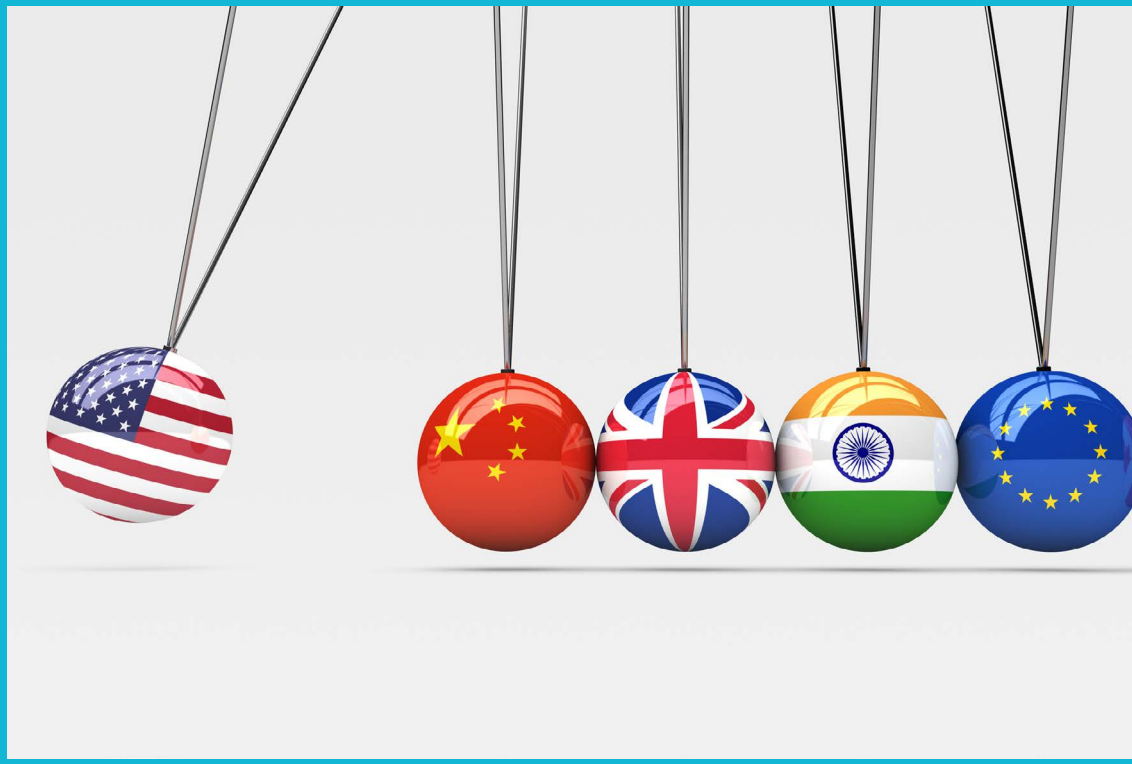
CYBER SECURITY
Gazette

2025: ACTIVITY REPORT OF THE CYBER SECURITY COALITION



CYBER SECURITY
Gazette

A word from our Chairman

Our community's message for 2026 is simple and bold: when we share, learn and act together, resilience stops being a goal - it becomes our reality. Thank you to every member, partner and OPS contractor who turns awareness into protection, and ideas into impact.

This year, let's commit to three habits that change outcomes:

*** Listen widely. The best defences start with diverse expertise across public, private and academic partners.**
*** Move faster. Share intelligence sooner; shorten time-to-detect and time-to-respond.**
*** Lift others. Invest in people and skills so every organisation can withstand and recover.**

VIDEO

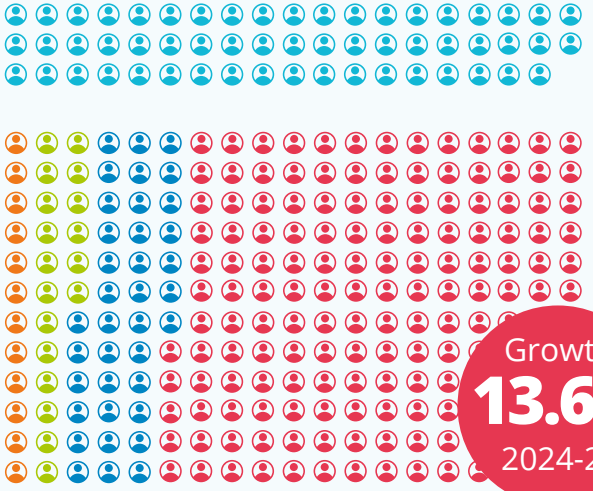
2025: Facts & figures

Members

2016
56

2025
226

12 Federations
18 Academic
36 Public
160 Private



12 focus groups

- Crypto
- Governance, Risk & Compliance
- OT/ICS Security
- Application Security
- Enterprise Security Architecture
- Awareness
- Privacy
- EU Regulations & Standardisations
- Cloud Security
- Cyber Security for Healthcare
- IAM
- Cyber Incident Detection & Response

49 Plenary meetings
964 Participations in plenary meetings

Events

1,340 Total participations
in **12** Experience Sharing Events

In Person / Hybrid Events
1,111

Partner events
229

Gender diversity

255 Speakers, Panellists & Moderators

Men
72%

Woman
28%

Theme 1

Cyber resilience in turbulent times

10 years of CCB: How Belgium became an international benchmark

The Centre for Cybersecurity Belgium (CCB) marks its 10th anniversary. What started in 2016 with a two-person team has grown into a dynamic organisation of nearly 140 experts coordinating Belgium's cybersecurity policy, prevention, and crisis response. Today, the CCB stands as a trusted national authority and an international benchmark for Active Cyber Protection. Meanwhile Belgium evolved into one of Europe's most cyber-resilient countries. In this video managing director Miguel De Bruycker and deputy director general Phédra Clouner look back and explain what Belgium's cybersecurity strategy for the next years entails.

VIDEO

“We’re in a grey area between war and peace”

The current era of escalating geopolitical tensions has brought about several profound shifts. These changes are also reverberating through the cyber domain. Within this new reality, Dutch journalist Caroline De Gruyter (NRC Handelsblad) has grown into one of the sharpest analysts of the European political stage.

“Today, more than ever, large blocs are competing over virtually everything: food, energy, trade, raw materials,” De Gruyter explains. “The weight one of these blocs can put on the scales is decisive. And that ‘weight’ is precisely what the European Union offers us as Member States.”

Europe as a service provider

Awareness of this dynamic, she argues, is more alive than ever. “You can see it among citizens – as shown by the Eurobarometer, which surveys public attitudes toward the EU every six months and has recorded historically high approval rates in recent editions – but also among politicians,” she says. “Among the latter, you can sense, especially in internal communications, that the perspective on sovereignty has been turned on its head. In the past, deeper European integration was seen as a loss of sovereignty. Today, the opposite view prevails: that Europe actually strengthens our collective leverage.”

Hence, the perception of the EU has fundamentally shifted. “It is no longer seen as a law-making machine, but rather as a service provider that countries turn to for solutions to their problems. This mindset allows those services to be delivered and formal structures to be built. Think of Frontex in response to migration, the Green Deal for climate policy, and of course defence, which has become an absolute necessity as numerous security reports point to sharply heightened threats. The Dutch Ministry of Defence even describes the current situation as a ‘grey zone’ between war and peace.”

>>>

“La crise de l’esprit”

In short, Europe now plays a nurturing role, creating the conditions in which solutions can emerge. As a result, it is being discussed more than ever. What was once dismissed as purely technical or bureaucratic has become political, and thus a matter of public debate. The same reasoning applies to cybersecurity: the EU, which has in recent years introduced far-reaching regulations, should be understood in that light.

This moment in European history fits seamlessly into a broader historical pattern, De Gruyter notes. “Aristotle pointed out that an external enemy can unite the fiercest rivals. And now we have arrived in the very world French philosopher Paul Valéry tried to imagine just over a century ago in his groundbreaking essay “La crise de l’esprit” (1919). At the time, European nations were the dominant powers on the global stage. Valéry, writing in the aftermath of the First World War, attempted to envision a world in which this was no longer the case: a world in which Europe itself would be dominated.”

What seemed highly unlikely then has become our reality now. Indeed, the future Valéry distilled from that thought experiment remains deeply relevant today. He argued that if Europe were ever cut off at the knees, it could only survive by using its head. “Translated into today’s terms,” De Gruyter concludes, “that means that by investing in the knowledge economy, Europe will always secure itself a place on the world stage.”

