Artificial intelligence:

Opportunity or threat for global connectivity?

Weighing the complex impact of AI on enterprise networks



Arelion

Change is happening fast

Arelion's 2024 Disruption report published in mid-2024, revealed that enterprise networks are implementing AI-based solutions at a furious rate.

Results showed that nine out of 10 decision-makers believed they would be using AI-based tools and/or systems to support their network management within 18 months, with half doing so by now.

Such rapid implementation raised some important questions – which this report now seeks to address.



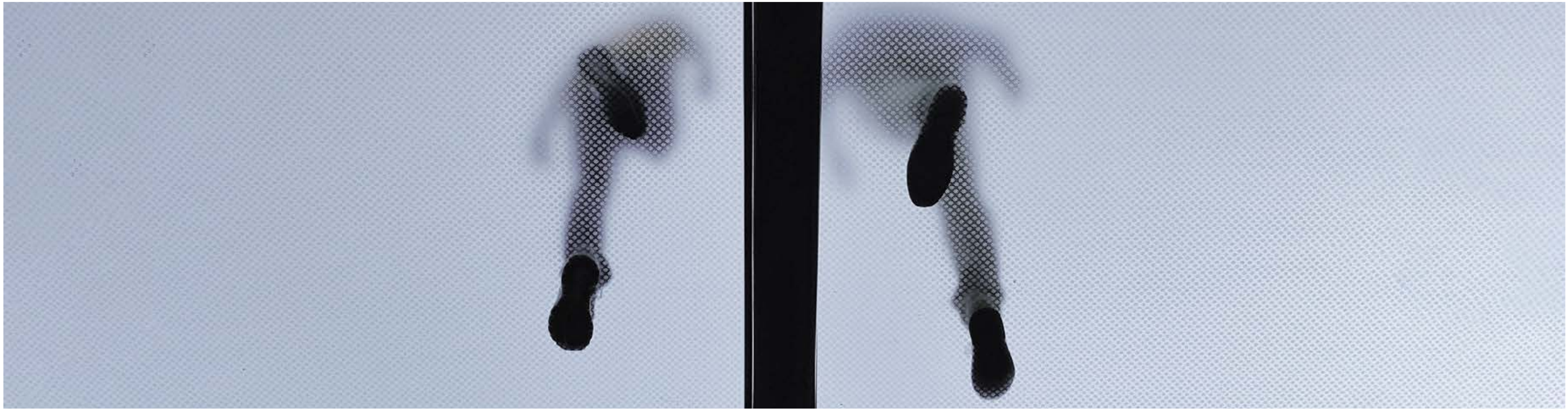
The overarching questions are simple enough: is AI a boon or a burden for businesses? Is it an opportunity for enterprise network operators or a threat to them? The answers are less straightforward. This report highlights the disruptive nature of AI and provides insights into the complex – and sometimes contrary – impacts that enterprise leaders are seeing it have on their organizations and networks.

The report is based on our research survey of senior decision-makers across a range of industry verticals, including Information services, manufacturing/engineering, banking and tech/business services. The respondents all have decision-making roles in companies with over 2,000 employees in four of the world's biggest markets – the US, the UK, Germany and France.





Executive summary



Real benefits already

- AI is living up to the hype that often surrounds it. When measuring the claims for AI against genuine business benefits, a majority of senior network decision-makers (55%) do not believe it has been overhyped. They are already seeing real benefits across their businesses.
- AI is also broadly welcomed when it comes to network operations. Most enterprise leaders (68%) are comfortable with AI taking an increasing role in their network operations, not least, perhaps, because 63% believe it will cut network costs over the next three years.
- But AI is not considered favorably by all. It should be noted that there are some significant regional and industry variations across the survey. For example, relatively large numbers of leaders in France and in the banking sector remain nervous about AI playing a bigger role in their network operations.



The number one network challenge

- Crucially, AI is also raising several major concerns for network operators. These include widespread fears that AI is:
  – Making network operations more complex
  – Leading to a loss of competency and skills
  – Resulting in increased bandwidth consumption.

- Most strikingly, the biggest AI-related threat for network operators is cybersecurity. Leaders in every region and industry sector cite AI-related cybersecurity threats as their #1 network challenge, while almost two-thirds expect DDOS attacks to be largely driven by AI (as opposed to humans) within four years.



