KPMG

Europe at a crossroads

Europe has a second chance in the chips industry

Maarten Wellens

March 2026

Europe has a second chance in the chips industry

Maarten Wellens is the CFO of Smart Photonics, a Dutch company producing photonic chips. He experiences every day how technological innovation, geopolitics and economic strategy are tightly interwoven.

His role as CFO expands beyond numbers: cybersecurity and digital autonomy are as much a part of his daily agenda as balance sheets and investment rounds. At the same time, the risk of espionage is looming.

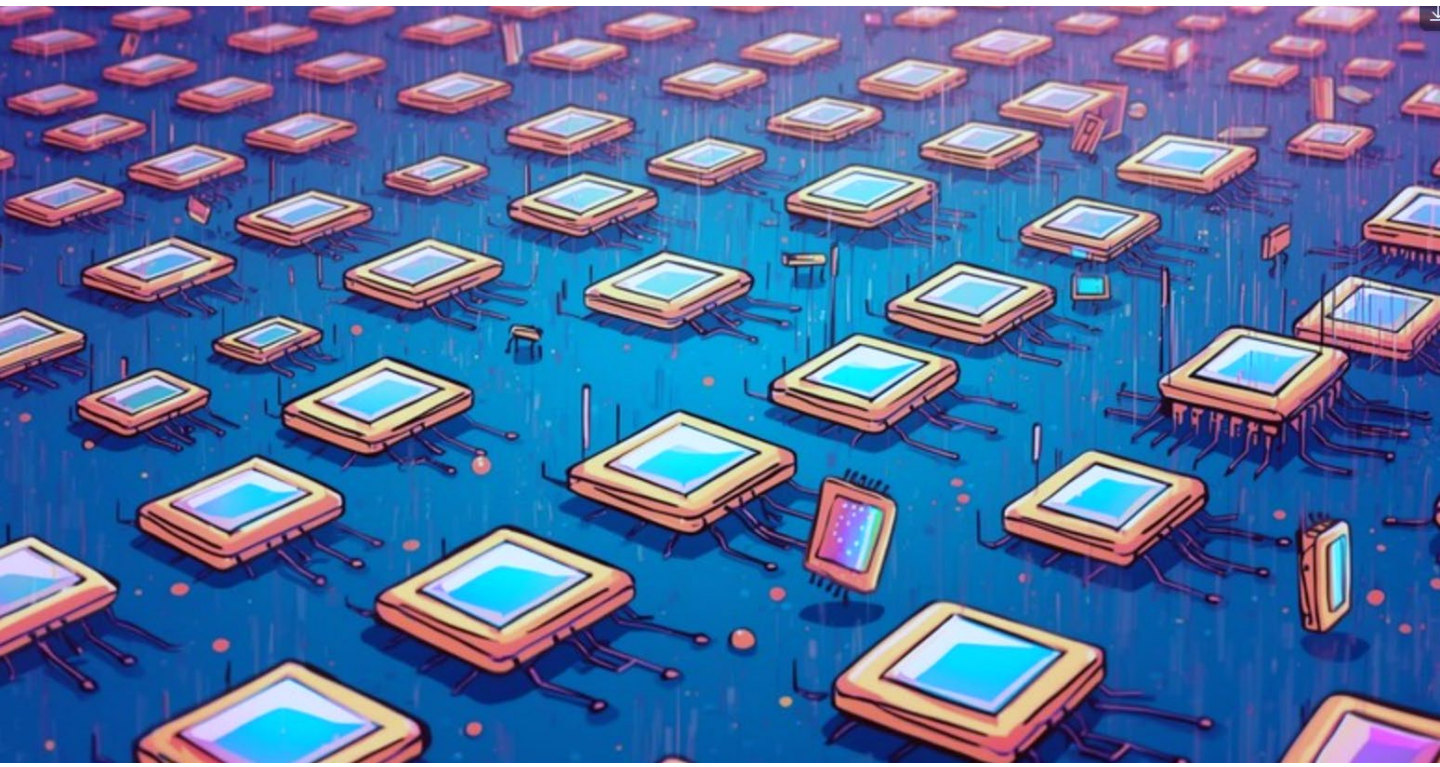
Smart Photonics builds chips that use photons instead of electrons. Photons have no mass, require little energy to move and allow for high-bandwidth data transmission at high speed. In an era of exploding data consumption, growing AI workloads and expanding data centres, this offers Europe a chance to build a strategic position in a promising emerging technology domain. One could compare it to how TSMC gained a position in Taiwan over the past decades. Whoever controls the factories and the supply chain in this new domain will define the future. It is clear that the stakes are high, as are the requirements in the domain of reliability and security.

