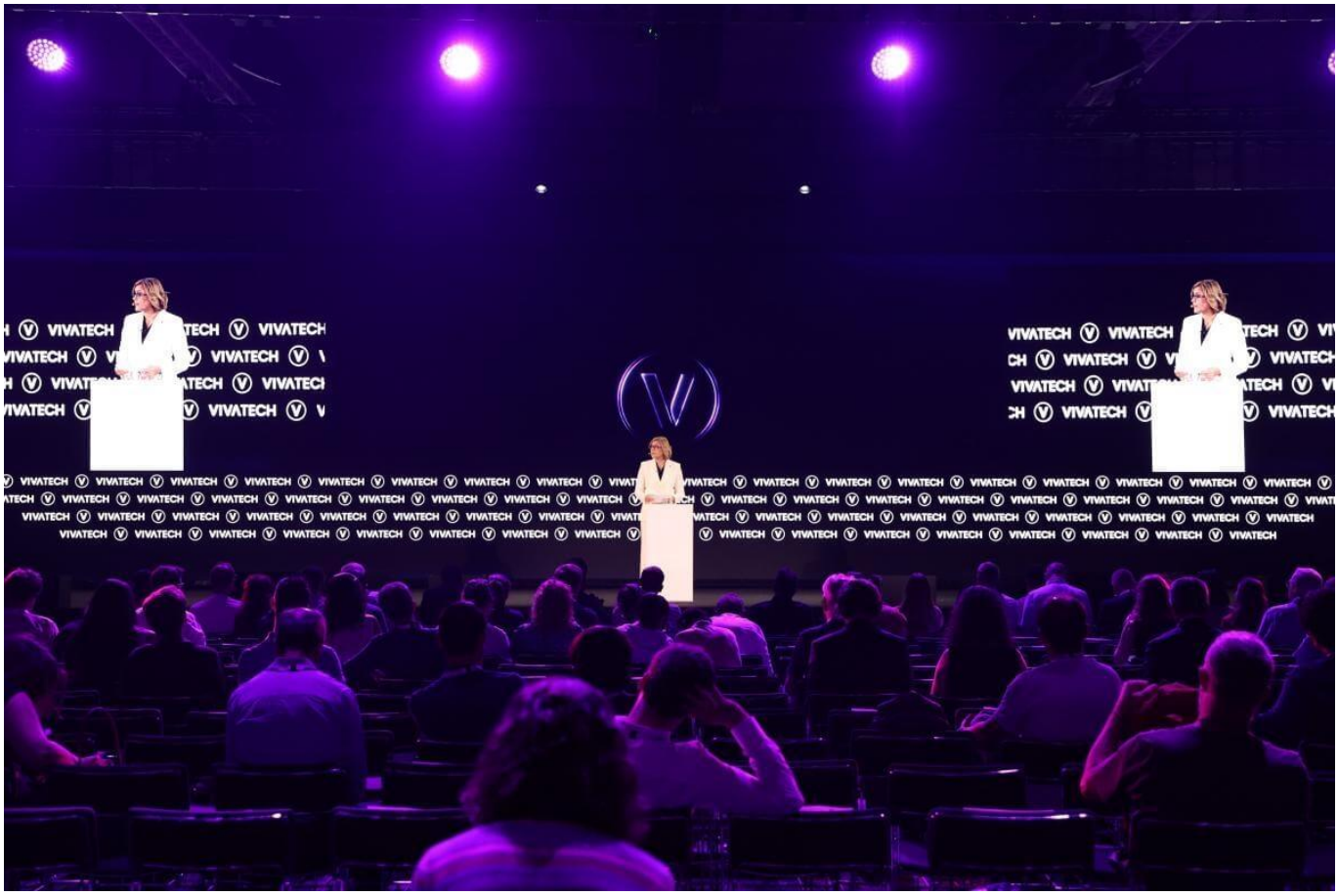
Tomorrow's Affairs
Analysis of today
Assessment of tomorrow

By: Elise Quevedo

VivaTech 2026 and the new reality of AI



If I had to use one word to sum up VivaTech 2026, it would be responsibility. That may sound surprising given that AI dominated almost every major discussion in Paris this year.

As one of the largest conferences in Europe, it showcased some of the world's most influential technology leaders, over ten thousand startups, groundbreaking innovations in robotics and quantum computing, and countless demonstrations of how artificial intelligence will reshape industries over the coming decade.

As the technology industry races ahead at an extraordinary pace, where do security, trust, and governance stand?

A few years ago, many technology conferences focused on possibility. Speakers discussed what artificial intelligence might eventually achieve. Investors searched for the next breakthrough. Companies experimented with early deployments and pilot programmes. I can officially say that that stage has ended.

Organisations now ask how quickly they can deploy AI, how deeply they can integrate it into operations, and how they can avoid falling behind competitors.

We saw that through the many conversations at VivaTech 2026. Many companies are accelerating their AI investments faster than they are strengthening their security foundations.

Jeff Bezos and the rise of physical AI

Jeff Bezos took the stage alongside former NASA astronaut Mike Massimino. The conversation moved far beyond the typical AI discussion that dominates most technology conferences.