Security will still rely on humans

- Further highlighting the complex impacts of AI, leaders recognize that AI facilitates a never-ending cycle of attack and defence. Not only does it pose cybersecurity challenges to their network operations, but it also enables mitigation solutions… and then, in turn, renewed attacks.
- In particular, decision-makers see AI enabling DDOS attack mitigation – primarily through real-time detection and response.
- But overwhelmingly, these leaders also display a chronic lack of faith in current AI-based cybersecurity, with 90% believing that hackers are more likely to trick AI-based cybersecurity tools than those operated by humans.

Arelion

Survey findings

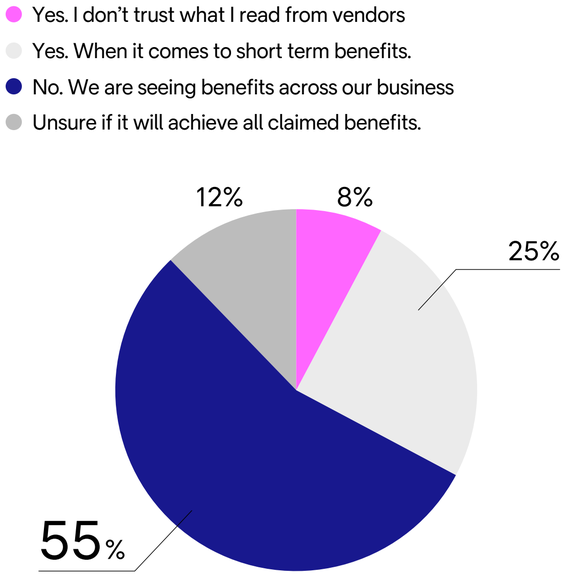


Artificial Intelligence is living up to the hype

In terms of its overall business impact, AI is living up to the hyperbole that often surrounds it. When measuring the claims for AI against genuine business benefits, **most senior network decision-makers (55%) do not believe AI has been overhyped**, because they are already seeing real benefits from it across their business. Significantly, an additional **25% of leaders foresee substantial mid- to long-term benefits from AI**, even though they DO think it has been overhyped in the short-term.

Manufacturers are seeing the greatest benefits (62%) – perhaps because automated, data-driven production systems are increasingly lending themselves to the potential benefits of AI. This finding may also explain why so many **(70%) of leaders in Germany, with its strong manufacturing sector, are seeing AI benefits.**

Have the potential benefits of AI in business been overhyped?