“Our motto is cyber force through partnerships”

Major General Pierre Ciparisse has led the Cyber Command since the summer of 2025. He emphasises that the unit’s role within Belgium’s defence structure will continue to grow in the coming years. At the same time, he stresses that this shift towards a more assertive posture requires embracing a philosophy of deep cooperation.

Today’s soldiers deployed at the frontline are for all intents and purposes carrying a spy in their pocket. “Opponents, for instance in the war in Ukraine, are effectively using smartphone signals to locate and eliminate enemy troops,” Ciparisse explains. “But that’s just the tip of the iceberg when it comes to how technology is being used in conflicts. Think of the sheer number of drones entering hostile airspace, including our own.”

No silver bullet

The military use of this technology is constantly evolving. “At the beginning of the war in Ukraine, we often saw the Russians conducting joint operations involving the simultaneous use of physical and cyber capabilities in strikes,” says Ciparisse. “Today, that’s far less common, as Russian units are finding it increasingly difficult to access enemy cyber environments, making such operations less effective. The notion that cyberattacks are the absolute ‘silver bullet’ of modern warfare, as many believed a few years ago, simply doesn’t hold. We will always face combined, multidimensional attacks.”

With cyber becoming an integral part of modern military conflict, it is now recognised as a fully fledged attack surface within Defence, with dedicated capabilities assigned to it. “Building up the Cyber Command within the Belgian Defence Forces is a long-term process,” says Ciparisse. “An important next step for us is deploying cyber experts to the other forces (Land, Air, Navy,

>>>

Medical Service) facing similar challenges. This reflects the reality that our current-day defence systems are interconnected.

Force through partnerships

Cyber defence, like any form of telecommunications, operates across three interconnected layers: the virtual, the logical and the physical. "It's not just about software or virtual networks," Ciparisse clarifies. "It also involves broader systems, physical cables and hardware infrastructures. Attacks on any of these – whether a cut cable, a hack, a social media disinformation campaign… – fall within our scope. A strong response must account for every layer."

But addressing such a broad spectrum of challenges can only be done through close and active collaboration. "Our motto is cyber force through partnerships. In practice, this means we're building on the philosophy of the Cyber Security Coalition, which has long been part of Belgium's cyber ecosystem. In this era of hybrid warfare and lightning-fast technological acceleration, that is the only viable path forward," Ciparisse emphasises.

This is why Cyber Command's operations are woven into the fabric of wider society, notably through the Belgian National Resilience Plan. "In practice, we work as closely as possible with the police, the federal prosecutor's office and government agencies via the Centre for Cybersecurity Belgium (CCB), which serves as the first point of contact in times of crisis. Together, we aim to develop the most effective threat analysis possible. Under the umbrella of the National Security Council, we consolidate as much intelligence as we can."

We aim to develop the most effective threat analysis possible.

Belgium can thus be considered a front-runner in the fight against military cyber threats. "This was demonstrated when the country diplomatically called out China after successfully attributing cyberattacks to Chinese actors. Many countries would hide behind the umbrella of NATO or the EU in such a case, but we didn't. That earned us considerable international respect," says Ciparisse. He also points to the European Space Agency's Cybersecurity Centre in Redu. "For the military domain, that's of major significance. All military communications depend on space infrastructure, and we fully support the expansion of this centre and the ambition to turn it into a true cybersecurity valley," he concludes.

“National Cyber Survey: “We should be able to weather the current storm”

A decade after its founding, the Cyber Security Coalition stepped into 2025 with the National Cyber Survey Belgium, an initiative that captured the pulse of Belgium’s cybersecurity landscape. Benoît Watteyne, Director of Cyber & Privacy at KPMG Belgium, which conducted the survey together with the Coalition, guides us through the most important results. “The key themes today are AI, geopolitics and third-party risks.”

In 2025, the Cyber Security Coalition celebrated its 10th anniversary with an important new achievement. In partnership with KPMG and supported by Agoria, it carried out the National Cyber Survey Belgium, a large-scale study involving 266 companies in Flanders, Brussels and Wallonia. The survey explored the most pressing cybersecurity priorities of the moment. Participants from all major sectors in the country answered a total of 177 questions. “The key themes today are AI, geopolitics and third-party risks,” says Watteyne. “The urgency and relevance of the topic are clear from the results, with half of the surveyed companies indicating that they have seen an increase in cyberattacks over the past year,” he continues. “In 16% of the cases, the attack resulted in actual damage. Clearly, there is a need to continue strengthening our defence mechanisms, but it also shows that the majority of attacks are thwarted.”

Successful attacks often stem from weak email security (38%) or poor credentials (31%). “At the same time, the general outlook for the future is quite positive. Companies are hopeful about the further integration of AI into cybersecurity. No less than 76% see AI as an opportunity, and 49% believe it will improve their cybersecurity over the next 12 months. Without the specified time frame, that number rises to 67%,” Watteyne explains. “There is also clear awareness of the risks arising with this trend, especially regarding data protection. It is therefore encouraging that 57% already have AI rules in place.

>>>

Geopolitical reality as a driver of awareness

Slightly more than half of the companies (53%) perceive a clear connection between rising geopolitical tensions and increased cyber threats. The link with financial losses is even more evident (71%). “The origin of the attackers shows a mixed picture. 30% come from Europe, 20% from Asia and 15% from North America. The origin of another 30% could not be determined,” he says.

The survey also shows a strong willingness to address the growing third-party risks. Half of the respondents are concerned that suppliers may not follow the same cyber security standards. 51% work with certifications when selecting suppliers, and 36% rely on independent audits. “At the same time, there is still a significant blind spot. 29% say they do not know whether an attack has taken place in their supply chain, and an even larger group (31%) believes there is too little awareness about the risks of supply-chain attacks,” Watteyne adds.

“Therefore, with this initiative, we aim - above all - to raise awareness of these issues. At the same time, we want to highlight the progress already achieved to strengthen resilience and confidence in Belgium’s cyber ecosystem,” Watteyne continues. In other words, the report emphasises the overall positive tone within this part of our economic fabric. “Throughout this story, we use the turtle as a metaphor. It may not be the fastest creature, but its strong shell, resilience and adaptability have made it one of the longest-living species on the planet.

By striving for these qualities, we should be able to weather the current storm,” he concludes.

“These campaigns always exploit existing weaknesses”

In this era of rising geopolitical tensions, the Cyber Security Coalition dedicated a panel to disinformation during its BE-CYBER Experience Day in October 2025. The discussion featured Dominika Hajdu, Director for Policy & Programming at GLOBSEC; Beatriz Marin Garcia, Team Leader of Strategic Communication at the European External Action Service; and Peter Van Aelst, Professor of Political Communication at the University of Antwerp. The session was moderated by Peter Booms, who, through his role at the Permanent Representation of Belgium to the EU, specialises in the topic.

“Although we are all aware of it, even within the cybersecurity sector we still underestimate the power and importance of disinformation. It affects the very fabric of our societal model, deep within our souls,” Booms immediately set the tone for the conversation. “Its ultimate goal is to sow doubt. We must collectively realise that the parties behind this have over 600 million euros invested in this effort. Clearly, they deem it extremely important.”

“Like throwing spaghetti at the wall”

While establishing a causal link between the spread of disinformation and its consequences is scientifically challenging, its impact is undeniably present in our daily reality. “When people are consistently exposed to certain viewpoints, they begin to shift in that direction,” Hajdu explained. “It’s crucial to realise that these campaigns always exploit existing weaknesses or fault lines within society, which are then further exacerbated. In practice, it’s not so much about foreign narratives being introduced but rather about narratives that already exist, which they try to push into the mainstream,” added Marin Garcia.

“What happens can best be compared to throwing cooked spaghetti at the wall. You know only some of it will stick, but you can never predict in advance which strands they will be. The same goes for disinformation campaigns. You can’t predict in advance what will stick and which opinions will shift as a result. That’s what makes it so difficult to combat, and thus so appealing to those who seek to exploit it,” said Van Aelst.

>>>

Peter Booms

The success of Foreign Information Manipulation and Interference (FINI) therefore depends on how well the information being spread – whether true or false – resonates. In other words, how well it aligns with existing societal fault lines. “That’s why these campaigns focus primarily on society’s so-called fringe groups, which are already marginalised and have lower trust in the government, making them more susceptible,” Van Aelst continued.

No quick fixes

A better understanding of how disinformation campaigns work also means recognising that there are no quick fixes. Rather, fighting them is a long-term effort requiring many combined measures. Above all, trust in traditional gatekeepers such as journalists and governmental bodies must be reinforced, especially among the fringe groups. “We must also become more assertive in blocking disinformation entering our networks. This is the basis of the European Commission’s new strategy on this issue, which builds upon the Digital Services Act,” Garcia explained.

