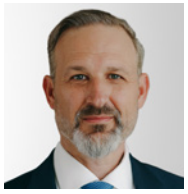
Allianz Global Investors

FEBRUARY 2026

Where AI meets geopolitics and security: key insights for investors



Greg MA Hirt
Global CIO Multi Asset

Jeremy Gleeson
CIO Global Technology Equity

The boom in artificial intelligence is creating exciting growth opportunities but also risks. Here, leaders from our multi asset and global technology teams examine the geopolitical and cyber threats involved with this emerging technology.

Exciting breakthroughs, enormous investments and surging demand for services characterise the booming artificial intelligence (AI) sector. While this technology has huge potential – so much so that we do not yet believe today's elevated valuations fully anticipate the long-term benefits – we also recognise challenges.

In a world that is highly digitally interconnected, a key worry is greater sophistication in cybercrime. Already a major concern for organisations of all sizes, cybercrime is set to become a greater threat as cyber criminals exploit AI tools to make their attacks more effective. In this article, we examine the scale of the AI opportunity, the geopolitical implications of this technology, and offer some insights to help investors ensure their portfolios are resilient against AI-powered cyber risks.

Key takeaways

- We do not currently consider there to be a bubble in AI – the scale of investment and strategic importance of the sector can justify high valuations.
- Amid the benefits, we see risks as malign actors exploit the technology to launch sophisticated cyberattacks.
- We believe the emergence of AI-powered cybercrime should prompt a greater focus on digital risk and cyber resilience.
- Due diligence may include analysing a company's incident history, recovery times, security spend and management responsiveness.

Tech that justifies the hype

Some commentators believe the potential impacts of AI to have been overstated. We do not share this view. In fact, we think the current wave of AI investment is fundamentally unlike the speculative dot com era with which it is often compared.

The AI-related businesses currently attracting investor attention are not start ups raising money on the vague promise of future revenues; they are profitable, cash generating firms reinvesting heavily into chips, data centres, AI infrastructure and application ecosystems. Demand for AI applications is strong and broad.

Another key difference is that the industry is dominated by companies with the scale to fund multi-billion-dollar research and development programmes. This dynamic is self reinforcing: more data, more compute and better models create higher competitive moats.

While it is true that valuations are high, we think they can be justified given sales growth and margins. That's not to say there won't be corrections along the way. But in terms of historical precedent, we would point to the growth of railways and electrification, rather than the dot-com bubble, as the most appropriate comparison. Each of those industries exhibited what we might call "normal" corrections after massive investments in infrastructure and hardware led to overcapacity and price pressure. The infrastructure that was built persists to this day.

The geopolitics of AI

The boom in AI is recognised as strategically important by governments. Against the background of an "AI arms race" with China, government action – for example the US CHIPS and Science Act (2022) and the EU Chips Act (2023) – secures competitive advantages for major players such as Nvidia, Microsoft and Google.

This makes sense from a political point of view. The top US tech companies invest hundreds of billions a year in research on AI, quantum computing, semiconductors and related technologies. These private investments strengthen the technological superiority of the US. The US military is involved too, with measures such as the 2026 AI Acceleration Strategy, which seeks to make the military an "AI-first" fighting force by integrating AI into decision-making processes, operational efficiency and data security.

Other regions recognise the importance of AI, though the approach is not always the same. Europe, for example, has passed the AI Act (2024), which is aimed at limiting harms from this emerging technology. The legislation, the most comprehensive of its kind, has been praised by some while prompting concerns that European businesses could lose out to more loosely regulated jurisdictions.

The impact of AI on cybercrime

Why is AI so strategically important? To fully answer this question is difficult, because the potential of this emerging technology is still

being explored. But cybercrime and cybersecurity are areas where AI is already exerting a significant influence. To give a sense of the scale of this issue, the Allianz Risk Barometer 2026 named "cyber incidents" as the top global risk for companies of sizes for the fifth year in a row (see Exhibit 1), while "artificial intelligence" leapt from tenth to second place in the same survey.

Other data sources echo the finding. "Cyber espionage and warfare" was named the fifth most pressing global risk, over a two-year time horizon, in the World Economic Forum Global Risks Report 2025.