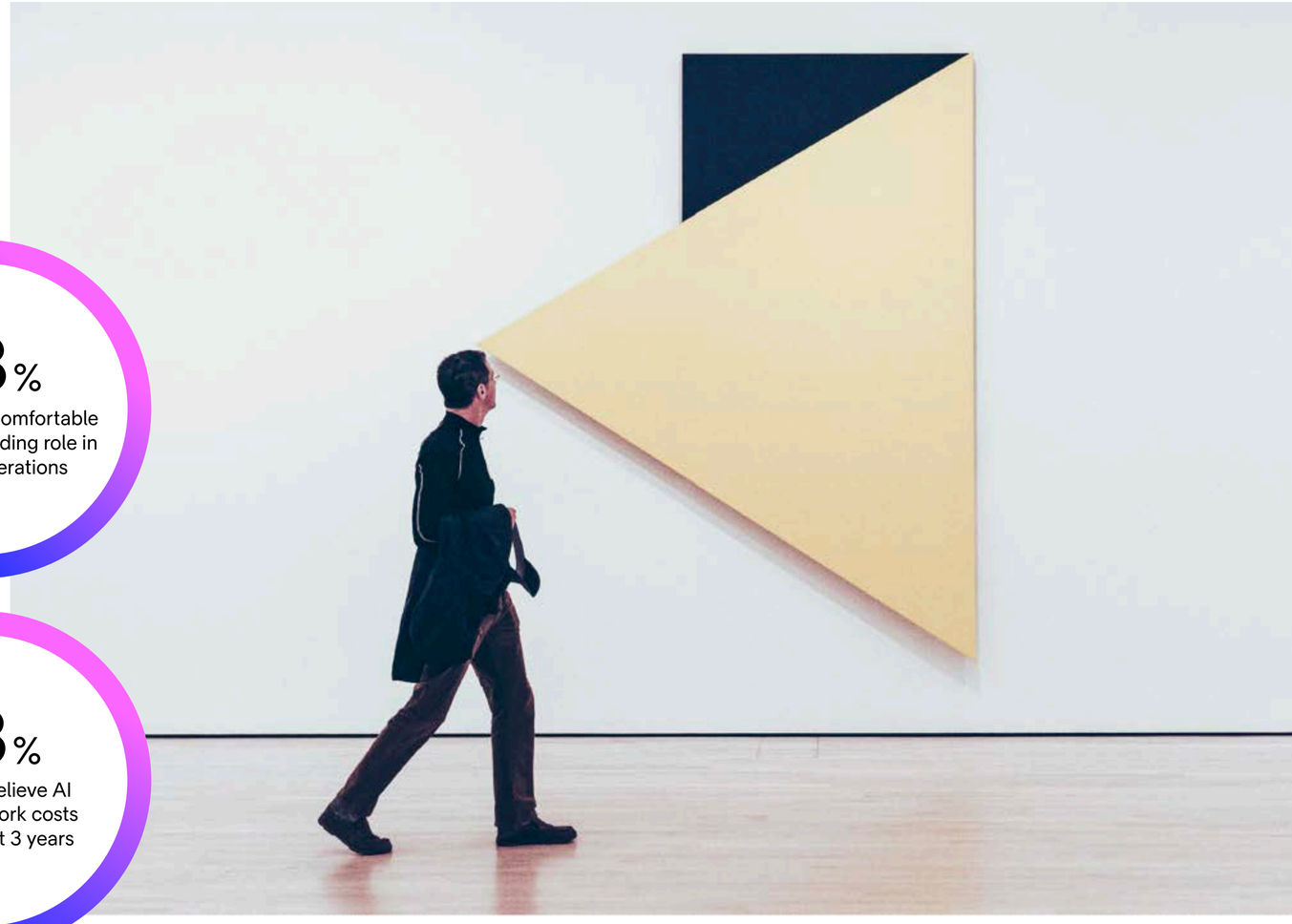




Leaders broadly welcome AI in network operations

Most enterprise network decision-makers (68%) are comfortable with AI taking an increasing role in their network operations. This may well be largely because a similar majority (63%) believe that **AI will cut network costs** over the next three years. Many leaders in the UK (32%), US (27%) and France (25%) are particularly confident AI will cut costs dramatically.

However, **37% of leaders in the banking sector and 35% of those in France are nervous about AI.** In the case of bankers, this could be because they are inherently cautious – their leaders may feel they have most to lose from potential AI vulnerabilities. After all, many have suffered severe cybersecurity breaches in the past.



68%
of leaders are comfortable with AI's expanding role in network operations

63%
of leaders believe AI will cut network costs over the next 3 years

But AI is also raising several major concerns

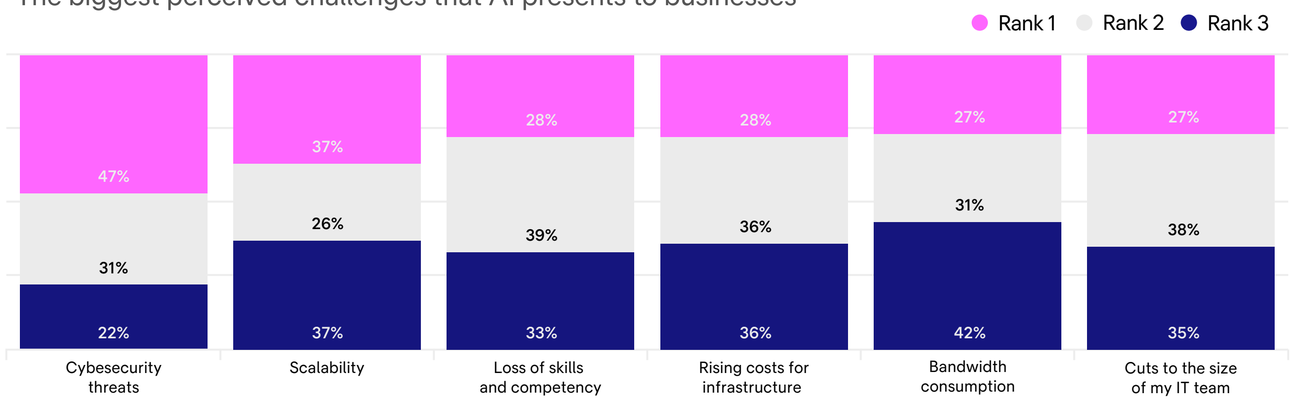
AI making network operations more complex – the view of 70% of leaders widely shared across industry verticals and regions.

AI leading to a loss of competency and skills in the workforce – with 39% ranking it as their second major concern.

Our earlier 2024 report, Building enterprise networks in a disrupted world, found that almost half of the enterprise network decision-makers surveyed (48%) struggle to get staff with suitable skills, including both hardware and software networking skills.

The degradation of human skills due to AI could exacerbate these existing skills shortages even further.