A concrete example of this more assertive approach, which was collectively praised by the panel, is the ban on political advertisements on Meta platforms: a particularly relevant measure for Belgium, where such advertisements were a common practice until recently. “Belgium is reasonably well-equipped in this regard, despite having significant and historically deep-rooted fault lines. This is evidenced, for example, by the strong trust people still have in public broadcasters,” said Van Aelst, who, with his research team, developed a dashboard aimed at mapping disinformation vulnerability across European countries for policymakers.

Based on this extensive research, Van Aelst and his team concluded, with unanimous agreement from the rest of the panel, that there’s no need for despair in Europe’s fight against disinformation. “There’s a sense of doom surrounding this issue, but in practice, we have proven to be pretty resilient. Look at the recent elections in Moldova. Despite large-scale disinformation campaigns from Russia, the pro-Russian candidate did not emerge as the winner,” Hajdu explained. “So, we shouldn’t overestimate the current impact, as it can backfire. By doing so, people may become suspicious of governments, which is exactly what the aggressors want,” Van Aelst concluded.

Dominika Hajdu, Peter Van Aelst and Beatriz Marin Garcia

Navigating uncertainty: How to future-proof cyber resilience

We live in interesting times. This isn't just a well-worn phrase; it's a stark reality. We face rapid geopolitical shifts, technological advancements, and increasing regulatory complexity. In such a dynamic environment, the traditional "predict then act" approach to business and decision-making falls short. We need to embrace a new way of thinking, one that acknowledges uncertainty and prepares us for a range of possible futures. This is where strategic foresight comes in. During the latest Women4Cyber event, we talked in depth about future-proofing cyber resilience in uncertain times with Rayna Stamboliyska, Uncertainty Management Specialist and CEO at RS Strategy.

Is it safe to say that you are not a believer of "Business as usual"?

Rayna Stamboliyska: "No, I find it rather terrifying. But it is in the human nature to stick to what we know. However, in today's world, this approach is no longer sustainable. The pace of change is too rapid, and the forces shaping our future are too unpredictable. To illustrate this point, let's look at a historical example. In the 1960s, Shell, a leading fossil fuel company, embarked on the so-called Long Range Project. They began to consider potential geopolitical and economic disruptions that could significantly impact their business. At a time when oil supplies seemed endless, discussing the end of oil reserves or surging oil prices was considered ludicrous. Yet, Shell persevered and developed scenarios addressing probable futures. One of these scenarios explored the impact of an oil price surge. In the early 1970s, the well-known oil crisis erupted, and oil prices quadrupled. While the rest of the world scrambled to react, Shell was prepared.

As the architect of modern futures thinking, Alvin Toffler, put it in his book Future Shock back in 1960: "In dealing with the future, it's more important to be imaginative than to be right". We must embrace unfamiliar and even conflicting visions of what may happen, keep an open mind, and accept that business as usual is no longer a viable strategy.

>>>

Why do you believe it is important to care about the future?

Rayna Stamboliyska: "The need to care about the future extends beyond corporate strategy. It impacts our daily lives. Consider the generational differences in the workplace. For the first time in human history, we have five generations working side-by-side. This presents tremendous challenges in communication, collaboration, and understanding.

Just as we navigate generational differences, we must also navigate the broader societal and global changes after a window of great growth and peace, especially in Europe. We are witnessing an exponential increase in geopolitical mutations, technological innovation, and regulatory complexity. These factors interact, resulting in a world where nothing is certain, and much is beyond our control.

This situation of deep uncertainty challenges decision-makers at all levels. Traditional approaches, relying on past data and risk assessments, are no longer sufficient. We need new tools and techniques to navigate this complex landscape."

In your presentation, you referred to the movie and book 'Dune' to illustrate the way we should look at the future.

Rayna Stamboliyska: "Indeed. In Frank Herbert's renowned science fiction novel Dune, the story unfolds in a galaxy that has experienced a technological apocalypse. Interstellar travel, trade, and life itself depend on a precious substance called "the spice." The spice, found only on the desert planet of Arrakis (Dune), enhances the human mind and enables prescience – the ability to see the future.

When the Atreides family is sent to govern Arrakis, they are betrayed, and the young son, Paul, is left to die in the desert. However, Paul survives by embracing chaos and using his developing so-called prescience: the spice opens his consciousness, allowing him to see different visions of the future. He uses these visions, contradictory and partial as they may be, to plot a path forward and ultimately take control of the planet. In other words, Paul turns his contradictory, incomplete visions into strategic assets and accepts that there are many plausible futures. The key takeaway here is that the future is not predetermined, and that agency does not lie with predictions. Instead, the future is a landscape of possibilities that we can influence and shape."

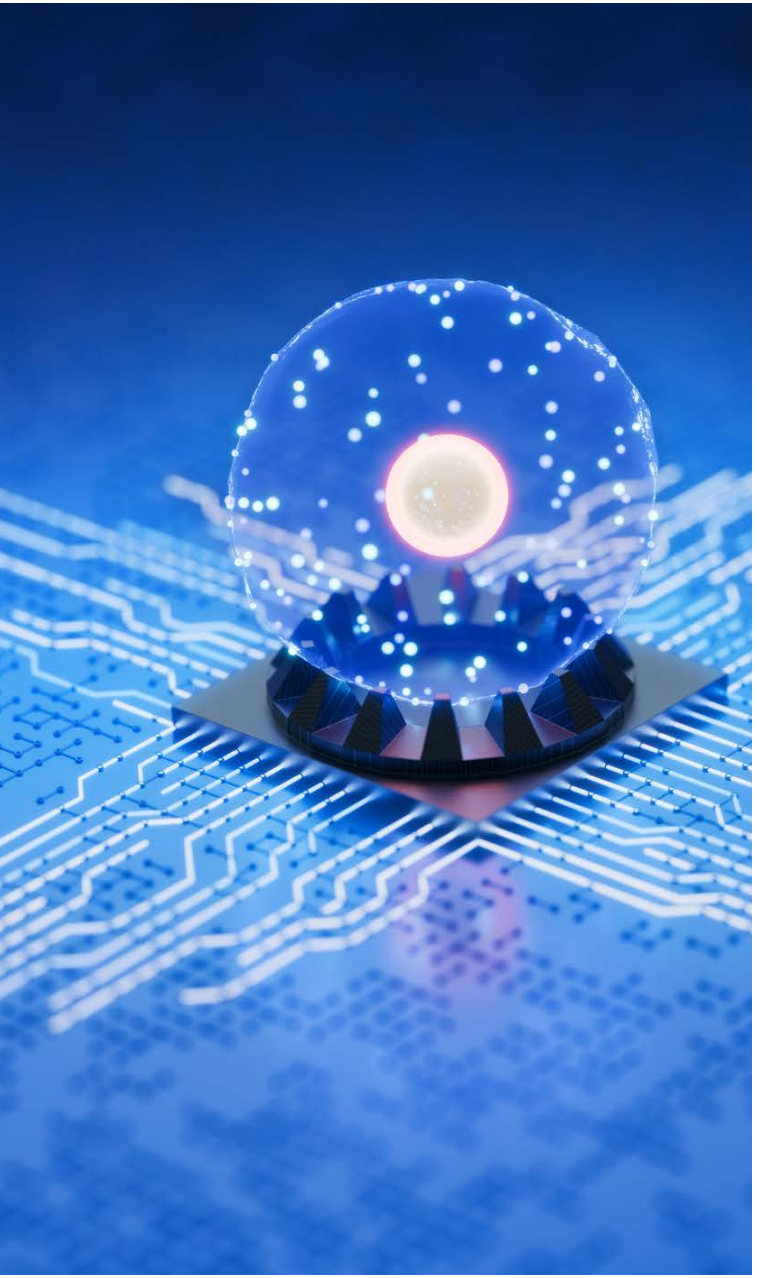
So how do we navigate this landscape of possibilities?

Rayna Stamboliyska: "Good question. How do we learn to think like Dune's Paul Atreides? How do we cultivate the ability to see the future and make decisions based on that? The answer lies in strategic foresight. Strategic foresight is a discipline that provides a structured approach to thinking about the future. It's not about predicting the future with certainty, which is impossible, but about understanding the range of possibilities and preparing for them. So, instead of identifying a few desired future scenarios based on specific preset conditions and assets, we would look at a wide range of scenarios and chart a strategy that performs well enough across many of these. Thus, we stop trying to predict future conditions and focus on ways forward that resist changes in external circumstances."

This requires a certain mindset, for sure?

