioning themselves for the dynamic challenges that lie ahead. It's time to act, to prepare your organization, so that it can be better, more resilient and better prepared for what is yet to come.

Proactive planning and response demands vigilance from everyone, not just governments and militaries. Businesses and individuals must take action to understand their attack surface, likely attack vectors and TTPs, and then take definitive action to better defend themselves from rapidly evolving cyber threats. By recognizing the pervasiveness of these threats and that every link in the digital chain is vulnerable, only then can organizations begin to mitigate the risks and safeguard our digital world from cyberwarfare.

Cyberwarfare demands a swift and decisive shift from solely reactive postures to a comprehensive security strategy. Managing the attack surface becomes crucial. Armis equips organizations with Armis Centrix™, the cyber exposure management platform. It is powered by the Armis AI-driven Asset Intelligence Engine, which sees, secures, protects and manages billions of assets around the world in real time.

ARMIS CENTRIX™

ARMIS CENTRIX™ FOR ASSET MANAGEMENT AND SECURITY

continuously discovers all of an organization's assets, including IT, IoT, cloud and virtual, managed or unmanaged.

ARMIS CENTRIX™ FOR OT/IOT SECURITY

secures manufacturing and critical infrastructure by achieving full visibility across IT, OT and IoT assets. Control, monitor and protect critical OT assets and critical infrastructure using the industry's most advanced cyber exposure platform.

ARMIS CENTRIX™ FOR MEDICAL DEVICE SECURITY

discovers and secures every clinical asset and tracks inventory utilization. Get complete visibility and maximize security across all managed or unmanaged medical devices, clinical assets, and the entire healthcare device ecosystem.

ARMIS CENTRIX™ FOR VULNERABILITY PRIORITIZATION & REMEDIATION

enables vulnerability managers to see all vulnerabilities and prioritize based on vulnerability criticality and business risk.

ARMIS CENTRIX™ FOR ACTIONABLE THREAT INTELLIGENCE

is an early warning, AI-based system that leverages dark web, dynamic honeypots and HUMINT to anticipate threats, understand their potential impact, and take preemptive action to neutralize them, effectively moving the security posture from defense to offense.

WHO ARE 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.

CYBER EXPOSURE MANAGEMENT EXPLAINED

As technology continues to advance and become more interconnected, the attack surface for potential vulnerabilities also expands. This has led to the need for effective cyber exposure management solutions to mitigate risks and protect against potential cyberattacks. Cyber exposure management involves the continuous monitoring and mitigation of cyber risks across an organization's entire digital infrastructure. This includes identifying, assessing and prioritizing potential vulnerabilities and threats in real-time.

As a leader in agentless device security, Armis provides comprehensive visibility, security and control over all connected devices within an organization's network. With Armis, organizations can gain a complete understanding of their cyber exposure and take proactive measures to secure their digital infrastructure. Armis' AI-powered platform continuously monitors and analyzes device behavior to identify potential risks and prioritize them based on criticality. This allows organizations to focus their efforts on managing the most significant threats and vulnerabilities, reducing response times and minimizing potential damage.

Additionally, Armis offers automated threat remediation capabilities, allowing for real-time response to potential attacks. This ensures that organizations can quickly and effectively mitigate any risks before they escalate into larger cyber incidents.

METHODOLOGY

The research and meta-data analysis was conducted globally by Censuswide in two parts.

The first survey was a sample of over 1,603 IT decision-makers in France, Germany, Singapore, the UK, and the U.S. Respondents work full-time at organizations with over 1,000 employees.

The second survey was a sample of 1,003 IT and cybersecurity professionals based across the UK, U.S., Canada, France and Germany.

Respondents work across industries including:

- Automotive
- Charity/Not-for-profit
- Distribution/Logistics/Transport
- Financial Services/Insurance
- Food/Beverage
- Government/Local Authority/Public Sector Agency
- Manufacturing/Engineering
- Medical/Healthcare/Pharmaceutical
- Oil/Gas/Mining/Construction/Agriculture
- Retail/Wholesale
- Technology
- Telecoms/Cable/Satellite
- Transportation
- Utilities: Energy/Water

Censuswide abides by and employs members of the Market Research Society and follows the MRS code of conduct which is based on the ESOMAR principles.

Dates of research:

- **Survey 1** was conducted between October 16, 2023, and October 30, 2023
- **Survey 2** was conducted between February 20, 2024, and February 23, 2024

THE STATE OF

CYBERWARFARE

Armis, the asset intelligence cybersecurity company, protects the entire attack surface and manages the organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world Armis ensures that organizations continuously see, secure, protect and manage all critical assets.

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 safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011

20240408-1

ARMIS®