The biggest perceived challenges that AI presents to businesses





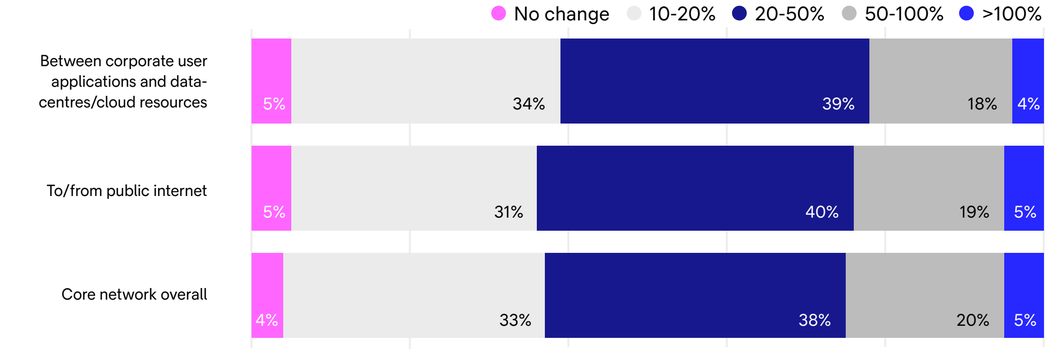


AI is driving bandwidth consumption – with 42% listing it as their third most palpable concern. Business leaders believe that such an increase will be caused by increased network traffic of all types (core network traffic, traffic to and from the public internet, and traffic between corporate users and datacenters/cloud resources).

Specifically, **40% of decision-makers anticipate a 20-50% growth in traffic** to and from the public internet, 39% predict it will be traffic between corporate user applications and datacentres/cloud resources, and 38% say that it will be an increase in their core network traffic.

Almost 1-in-4 leaders predict a staggering 50-100% rise in their core network traffic (UK and Germany), traffic to and from the public internet (UK), and traffic between corporate users and datacenters/cloud resources (France).

Anticipated traffic increase from AI technology and applications per area



Artificial intelligence and the cybersecurity conundrum

—

Highlighting the complex impact of AI, leaders recognize that AI facilitates a never-ending cycle of attack and defence on the cybersecurity battlefield. Not only does it pose cybersecurity challenges to their network operations, but it also enables mitigation solutions... and then, in turn, renewed attacks.

Fundamentally, enterprise network decision-makers in every region and industry sector say that **AI-related cybersecurity threats are their #1 network challenge.**

65% of leaders expect DDOS attacks to be largely driven by AI (as opposed to humans) within four years. Over a quarter (27%) anticipate this happening within just two years.

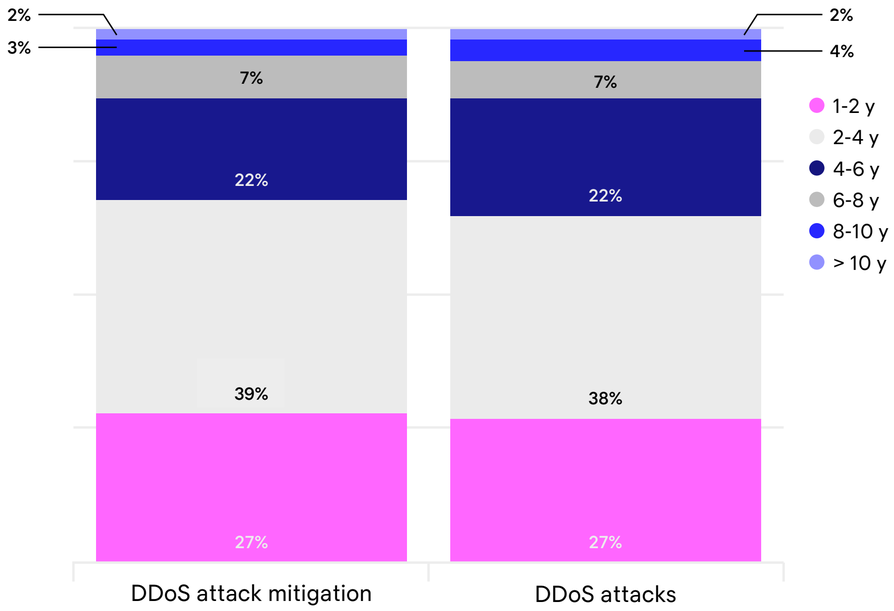
> AI-related cybersecurity threats are the #1 network challenge for enterprise leaders

Perhaps alarmingly, a significant number (25%) say they are **already** facing DDOS attacks specifically engineered to circumvent AI-driven cybersecurity defences with an additional 60% anticipating this occurring within the next two years.