AI is potentially problematic because it gives criminals the ability to automate, personalise and scale attacks. Phishing or spoofing attacks, in which users are tricked into revealing information or providing access to hostile actors, are becoming harder to spot thanks to the power of AI – think "deepfake" videos, for example.

Attacks vary from lower priority raids, for instance in retail or manufacturing industries, to higher priority attacks with systemic implications – such as strikes on power plants and critical infrastructure, or the global banking system. Given that a significant amount of modern warfare today is digital, it is no surprise to learn that many of these attacks are state sponsored and highly organised.

Investment implications of AI cyber risks

For investors, the implications are varied. Asset prices tend to react negatively to cyberattacks, typically based on the reasoning that a successful attack reveals weakness in corporate governance. On top of this are potential regulatory implications,

Exhibit 1

The 10 most important business risks in 2026

Rank		(%)	2025 Rank
1	Cyber incidents (eg, cyber crime, IT network and service disruptions, malware / ransomware, data breaches, fines, and penalties)	42	1 (38%)
2	Artificial intelligence (eg, implementation challenges, liability exposures, misinformation / disinformation)	32	10 (10%)
3	Business interruption (incl. supply chain disruption)	29	2 (31%)
4	Changes in legislation and regulation (eg, tariffs, new directives, sustainability requirements)	26	4 (25%)
5	Natural catastrophes (eg, storm, flood, earthquake, wildfire)	21	3 (29%)
6	Climate change (eg, physical, operational, and financial risks as a result of extreme weather)	19	5 (19%)
7	Political risks and violence (eg, war, political instability, terrorism, polarization, coup d'état, civil unrest, strikes, riots, looting)	15	9 (14%)
8	Macroeconomic developments (eg, inflation, deflation, monetary policies, austerity programs)	14	7 (15%)
9	Fire, explosion*	13	6 (17%)
10	Market developments (eg, intensified competition / new entrants, M&A, market stagnation, market fluctuation)	13	8 (14%)

Source: Allianz Commercial. The 15th annual Allianz Risk Barometer survey was conducted among Allianz customers (global businesses), brokers and industry trade organizations. It also surveyed risk consultants, underwriters, senior managers and claims experts in the corporate insurance segment of Allianz Commercial and other Allianz entities. Figures represent the number of risks selected as a percentage of all survey responses from 3,338 respondents. All respondents could select up to three risks per industry, which is why the figures do not add up to 100%. The full Allianz Risk Barometer survey includes 20 global risks.

* Fire, explosion ranks higher than market developments based on the actual number of responses

which could occupy managers' attention to the detriment of the core business. To some extent, damage to a company's credibility depends on whether the attack has been observed elsewhere – markets tend to punish victims of copycat attacks more harshly on the basis that these businesses ought to have known better.

The impact on valuations can be significant. For example, retailer Marks & Spencer suffered a cyberattack in April 2025 that led to widespread problems in online orders and contactless payment. The share price fell 7% in the following seven days – equivalent to GBP 700 million of lost value.

Another victim was carmaker Jaguar Land Rover. In September 2025, the business was hit by a ransomware attack in which criminals were able to halt production for several weeks, causing delays across its supply chain.

Smaller companies may be especially vulnerable to cyberattacks. They tend not to have big budgets for security and cyber insurance, they may have a high dependence on core systems (whereas large corporations have redundancies and evasion processes), and they typically do not have big PR resources to assist them in handling crises.

For investors, we think the growing cyber risk should prompt a greater focus on cyber resilience when valuing investee companies. Due diligence can encompass a company's cyber posture, incident history, recovery times, security spend and management responsiveness. These can offer valuable clues as to how the investee business will perform when its cyber defences are tested.

Navigating the AI era

In this article, we have focused on the risks associated with AI, but it's important to recognise the opportunities too. For example, as criminals become more sophisticated, so do the resources available for countering them – namely, AI-powered tools to detect and respond to attacks.

Indeed, cybersecurity can itself be seen as an arms race, in which success depends on staying at the forefront of technology. At AllianzGI, our own cyber strategy involves positioning digital risk and resilience as a central unit, with strict protocols on vulnerability management, continuous reduction of legacy IT, and incident detection.

As society continues to reap the benefits of AI, it important to be aware of the threats. One of the best ways an organisation can protect itself is by maintaining a resilient cyber posture.

February 2026 DG-SM

MACS-P-16789331

ADM-5165504