Instead of focusing on chatbots, content generation, or productivity tools, Bezos discussed a much larger vision. He spoke about the future of engineering itself.

Part of the conversation focused on Prometheus, the artificial intelligence company that has attracted global attention because of its ambition to create what Bezos describes as an Artificial General Engineer.

Prometheus aims to move AI into the physical world. The goal is to accelerate the design, development, testing, and manufacturing of complex products, ranging from industrial systems to aerospace technologies. Is this the beginning of the next phase of the AI revolution?

The first wave focused on information, the second on automation, and the next on creation.

> Systems can now simulate, analyse, and optimise at speeds that humans cannot match

Artificial intelligence will increasingly influence how we design aircraft, manufacture products, develop medicines, construct infrastructure, and solve engineering challenges that currently require years of research and development. Those are facts.

But this transition carries enormous economic implications. Systems can now simulate, analyse, and optimise at speeds that humans cannot match.

That capability creates extraordinary opportunities for innovation.

It also introduces entirely new categories of risk. Nicole Carignan, Senior VP of Security & AI Strategy and Field CISO at Darktrace, was an expert panellist on the Cybersecurity & Defense programme at VivaTech, and she questioned whether we are investing enough in security.

When AI becomes embedded in physical infrastructure, manufacturing systems, transportation networks, healthcare environments, and critical industries,

cybersecurity becomes a societal issue.

Europe's AI ambition has matured. So has the competition

VivaTech 2026 remains a symbol of Europe's growth. Conversations about artificial intelligence always centre primarily around Silicon Valley and China. Europe often positioned itself as a regulatory voice in the global technology debate.

But now, Europe no longer wants to compete through innovation. Founders, policymakers, investors, and technology executives discussed sovereign AI, strategic autonomy, digital infrastructure, and long-term competitiveness.

Artificial intelligence has become an economic, geopolitical, and national competitiveness issue.

Countries understand that future economic growth will depend on access to advanced computing infrastructure, AI talent, secure cloud platforms, semiconductor technologies, and trusted digital ecosystems.

> Many startups have moved beyond building AI for the sake of AI

This new thinking explains why AI investment has accelerated. The VivaTech startup ecosystem was a perfect example of the quality of the solutions on display. Many startups have moved beyond building AI for the sake of AI.

Instead, they focus on solving real-world challenges across healthcare, climate technology, industrial operations, logistics, financial services, and cybersecurity.

Investors are tired of flashy showcases (unless you are in entertainment technology, in which case that is a bonus!), and so am I.

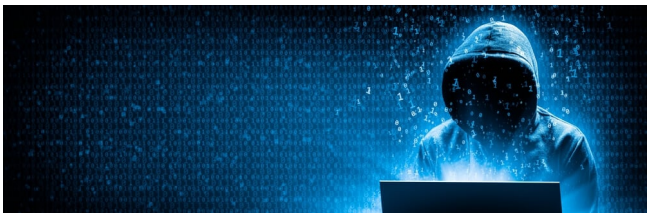
The industry is beginning to mature, and that maturity creates opportunity. Organisations can no longer deploy AI just because competitors are. They need to deploy it responsibly, and here is where cybersecurity comes in.

The cybersecurity question nobody can afford to ignore

According to VivaTech's 2026 Confidence Barometer, 39 per cent of executives admitted that they had shared company information with AI tools they did not fully trust. Can we please stop thinking about that for a second?

People naturally prioritise productivity. They seek efficiency and competitive advantage. When new technologies promise faster results, people adopt them quickly.

The challenge is that when history repeats itself, security often arrives after adoption.



The same technology that helps businesses improve efficiency also helps threat actors improve effectiveness

Without considering the ramifications, businesses integrate AI systems with supply chains, software development workflows, financial systems, customer databases, intellectual property repositories, and strategic planning procedures. New vulnerabilities are created with each integration.

Cybercriminals understand the new reality better than many executives do. Attackers now also use AI to create sophisticated phishing campaigns, automate reconnaissance, generate convincing social engineering attacks, identify vulnerabilities, and accelerate malicious operations.

The same technology that helps businesses

improve efficiency also helps threat actors improve effectiveness.

So, are we investing enough in cybersecurity relative to our investment in artificial intelligence? I don't believe we are.

Many organisations continue treating security as a supporting function while treating AI as a growth function. A company that deploys advanced AI capabilities without strengthening security controls creates future liabilities.

An industry that celebrates innovation while neglecting protection undermines its own progress. Trust is going to become one of the most valuable assets in the digital economy. Because customers trust organisations that protect their data, and investors trust organisations that manage risk effectively. Trust grows from security.

VivaTech 2026 gave us a glimpse into an extraordinary future, but for that to happen, the conversation needs to evolve.

We need to stop discussing artificial intelligence as a standalone technology. We need to discuss artificial intelligence as part of a larger ecosystem that includes cybersecurity, governance, ethics, resilience, and human leadership.

Innovation without protection creates fragility. Innovation with protection creates progress.

Can our commitment to security, trust, and responsibility grow just as fast as innovation? It can, when we do it together.