Rayna Stamboliyska: "It does, and developing a foresight mindset requires several key attributes. First, we need to be curious. We need to be open to new ideas and new ways of thinking and doing. We also need to be willing to challenge our assumptions and to question the status quo, however uncomfortable that is.

>>>



Next, we need to be willing to experiment and to learn from our mistakes. And finally, we need to be willing to collaborate with others, to share our ideas and our insights and listen to others."

How can strategic foresight be used?
Rayna Stamboliyska: "It can support developing strategies. To identify the goals that we want to achieve and to develop plans to achieve those goals. Implicitly, you can use it to make robust decisions, to evaluate different options and to choose the most adequate course of action. And lastly, it can be used to innovate. To identify new opportunities and to develop new products and services."

What are the tools and techniques used to support strategic foresight?
Rayna Stamboliyska: "Several tools and techniques can aid in strategic foresight. One of the most common is Scenario Planning. As exemplified by Shell, this involves developing different plausible scenarios of the future and analysing their potential impact. Another one is Trend Analysis or identifying patterns of change over time and analysing their potential impact. And finally, I would like to highlight a favourite, often called "How To, What If". It is a combination of back-casting and fore-casting, that is, you define several realities you'd like to reach, then work backwards to identify chains of events that need to occur to make that reality happen. Then comes the fore-casting: what would be chains of consequences if that reality came to be? I use this one with clients and students alike.

Can you highlight some of the challenges and benefits of strategic foresight?
Rayna Stamboliyska: While strategic foresight offers significant benefits, it also presents challenges. We all have biases that can cloud our judgment, and strategic foresight requires time, effort, and resources. However, the benefits of strategic foresight far outweigh the challenges. It enables us to make more sustainable decisions, identify opportunities, foster innovation, and build resilience.

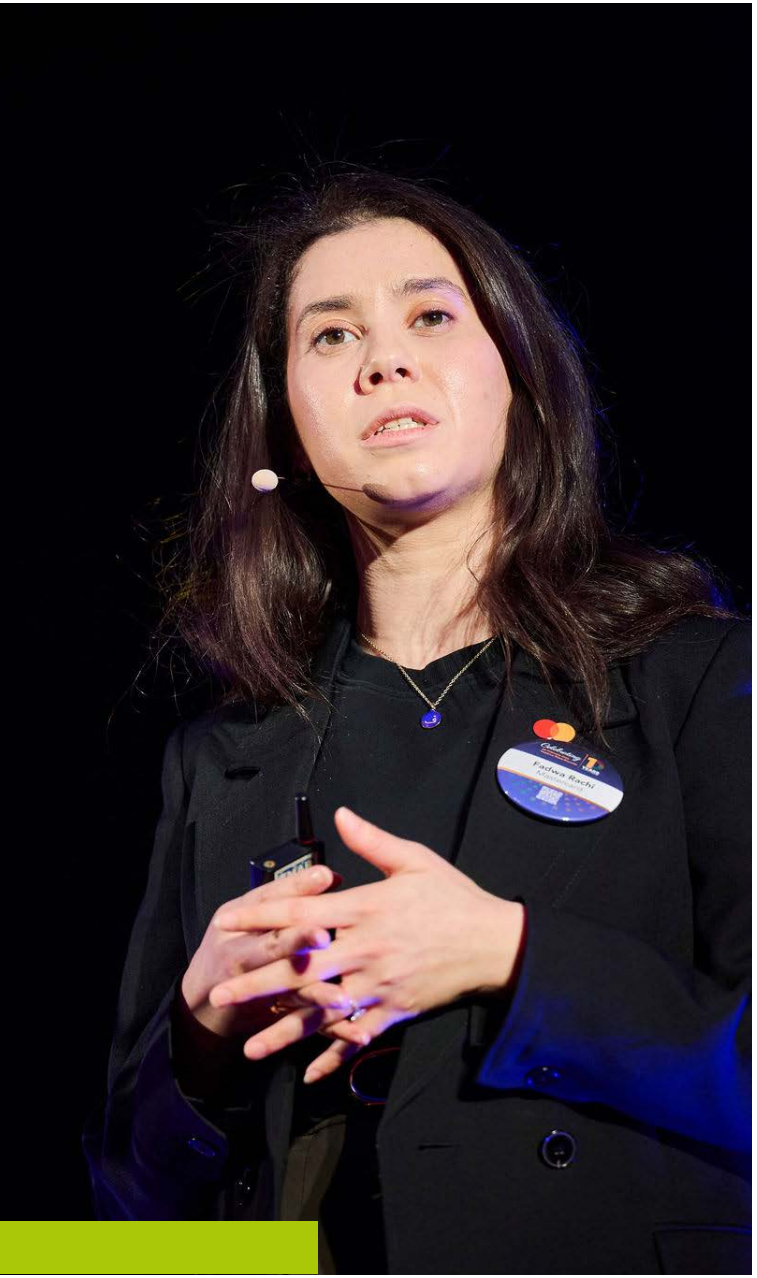
How can you use strategic foresight in cyber security?
Rayna Stamboliyska: "Let us take the example of the implementation of NIS2, which is a requirement for many companies throughout Europe. So, within this framework, how can businesses create a long-term strategy that is robust enough to anticipate heterogeneous transpositions across the EU, requirements

>>>

for incident notifications in 24 languages and wildly diverging maturity levels? I have been working with a client to support building a robust implementation strategy for NIS2 and embed resilience into governance structures. In this particular case, we used the Dune analogy I talked about earlier to develop a game which we used to stress-test the client's NIS2 approaches and converge towards a robust strategy.

Tell us more about this game...
Rayna Stamboliyska: "We modelled a game on strategic foresight. This company has specific challenges: heterogeneous NIS2 transpositions in the 10 countries they operate, challenging incident reporting, and a complex supply chain. The game starts with defining the uncertainties: for instance, heterogeneous transpositions. These are elements beyond your control. Next, you identify so-called levers, or all the things you can do to act within the given context to address uncertainties. For the challenge of the diverging transpositions, the levers could be either to harmonise compliance or tailor it by country. The next step is to develop the relationships between the uncertainty and the different levers. In this case, this was either a harmonised approach towards NIS2 by establishing a transborder governance group and monitoring the requirements, or else let each country handle it on their own and do no monitoring. The final part of the game is to define metrics for each of these pathways or storylines. By playing the game, you can come up with a strategy that offers the most resilient approach."

Lots to think about. Any final thoughts to share with the cyber security audience?
Rayna Stamboliyska: "I tend to say that we are all migrants to the future. When you go to another country you see that things are different than in your own. It does not mean that one is better than the other. You cannot anticipate everything and that is fine. On the other hand, you cannot let aversity to change lead to paralysis and not do anything. By embracing a foresight mindset, utilising appropriate tools and techniques, and fostering a culture of continuous learning, we can navigate uncertainty, make informed decisions, and shape a more resilient future. And let us as technologists never forget that what we do in cyber, we do for people. So, whenever we design systems, we should always remember that those systems must serve the people, not the technology."



Strategic foresight: anticipating and preparing for emerging cyber threats

Celebrating the 10th anniversary of the Cyber Security Coalition, Fadwa Rachi, Head of the European Cyber Resilience Centre (ECRC) at Mastercard, delivered a keynote on the pressing need for strategic foresight in cyber security: "As cyber threats become more sophisticated, she emphasised that resilience hinges not only on immediate threat mitigation but also on long-term preparedness."

Looking 10 to 15 years ahead allows us to guard against strategic surprises.

Rachi highlighted the increasing complexity of cyber threats and their deep societal impact. "Cyber crime is no longer just a collection of isolated incidents. It has evolved into a fully developed industry, commoditised and accessible to those willing to pay," she stated. "From fake software updates spreading malware to credential theft and the growing prominence of cyber-crime-for-hire services, attackers have become faster, more precise and more scalable."

One of the key trends she identified was the dark web's role in enabling cyber criminals. "Everything is for sale: DDoS attack tutorials, phishing kits and access credentials. Organisations need to assume that their information is a target and act accordingly," she warned. Rachi also underlined the significant role AI plays in amplifying these threats. "Phishing attacks are now so tailored and convincing that even cyber security professionals pause to verify them. Imagine how difficult this is for the average employee or consumer."

>>>

Cyber resilience: a collective effort

Belgium has set itself the ambitious goal to be one of the least vulnerable countries in Europe when it comes to cyber security. Fadwa Rachi acknowledged the importance of collaboration between government, industry and academia in achieving this goal. “Mastercard, along with other industry players, is actively working to protect infrastructures, employees and consumers, but cyber security cannot be addressed in silos,” she stressed.