1/4

of leaders say they are **already** facing AI-evasive DDoS attacks

Predicted timeframe for a DDoS landscape that is predominantly driven by AI

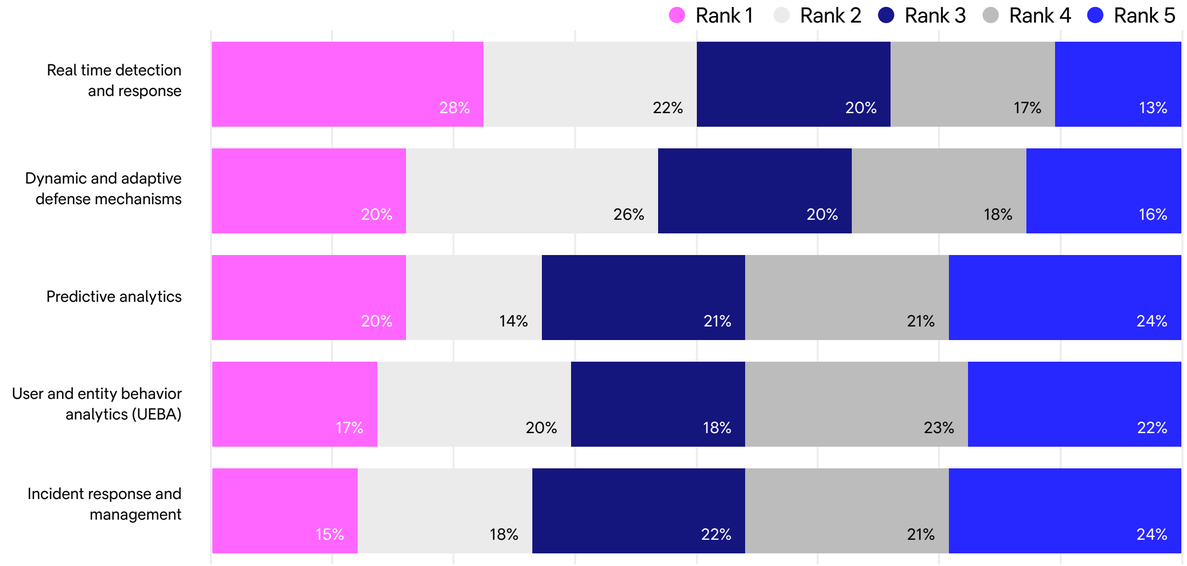




When asked where they felt AI will have the biggest impact on **DDOS attack mitigation**, business leaders predominantly cited real-time detection and response.

The only exception to this was decision-makers in France who elected predictive analysis as the primary most impactful area. Second to real-time detection and response, leaders said that they see AI offering DDOS attack mitigation through dynamic and adaptive defence mechanisms – with **68% of business leaders expecting such mitigation to be largely driven by AI (as opposed to humans) within four years.**