Smart Photonics plays an important role in how Europe, and/or the Netherlands, can stand on their own feet technologically. The promising future is based on the fact that the business model is similar to TSMC's very successful foundry approach, but in photonics. Given the strategic importance, how has the threat landscape changed for your company?

"There are two main types of threats: system threats, people trying to penetrate our IT, and insider threats, which we hadn't focused on as much before. Now, we're very aware that individuals can be recruited by hostile actors, sometimes after years inside the company. We now screen people more carefully, monitor behaviour both online and offline, and compartmentalise access to critical information. Not everyone can see the whole picture, and only a handful have access to the crown jewels."

Europe has issued new regulations such as the NIS2 Directive. How does that impact your policy?

"Although NIS2 sets the regulatory expectations for us, we use the NIST Cybersecurity Framework internally because it gives us a structured, measurable maturity model. The initial self-assessment, covering five areas was sobering: we scored 0.5 out of 5. But this was not a cause for despair, it was a baseline for action. Our ambition is to reach a score of 3.5 by the end of next year. The framework provides a clear goal and forces us to keep taking action. Every quarter, we execute a set of activities ruthlessly, always aiming to move the score up. It's not just about reaching a number; it's about staying ahead of the curve by investing heavily in both technology and people. One example is the regular penetration tests, where sometimes we even use actors to attempt physical breaches. We test ourselves constantly, bringing in outside experts and learning from every exercise. We also have regular dialogue with national intelligence services to compare notes on threats and monitoring. Our awareness campaigns have also intensified. We regularly test staff with phishing emails, and there's always a handful who fall for it. That's why we repeat these exercises every quarter. The stakes are high. We spend a lot on cybersecurity, but it's necessary. One successful attack could shut us down for half a year. That's a risk we simply can't take."



The company is part of the national technology strategy, and photonics is one of ten critical technologies for the Netherlands. What is your take on this opportunity to warrant more autonomy for Europe in the current geopolitical turmoil?

"We've seen how the electronics industry moved to Asia over the past decades. The investments required to bring leading-edge chip manufacturing back to Europe are enormous, 40 billion euros for a high-end factory. That ship has sailed, but with photonics, we have a second chance. This vision shapes every strategic decision in our company. Against that background, we collaborate with other European companies to build a resilient supply chain. We also prioritise European funding to strengthen strategic autonomy. Our current funding round is focused on European investors, even though American parties are interested. We need local support to maintain autonomy.'

What role should government play in this?

"Consistent policy is vital. Taiwan's success with TSMC was built on decades of investment and subsidy. Europe needs to do the same, not just as a one-off, but as a long-term commitment. The spin-off benefits are huge, but so are the risks if we don't act. Therefore, we are actively involved in shaping European policy. We contributed to a report for the EU on building a resilient photonics supply chain, which is now feeding into the next European Chips Act. Our CEO spends a lot of time lobbying in Brussels, because without those relationships, you're left out."

What key lesson learned would you share with others about this journey?

"Don't try to do it all yourself, learn from your peers. Bring in advisors who understand your industry. Sector-specific advisors know where peers invest, what regulators expect and where attackers focus. That avoids wasting time and money on activities that look good on paper but do not reduce real risk. And prioritise ruthlessly: anchor priorities to strategic risk, not completeness."

Viewpoint
Hokkie Blogg

Partner KPMG, Cyber & TechLaw

New reality of risk: geopolitics, AI, and cyber threats

The current global landscape is increasingly shaped by complexity and uncertainty arising from political tensions, conflicts, and shifting international dynamics. Geopolitical risks refer to threats stemming from interactions between nations, including territorial disputes, economic sanctions, commercial and territories disputes, and strategic alliances.

Most of the emerging risks have always existed; however, in recent years, their likelihood of materializing has increased significantly. Companies must now strengthen their risk identification analysis to inform financial planning and risk appetite decisions, and to capture their potential impact on management metrics, while also building resilience and adapting to evolving regulations in order to effectively address these risks and identify new opportunities.

As a result, businesses face a wide range of risks that demand decisive attention, as economic integration is increasingly shaped by geopolitical and national security priorities.

Also the rapid development of disruptive digital technologies, such as artificial intelligence is accelerating the radicalization and destabilization of societies.

These technologies are increasingly used for disinformation, cyber-attacks, and politically or economically motivated manipulation, creating a new and alarming reality. This evolving threat landscape significantly raises operational risks and forces organizations to invest heavily in secure, resilient, and ethical digital transformation. Companies and institutions must prioritise cybersecurity, data integrity, and responsible technology governance to navigate this increasingly volatile environment.