A culture of security awareness is key. Employees must be equipped with knowledge, such as recognising the dangers of reusing passwords or falling victim to social engineering tactics. “Security is not just the responsibility of IT teams. It must be embedded in the DNA of every organisation,” she asserted. The implementation of multi-factor authentication and Zero Trust frameworks, where breaches are assumed and continuously mitigated, were highlighted as necessary steps.

Collaboration remains the key to resilience

Beyond addressing current risks, Rachi emphasised the importance of ‘threatcasting’ as a methodology to anticipate future cyber threats. “Looking 10 to 15 years ahead allows us to guard against strategic surprises,” she explained. Mastercard, in collaboration with experts and researchers, uses this approach to identify potential cyber risks and develop proactive strategies.

Emerging technologies such as AI, 6G networks and autonomous software will become so embedded in daily operations that threats may become nearly imperceptible. “We must prepare now to prevent a future where cyber risks outpace our ability to respond,” she cautioned.

Fadwa Rachi’s final message was one of collective action. “Cyber criminals collaborate, and so must we. Public/private partnerships, information-sharing and cross-border cooperation are essential. We all have a role to play in protecting the digital ecosystem.”

Theme 2

NIS2: From policy to practice

Vlaams Centrum voor Digitale Veiligheid: “NIS2 is a tool to strengthen each other’s resilience”

In May 2025, Digitaal Vlaanderen established a dedicated centre for digital security. This centre ensures that Flemish public services and local authorities comply with the Flemish digital security policy and the NIS2 directive. At first glance, the directive may seem like just another legislative framework that organisations must adhere to, but in practice, it is much more than that. “NIS2 forces us to accelerate towards a digitally secure Flanders,” state Steven Vermeulen and Carolina Stevens from the Vlaams Centrum voor Digitale Veiligheid.

The NIS2 directive has a significant impact on the Flemish public sector: many activities for which local authorities and Flemish public institutions are responsible fall within its scope. As a result, hundreds of organisations must thoroughly reconsider their cybersecurity policies. However, Steven Vermeulen, CIO of Digitaal Vlaanderen, notes that “the varying levels of maturity make translating the directive into practice complex. Budgetary constraints and geopolitical tensions increase the challenge.”

More than just another regulation

The establishment of a dedicated centre for digital security strengthened and expanded Digitaal Vlaanderen’s role as the single point of contact for the Flemish government and local authorities in implementing the NIS2 directive. “But NIS2 is more than just a directive for us. It’s a lever to elevate the security policies of Flemish and local authorities, providing them

>>>

with insights into their current digital resilience and helping us identify vulnerabilities in the ecosystem," states Carolina Stevens, who is NIS2 Implementation Coordinator at Digitaal Vlaanderen.

In addition to supporting authorities in Flanders with NIS2 compliance, the Vlaams Centrum voor Digitale Veiligheid also assists in the development of their security policies. Stevens: "We focus on providing practical support, including risk analyses, toolboxes and targeted training."
In terms of NIS2 compliance, 18 April 2026 is an important milestone: by that date, all institutions concerned must demonstrate that they are taking the necessary basic measures to mitigate cyber risks. "We start out by looking at the warning signals: indicators that point to significant deviations or gaps in the current security approach. Then, we map where work still needs to be done and how we can close the security gap," explains Carolina Stevens. This exercise will also be valuable for the new centre itself, as its supervisory role is not merely about control. "We see it as an interaction, where we start from the idea that the NIS2 directive is a tool to strengthen each other's resilience. After all, we all benefit when no one is left behind."

The time to act is now

All institutions should be aware that they are a possible target for cybercriminals. A passive security policy is no longer sufficient, and organisations must continuously reassess their risks. Steven Vermeulen: "Digital security is an ongoing process. In the past, the focus was on firewalls, passwords and privacy. Today, strategic independence, sovereignty and geopolitical context play a role, as well. Digital security also affects trust in governments. Our task is to restore that trust by providing clarity and creating digital simplicity."
At the same time, however, all public institutions face budgetary constraints, which makes the task for the new centre even more complex. The message it wants to convey is that the time to act is now. "It's a pipedream to think that the work will ever truly be finished. But what's critical is to get started, because the chain is only as strong as its weakest link," concludes Stevens. "In this respect, NIS2 is the perfect lever. And we want to be the guide that provides direction and sets the bar for everyone."

“After concentrating on data collection in 2025, it’s time for action”

Translating NIS2 into actionable plans is currently one of the main drivers of progress within our country’s cybersecurity landscape. For the Public Service of Wallonia (SPW), the Agence du Numérique (AdN) is playing a pivotal role in this process. According to Jérémy Grandclaudon, Senior Cyber Security Specialist at AdN, it’s a journey that should be viewed as a significant catalyst for the public sector: “NIS2 has made us realise we’re all in this together.”

“As NIS2 arrived and its far-reaching implications were recognised, the office of Walloon Minister of Economy, Pierre-Yves Jéholet, approached us at AdN to take on a guiding and supporting role in the transposition of the European directive for the broader public sector in Wallonia,” says Grandclaudon. “We began with identification: determining who falls under the scope of the regulation, or in other words, who must be considered ‘essential’.”

From plan to action

The exercise taken on by AdN specifically addresses the role and value of each entity within the Walloon public sector. “We consulted around 130 to 150 entities and essentially taught them to speak the same language as the Centre for Cybersecurity Belgium (CCB). We reviewed their data and prepared it for submission to the CCB,” he explains. “This convinced me that NIS2 is a huge opportunity for the entire societal fabric. While everyone was already aware of the need to do something about security, today we have a legal framework that serves as the basis for concrete action plans. Doors are truly opening that were previously closed.”

This places Grandclaudon in an excellent position to assess where the greatest challenges lie in this process. “Everyone clearly understands that we need to act, but the big question for many is how to approach this and what tools can be used,” he says. “This will undoubtedly be our priority for 2026. After concentrating on data collection in 2025, it’s time for action.”

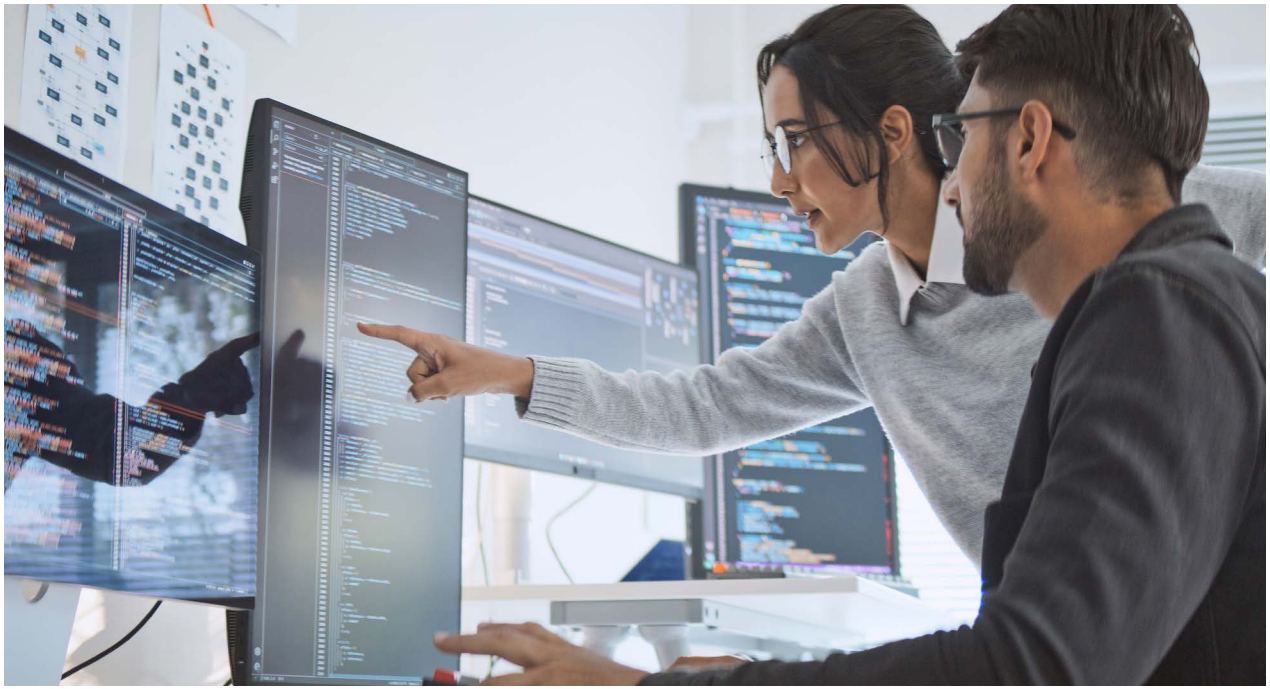
>>>

A culture of mutual trust

To successfully take this step, he emphasises the need to focus on both collaboration and strengthening the existing ecosystem. “Considering the budgetary context in our country, this is the only option available to us. For the Walloon public sector, which is very heterogeneous, there is no sense in trying to reinvent the wheel every time. We must fully embrace knowledge sharing and break down existing silos as much as possible,” says Grandclaudon.