The potential impact of AI on DDoS mitigation

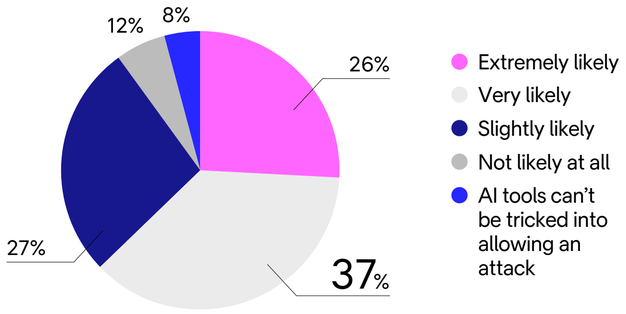


Leaders lack faith in AI-driven cybersecurity solutions

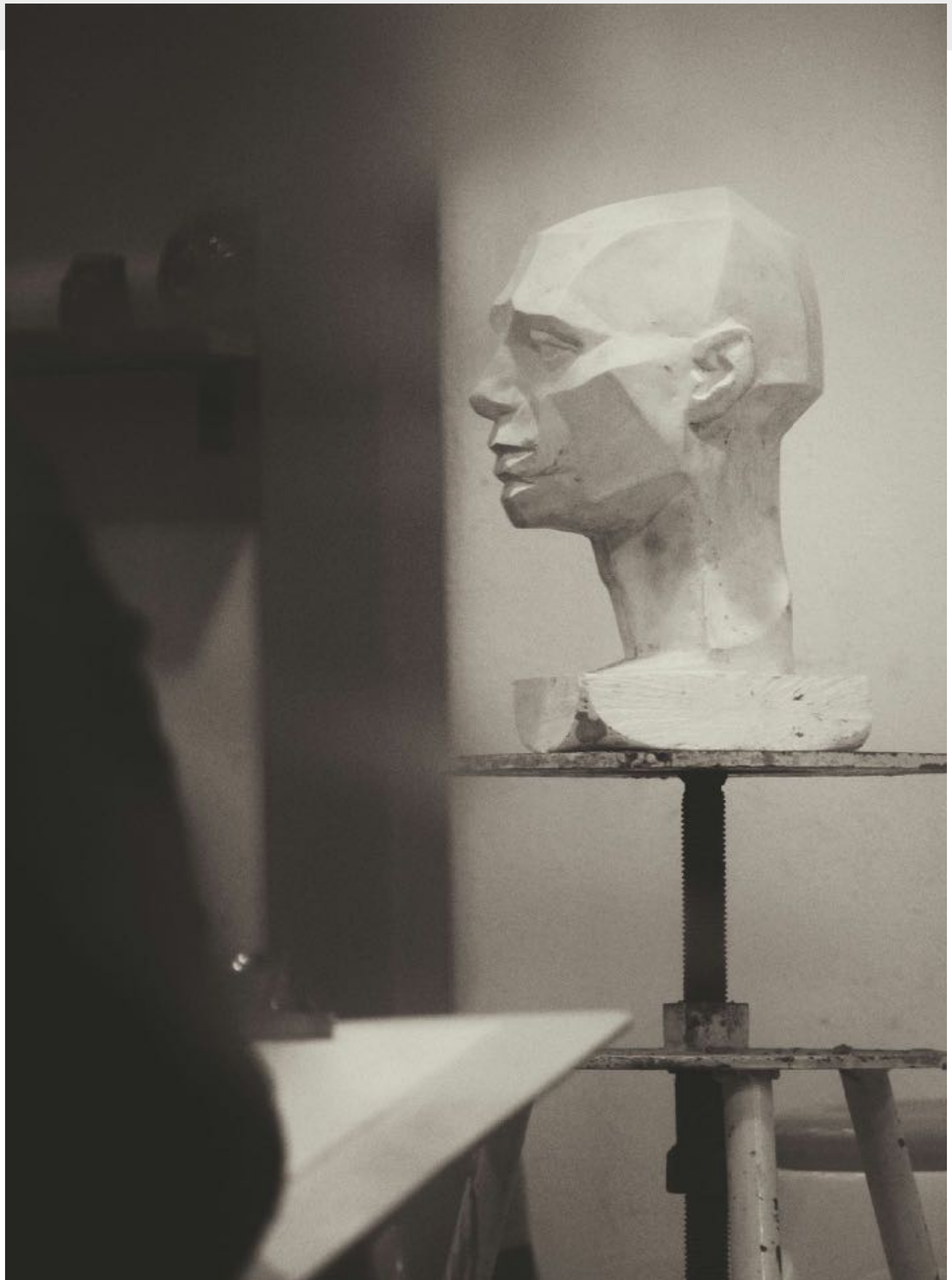
Worryingly, the majority of decision-makers show a chronic lack of confidence in current AI-based cybersecurity, with **90% stating that they believe that hackers are more likely to trick AI-based cybersecurity tools than those operated by humans.** This is particularly true of 34% of US and 29% of UK business leaders.

This finding suggests that the role of **human cybersecurity experts will remain critical** – alongside the need to maintain and upgrade their skills (which many fear may be in decline).

Are AI tools more likely to be exploited by hackers than human-operated systems?



9 out of 10 leaders believe hackers are more likely to exploit AI cybersecurity tools than ones operated by humans



Conclusions



AI is (broadly) a boon for business

—

Our research reveals that AI is generally regarded as something positive by businesses, with a majority of leaders reporting that they are already experiencing benefits from the technology.

AI is also – broadly – welcomed by network operators. It is bringing opportunities, notably, the ability or potential to reduce network operating costs.