Mutual trust is essential to further fuel this cultural shift. “NIS2 has acted as an external pressure, making us realise that we’re all in this together. We cannot simply leave parts of the public sector behind, or we will end up with a landscape full of weaker links—which is exactly what hackers are targeting today.”

This same culture of mutual trust and belief in knowledge sharing is also present between the country’s various governments. “The decision to place the transposition of NIS2 at the regional policy levels has proven to be the right one. They have easier access to on-the-ground information and are best acquainted with the heterogeneous reality. This has contributed to Belgium being an undeniable leader in NIS2 implementation in Europe. We must ensure to maintain this position. Without it, the public sector will face more attacks and a decline in public trust, at the very moment when trust is indispensable”, he concludes.



Industrial security and the impact of NIS2: “The timeframe fo implementation is not feasible”

The ongoing digital transformation has profoundly reshaped our industrial landscape. In the manufacturing industry, increasing cyber threats and evolving legislation create complex challenges that traditional IT security profiles do not always fully grasp, states Sam Van Hauwaert, an expert in industrial cybersecurity. “The aim should not be to tick boxes, but to genuinely understand and manage the risks to the organisation.”

“If a company in the water or energy sector is hit by a cyberattack, the consequences can be immediate. A halted factory or a stopped water utility can lead to environmental disasters or even life-threatening situations,” Van Hauwaert begins. “That is why we always first focus on the safety of people and the environment, and only afterwards consider the traditional aspects of network and data security, such as confidentiality and integrity.”

One of the key lessons he draws from his work as an Industrial Security Advocate is the necessity of knowledge sharing between IT and OT professionals. In industrial practice, however, it is often difficult to bridge these two worlds, leading to misunderstandings about technology and insufficient risk management. “IT cannot simply assume that OT shares the same concerns about cyber threats, and vice versa. That is why it is so important to bring the two worlds together through training and collaboration. I always consider it my first task to teach them to speak the same language.”

NIS2 as a catalyst for change

A fundamental building block in linking cybersecurity with industry is risk management. Thus, Sam Van Hauwaert emphasises that risk management is not just a technical matter. In essence, it is a business issue. “It is essential that company

>>>

management understands the impact of a cyberattack and makes strategic decisions based on risk analysis."

The introduction of NIS2, he argues, therefore represents a crucial opportunity. At the same time, he emphasises that it presents a major challenge for many industrial companies. "I fully support the underlying mission of the legislation, but the pace of implementation in sectors such as energy, water management, and the chemical industry is simply not feasible within the stipulated two-year timeframe," he explains. The complexity of the systems and the long lifespan of industrial technologies - machines are typically designed to last several decades - makes it virtually impossible to achieve full compliance in such a short period.

Focusing too heavily on compliance, he warns, risks creating a checkbox mentality. "Companies may simply follow the rules without truly understanding the real impact of cybersecurity on their business. That cannot be the goal. The aim should not be to tick boxes, but to genuinely understand and manage the risks to the organisation."

Pragmatic realism

For this reason, Sam Van Hauwaert advocates for more flexibility in legislation and greater support from governments and regulators. "The law must allow companies to meet requirements step by step, without being panicked by the pressure to achieve compliance on time. In other words, it is important that lawmakers are realistic about the pace at which industrial companies can meet these obligations."

The aim is not to tick boxes, but to genuinely understand and manage the risks.

"Many companies are still barely aware of the new reality brought about by NIS2. Starting supervision or auditing now seems far too early," he continues. "In fact, the security community needs to recognise that a one-size-fits-all approach is not suitable for this context. The industrial field is simply too specific and diverse. This is inevitable, given how many sectors are affected by this legislation, and especially when considering its impact on their suppliers. A pragmatic approach is therefore required at this stage."

To build this culture of support, he first looks to the Centre for Cybersecurity Belgium, while also recognising that the broader cybersecurity ecosystem - with the Cyber Security Coalition serving as a vital bridge - cannot be overlooked. "As a society, we have somewhat lost trust in our digital technology, and NIS2 can be a step toward reversing this trend. The real challenge lies in implementing the right culture and continuing to invest in knowledge and technology."

NIS2 One year on: Where policy meets practice

It has been a year since Belgium implemented the NIS2 law — a milestone in strengthening cybersecurity across the EU. In this episode, we look back at how far we've come and what challenges remain. Join our podcast hosts as they reflect on one year of NIS2: the progress, the lessons learned, and what's next for organisations navigating the new security landscape. Tune in and find out where Belgium stands — one year after NIS2 became law.

Theme 3

Standardising AI for a secure future

AI in cybersecurity: an arms race the European Commission cannot afford to lose

Artificial intelligence (AI) is changing cybersecurity on both sides of the battlefield. Attackers use it to automate and improve reconnaissance and social engineering; defenders strive to match their speed and precision. Inside the European Commission, DG DIGIT's cybersecurity teams are learning how to make AI an ally without creating new vulnerabilities. Efthymios Lalas, Deputy Head of Unit at DIGIT.D1, explains how the Commission protects its own systems and what Belgian institutions and companies can learn.

Efthymios Lalas has two decades of experience in IT and security, including work in law enforcement and the private sector. At DG DIGIT, he helps shape the Commission's internal cybersecurity strategy, including how AI is deployed safely and used to strengthen defences.

Artificial Intelligence is both a threat and an opportunity. What is the state of affairs right now?
AI is everywhere: in personal apps, in commercial services, and increasingly in the attacker's toolbox. Malicious actors use it to scan for weaknesses, orchestrate chained attacks more quickly, and create convincing phishing or fake websites. That puts pressure on defenders to up their game. At the Commission, we see AI as both a challenge and an opportunity: we must protect the AI systems we deploy and at the same time use AI to strengthen our defences.

So defenders are adopting AI themselves?
Yes. We have built AI into four classic functions: content generation, prediction, recommendations and decision support. For example, AI helps us draft clearer vulnerability and incident reports, summarise external threat intelligence, and spot weak points

>>>

in complex risk assessments. It also assists analysts in proposing security controls and in making time-critical decisions, such as blocking or neutralising suspicious activity.

But can you rely on AI in a field where the unpredictable is often what matters?
No, and we do not. Humans always stay firmly in the loop. AI can filter noise, speed up triage, and surface patterns, but the final judgement still lies with experienced analysts. Attackers are creative and adapt quickly; it is unrealistic to think AI alone can outsmart them. Our strategy is to combine automation with human oversight and continuous learning.

What new types of attacks has AI made more concerning?
We see three big trends. First, reconnaissance: gathering information and mapping entry points is faster and more effective with AI. Second, social engineering: it has become more persuasive, with phishing and deep-fake content becoming harder to spot. Third, chained attacks: automation enables what used to take days or weeks to now unfold in minutes. These trends are forcing us to harden systems and train people to detect subtle cues.

What boundaries does the Commission set for itself when deploying AI?
We apply strict internal security controls and align with best practices from international frameworks before any AI capability goes into production. We run security assessments specifically for AI risks and maintain our own general-purpose generative AI solution. And we issue clear guidance to staff about when and how they may use external AI tools.

Private companies often move faster than public bodies. Does that help or hurt?
The private sector is agile and quick to adopt new tools, which can be an advantage but also increases exposure if security is not built in. Public institutions, including the Commission, move more cautiously, with slower adoption but a stronger focus on sovereignty, compliance and data protection. I think that, for private companies, AI is really a business tool, so they are quicker to adopt it and more willing to take risks.

What advice would you give Belgian organisations?
First, make AI and cybersecurity a joint strategic priority: do not let experimentation drift without oversight. Second, build on existing EU initiatives and trusted ecosystems: using European AI services can help with data sovereignty and compliance. Third, adopt proven best practices and share information among peers. Collaboration is vital: no single organisation can keep up with attackers alone.

Looking ahead five years, who will have the upper hand?
It will remain an arms race. Attackers will always try to be one step ahead with new tools, perhaps post-quantum attacks or more sophisticated AI-driven exploits. Defenders must keep evolving, automating routine work so scarce human expertise can focus on complex threats. We will not eliminate the race, but we can stay competitive — and that is the real goal.

From risk to responsibility: What AI maturity really looks on the shop floor

Across Europe, organisations are discovering that implementing AI is as much about governance and culture as it is about data and technology. For Johan Lambert, who leads Risk Advisory Services at L&S Registered Auditors, the path to trustworthy AI begins long before the first algorithm is deployed. With experience in cybersecurity, quality and safety management, he explains what AI maturity really looks like on the shop floor.

As head of Risk Advisory Services at L&S Registered Auditors, Johan audits and advises organisations on cybersecurity, quality, environment and safety, and the governance of AI systems. Working across Belgium, the Netherlands, France and Luxembourg, he helps teams translate standards and regulations into practical controls and roadmaps. He focuses on making AI explainable, auditable and ready for production.

You audit companies across industries, from logistics hubs to manufacturing sites. In terms of AI, what are you seeing on the ground?

We see that there is a lot of experimentation going on, but also a lot of confusion. Many organisations still have a policy that literally says 'AI is prohibited', while at the same time their teams are quietly using it. That creates a dangerous gap, because people are using external tools without clear rules on what data can leave the company or who is accountable if something goes wrong. My first recommendation is simple: write an AI policy. Define what is authorised, what is not, and who decides. Once the rules of the game are clear, you can experiment responsibly.

That sounds like a governance issue. How do you help companies turn the policy into daily practice?

You start with a small group of AI champions: bring together IT, risk, operations and HR,

>>>

and give them a mandate to explore and test use cases safely. The key is language. AI only becomes useful once it understands the company's unique grammar: product names, operational codes, financial terms, etc. The same word can mean something completely different between business units. Without a shared vocabulary, you cannot compare outcomes or audit results. We often ask clients to document their definitions early and embed them directly in their ERP or knowledge systems. That is how traceability begins.

Traceability is a word auditors love. How does that apply to AI systems?

Traceability is the foundation of accountability and, together with explainability, the basis for trustworthiness. You must be able to explain how data was collected, cleaned, transformed and used. If you cannot, you will never be able to justify a decision. Documentation is not a bureaucratic exercise; it is what turns experiments into operational capability. When you know who did what, when, with which data and under whose approval, you can scale. If you do not have this oversight, you risk creating 'shadow AI' systems that no one can reproduce or defend. This is a real risk that the EU wants to collectively mitigate with the AI Act.

You also mentioned human factors. What are you seeing in teams?

People are under pressure. They hear that AI is moving fast and fear being left behind, so they rush in. But AI requires maturity. One careless query or mislabelled dataset can have cascading effects. Cognitive bias also plays a role. Humans tend to confirm their own assumptions, and that bias often becomes embedded in prompts or models. I see a real need for psychological safety so teams feel free to admit mistakes, but also clear authorisation requirements so that not everyone can connect to external systems unchecked. Because every model has at least one bias, I always refer to the well-known principle 'garbage in, garbage out'. Models and algorithms are rooted in human assumptions, including human bias. To illustrate this, I recommend the Cognitive Bias Codex, which can help in the detection and description of a wide range of common biases. It certainly raises awareness! Wikipedia also offers an interactive documented codex. The people tasked to be 'the human in the loop' should be able to refer to formally described biases. Furthermore, I prefer the term 'Quality in, quality out'.

Some companies build their own models, others rely on Microsoft, Google or SAP. Is there a 'right' approach?

There isn't really a 'right' approach. In practice, most organisations build on the large platforms and then adapt them to their specific workflows. What matters is not whether you build or buy, but how you control and assess the impact of every change. A new feature or model version should trigger a documented change request, just as in Secure DevOps. That discipline keeps systems reliable and auditable. Without it, you risk brittle solutions that no one fully controls.

You have been auditing management systems for years, from quality and safety to environment. How does that experience translate to AI?

AI follows the same logic. The new ISO 42001 standard on AI management systems is a good example. It brings AI into the same family as ISO 9001 or 27001, with risk management, controls and continuous improvement. It is not about slowing innovation, but about knowing what you are doing, documenting it, and improving over time. Exploratory projects can move fast, but high-risk use cases need deeper assurance.

>>>

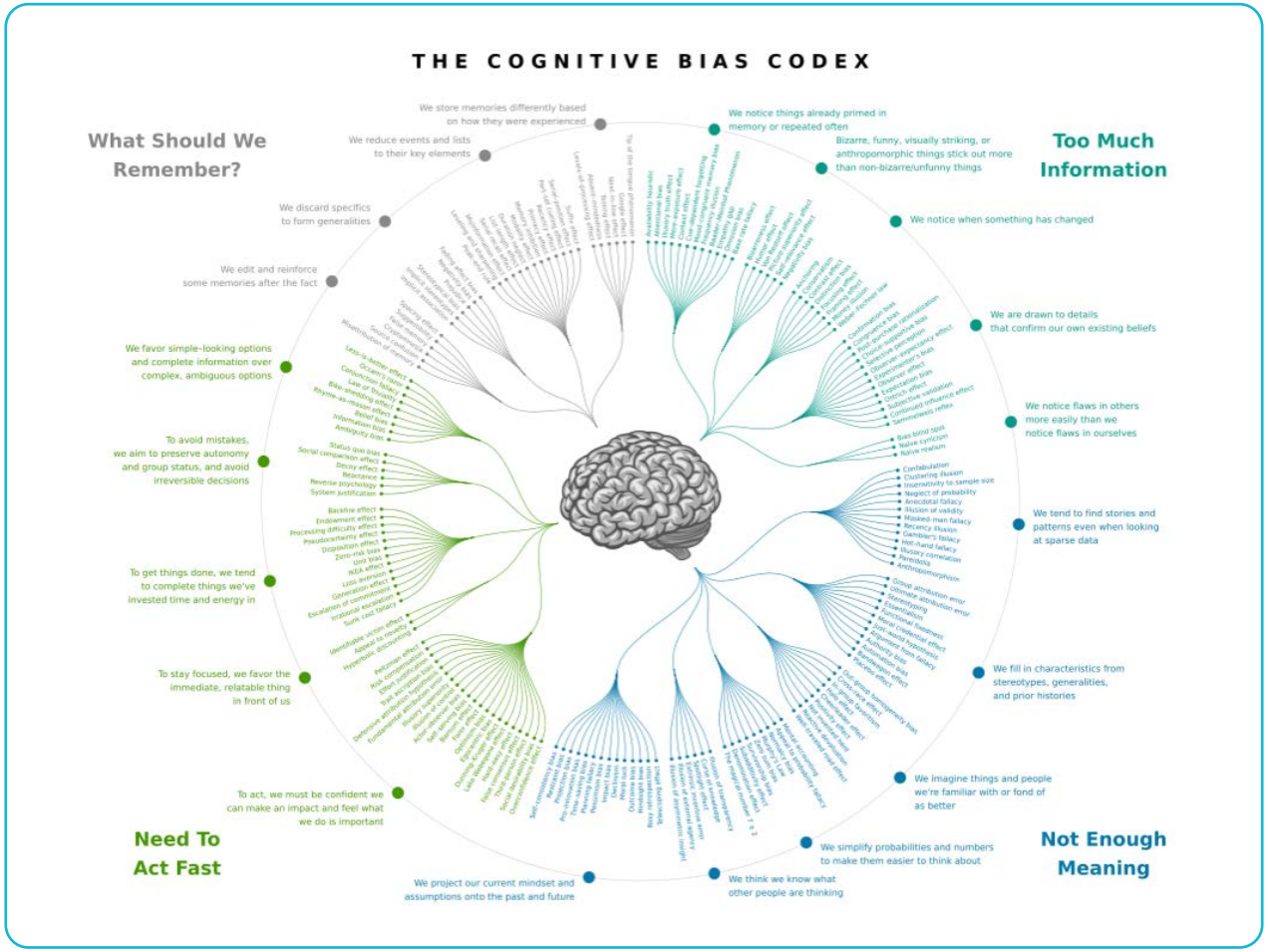
The test I use is simple: could you explain your system to an auditor, and would you be comfortable defending it after an incident?

One final point: talent. You have mentioned that younger engineers sometimes skip the 'logic' layer that older ones had to learn. Why does that matter?

Because AI hides complexity. Generative tools make it easy to code, but they also conceal the structure underneath. When you don't understand what is happening below the surface, you cannot detect systemic errors and hidden biases. I believe we should still teach young people to code, even if only to learn to think logically. That discipline develops your ability to reason about data and systems, and ultimately about responsibility.