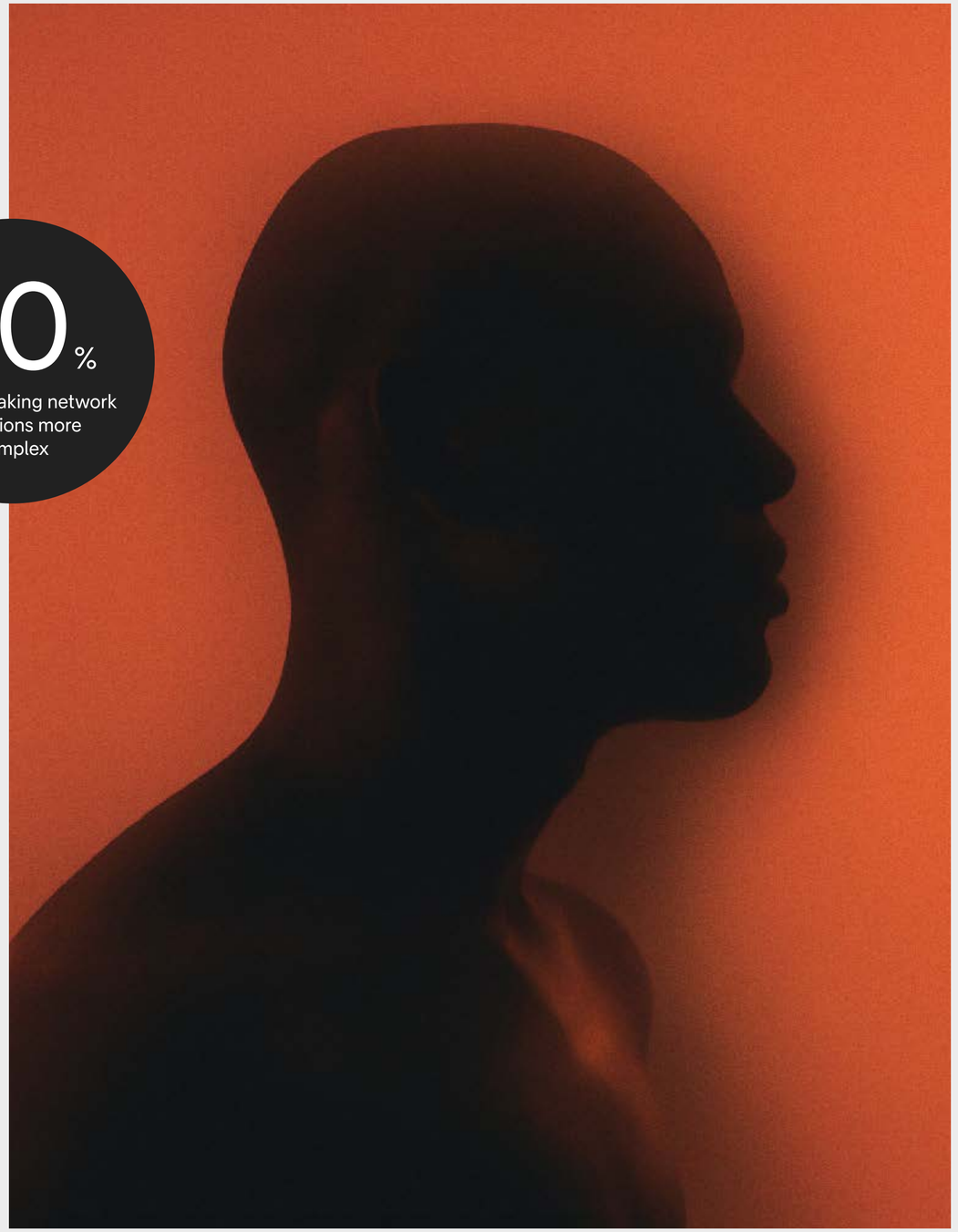


AI brings challenges and solutions

—

Potential AI-related problems include more complex network operations, erosion of human skills, and increased use of bandwidth. Network operators will need to consider remedial action in all three areas. For example, if complexity is not understood and overcome, hoped-for cost reductions may not be realized. If workforce skills are not maintained through adequate recruitment and training, lack of human back-up could prove disastrous if AI-driven solutions misfire. And insufficient network capacity will clearly hamper organizational performance at a fundamental level.

> Lack of human back-up could prove disastrous if AI-driven solutions misfire.



The cybersecurity stakes are high

The most significant AI-related threat is cybersecurity. Network operators face an ongoing war of attrition with cyber criminals. AI already provides many possibilities for bad actors to target areas of vulnerability in a company's defences. They now have the ability to set a series of protocols to attack relentlessly until it eventually overwhelms cyber defences.

But AI also offers cybersecurity solutions. Intelligent automation is as vital to cyber defence as it is to attackers. AI offers the potential for improved DDOS attack mitigation, particularly through real-time detection and response through machine learning and other techniques .

The prospect of endless cyberattack versus cyber defence – with ever more sophisticated and complicated AI tools deployed by both sides – means network operators must be prepared for a permanent struggle. Furthermore, they will need to take a hybrid approach that embraces human skills alongside AI-driven solutions.



Coping strategies will be key

These radical, far reaching impacts of AI mean that enterprise network operators need support. Organizations cannot cope with the complex impacts of AI on their own.

They need assistance in the form of external resources, expertise and collaboration – particularly when it comes to cybersecurity.



Arelion

Implications for enterprises



Enterprises looking to mitigate the evolving cyber threats from AI need to be prepared for the long haul. AI is allowing bad actors to set a series of attack vectors to cycle randomly and indefinitely, and then walk away for as long as their target's technical resources last.

Indeed, this sort of thing is being slowly integrated into the stress test sites – where random carpet bombing is now just another option.

Organizations will, if they are not prepared, have their engineers sitting at a computer, responding for hours on end to the shifting vectors. Eventually they will make a mistake, and the service will go down.



The research suggests that enterprise network decision-makers need to take account of key AI-related issues when considering their network strategy and their choice of network provider.

Enterprise network decision-makers need their network provider to offer:

- **Cybersecurity support** – with sufficient scale, experience, expertise, flexibility and speed of response to help react fast to manage fast-moving cybersecurity threats effectively. It's essential to select a suitably large and capable network provider who can absorb the physical impact of DDoS attacks (of any attack).
- **Automation** - is key both at the volumetric level and also at defending your applications from resource exhaustion.
- **DDOS protection capabilities**, including:
  - Large-scale monitoring capacity.
  - An enhanced level of automation with regards to network adaption and filtering bad actors.
  - Commitment to DDOS protection that quickly adapts to the circumstances, and to develop such technology to defend against hackers who now use AI and other automated techniques to try and overwhelm human engineers.
  - Large-scale network capacity. No matter how much intelligence is put behind an attack, the fact remains that DDOS is a resource exhaustion technique, so to remain secure it is vital to stay ahead in terms of raw resources. A large and capable network provider can absorb the physical impact of DDoS attacks and other cyber threats before they reach you.
- **Independent advice and expertise** – including pan-industry perspectives, resources and clear thinking to unravel increasing complexity in network operations.
- **Support on skills** – helping to nurture in-house workforce talent and offering supplementary external advice and services where necessary.
- **Scalable bandwidth** – offering sufficient network capacity, with flexibility to scale up when required.
- **Geographical spread** – with local knowledge to provide guidance and support in specific markets.
- **A partnership approach** – with a willingness to work collaboratively.

What Arelion is doing to counter AI-generated DDoS threats

Arelion has significantly enhanced the capabilities of its DDOS protection:

- **A doubling of monitoring capacity**
- **An enhanced level of automation** with regards to flowspec filtering and automatic responses in network to attacks
- **Adaptive DDOS: machine learning** is employed in order to real time adapt to hackers using multiple vectors and changing them rapidly (carpet bombing is a key example). Adaptive DDOS is still being developed going forward, and will be directly responding to AI and other automated techniques that attempt to overwhelm human engineers.
- **The sheer volume of capacity in the Arelion network is an effective line of defence in itself.** No matter how much intelligence is put behind an attack, if the resources cannot be raised to break the carriers network, then one of the main tools, volume, is far less effective.

> By far, the greatest danger of Artificial Intelligence is that people conclude too early that they understand it.
>
> – Eliezer Yudkowsky founder of the Machine Intelligence Research Institute

Research methodology

This research was conducted on behalf of Arelion by Savanta, a global leader in digital data collection. An online survey was carried out in the second half of 2024 with 510 industry representatives in the US, UK, Germany, and France.

All participants in the research work for enterprises with more than 2,000 employees. They come from a range of industries, led by:

- Information services: 202
- Manufacturing/Engineering: 85
- Banking: 74
- Tech/Business services: 63.

All participants are involved in decision-making regarding their company's network development strategy (including data center, cloud, and connectivity), with 60% having the last word and final sign-off responsibility for this area.



Arelion

About us

Arelion is a leading light in global connectivity services. Formerly Telia Carrier, we've been keeping the world connected since 1993 and today our global IP backbone, AS1299, is ranked number one in the world.

Our network spans Europe, North America and Asia, with 75,000km of optical fiber and 1,700 MPLS end points serving customers in 128 countries. Our award-winning customer service team supports our expansive customer base, who rely on us for their business-critical services.

Follow us on LinkedIn and X (formerlyTwitter)
Discover more at www.arelion.com