So if you had to summarise the path from risk to responsibility in one line?

Write down how you will use AI. Teach the system your language. Teach your organisation the AI basics and set the basis for your own AI culture. Instrument everything suitably and adequately. Humans must always remain in control. Start small, document every change, and expand only when your controls hold. That is how AI becomes not just clever, but trustworthy.



“Trusting AI is different for a recruiter than for a heart surgeon”

Artificial intelligence (AI) is racing ahead and Europe is the first continent to put legal boundaries around it, with the AI Act. There’s an ongoing debate over whether this will strangle innovation or provide the trust that makes innovation possible. Jelle Hoedemaekers, Expert Data Economy at Agoria, works every day at that intersection.

Jelle Hoedemaekers specialises in policy on AI, data, and cloud at the European, Belgian and international levels. For more than seven years, he has been active in ICT standardisation committees. His mission is to ensure that companies—especially SMEs—can navigate the ethical, regulatory and technical challenges of the AI Act without losing sight of innovation.

AI Act is about to take effect, yet the technology it aims to regulate is still shifting under our feet. How do you legislate for something that refuses to stand still?
Regulation doesn’t inherently stifle innovation. Its clarity and coherence determine whether it enables or blocks value creation. Good regulation creates trust. But trust means quite different things in different contexts. If an AI tool is used to screen CVs, the key issues are bias, fairness and privacy. If it is used to support a heart surgeon during an operation, the bar is drastically higher: life-or-death accuracy, real-time reliability and safety validated in clinical trials. The AI Act tries to reflect this reality: low-risk systems face lighter obligations, while high-risk systems must prove safety, transparency and strong governance.

You describe trust almost as a currency. In concrete terms, how does regulation translate into competitive advantage?
Firms that can show their AI is fair, transparent and safe will win over clients, partners and regulators. A harmonised EU framework also reduces fragmentation and legal risk, making it easier to scale across borders. Done well, this is not about ticking boxes but about laying the foundations for sustainable innovation.

Most companies look at this as compliance, but you link it to something larger. Where does that perspective come from?
The AI Act raises the bar for the data economy.

>>>

Companies now need to check governance, auditability, transparency and bias. That adds cost, but also credibility. In democratic societies, unregulated AI can amplify misinformation, entrench discrimination, or undermine trust in institutions. By requiring transparency and oversight, the AI Act protects fundamental rights. For Europe and Belgium, it's about positioning: we may not outspend the U.S. or China in raw AI power, but we can lead in building a trusted digital economy where values are embedded in technology. That requires capable national authorities and clear, uniform implementation. If Belgium executes this well, it could even become a competitive advantage.
Still, compliance with the AI Act remains an area where we see significant risks, especially for SMEs. Belgium has many AI start-ups developing highly innovative solutions that bring substantial value. However, under the strict provisions of the AI Act, these companies will be required to make considerable efforts to ensure their solutions comply with the regulations. This is a key point that Belgian regulators should be particularly mindful of when implementing the AI Act.

Policymakers stress the importance of trustworthiness and fairness. When you sit with a company, how are these principles put into practice?

On their own, principles like trust and fairness are too vague. Standards define what level of accuracy is acceptable, how documentation must be kept, how bias should be tested.
In finance, for example, an AI system that calculates loan repayments must prove it does not systematically disadvantage certain groups. In public services, when authorities use AI to allocate benefits, citizens have the right to clear explanations and safeguards. Transparency also depends on the audience: a customer might need a simple explanation of why a loan was refused, while regulators will demand full technical documentation.

What are the potential pitfalls for Belgian companies when dealing with the risks of AI?
The first gap is awareness: many firms don't even know what AI they are already using - whether embedded in software, offered as SaaS, or developed internally. The second is role definition: companies are often unclear as to whether they are providers, deployers, or both - and that matters enormously for their obligations. And third, training is underestimated. The AI Act explicitly requires that when employees are given AI tools, employers must also provide training so they know how to use them responsibly. Without that, the risks of misuse or data leaks rise sharply.

If you were advising a CEO tomorrow morning, where would you tell them to start?
With an inventory. Map all the AI systems in use across the company. Align that with the European definition of AI so you have a clear understanding of what falls under the Act. Once you know what you have, clarify your role: are you a provider of models, a deployer, or both? Each role carries different obligations and timelines. Then assess the risks: what could go wrong with each application, who might be affected, and how serious could the harm be? That assessment shows which systems may be high-risk and require stricter checks or even restrictions. Alongside this, set up governance structures: data management policies, bias-mitigation processes, documentation and monitoring of models over time.

When you put it like that, the Act sounds less like a legal straitjacket and more like a chance to build credibility.
Exactly. Preparing in this way is less about checking off requirements than about embedding trust and foresight into everyday business. Companies that take it seriously will not just avoid fines, they'll also gain an edge in markets where reliability and ethical use of AI are decisive.

AI and the Path to Digital Trust: Real-Life Blueprints

Artificial Intelligence (AI) has permanently changed the rules of cybersecurity. Recent innovations show a convergence of approaches across industries: blending proactive risk detection, data quality, privacy and advanced machine learning techniques. Two compelling examples – EURid's domain name abuse prevention and early warning system (APEWS), and CETIC's Federated Learning project with a cybersecurity case study that includes anomaly detection (AIDE), demonstrate the transformative impact of AI on how we secure online infrastructure. While rooted in different contexts, their underlying philosophies reveal key lessons for the future of digital trust and cybersecurity.

"The programme I lead focuses on abuse prevention within the .eu domain name framework. Our goal is to support public authorities and protect consumers," explains Philip Struyf, Program Manager in Domain Name Abuse Prevention. "In the past, detecting abusive registrations was a manual process, time-consuming, largely reactive, and often slowed down by the delay between registration and response. But with increasing pressure from both regulatory bodies and the market to ensure a safer digital environment, it became clear that a new approach was needed."

EURid is the registry for the .eu domain name. In 2019, it embarked on a transformation journey to develop an innovative methodology capable of predicting whether a domain name could potentially be used in an abusive manner. The AI-powered solution, developed in collaboration with KU Leuven, combines predictive machine learning models with rule-based logic to assess the likelihood of abuse at the point of registration, before a domain even goes live. It analyses detailed registration metadata not only to flag suspicious registrations for immediate suspension, but also to trigger layered "Know Your Customer" procedures. In other words, if a domain name holder fails to verify their identity, the domain is withdrawn before it can cause any harm. The approach relies on close collaboration among all actors involved in the registration process.

>>>

Philip Struyf

"Thanks to this capability, we can now act the moment an anomaly is detected," explains Struyf. "It allows us to stay one step ahead, protecting the integrity of the .eu space and ensuring a more reliable digital landscape for everyone."

Data quality and federated learning

At the same time, CETIC, an organisation that aims to translate existing ICT expertise into business applications in Wallonia, has advanced anomaly detection through the use of AI. The central challenge is that, because organisations are understandably reluctant to share sensitive logs or proprietary information, context-rich anomaly data is extremely scarce. "To make a system effective at detecting irregularities, you first have to teach it to recognise 'normal' behaviour. This is crucial to avoid too many false positives," says Philippe Massonet, Scientific Coordinator at CETIC.

"It's a complex task, but by experimenting with different learning methods, we have managed to create a workable system. A key element in this success is our use of federated learning: a pioneering technique where models are trained locally on private organisational data," Massonet continues. "Rather than sharing raw data, only model parameters or updates are aggregated centrally. This not only preserves privacy but also enables much richer training."

Blueprints to digital trust

The AIDE project, funded by the Federal Public Service Policy and Support (FPS BOSA), clearly demonstrates the strong growth potential of this approach. "You can continue to train and apply it in different contexts by using more specific data as training material for the systems," Massonet explains. "CETIC therefore actively invites organisations across sectors to participate, with a vision to develop use cases from healthcare to banking and critical infrastructure." The AIDE project on Federated Learning is a collaboration between KU Leuven, Ghent University/IMEC, UCLouvain and CETIC.

A similar sense of optimism can be felt at EURid. "Our current project should be seen as a building block within a larger infrastructure," says Struyf. "We are currently expanding the system, primarily by making it modular through containerisation, paving the way for cross-registry cooperation while remaining fully compliant with strict data protection laws."

EURid and CETIC both suggest a blueprint for a future in which they successfully combine abuse prevention and anomaly detection with unprecedented collaboration, a strong commitment to privacy, and proactive risk management. The path to digital trust lies not only in smarter algorithms but in the intelligent networking of people, processes and systems working together toward a safer, more resilient cyber ecosystem.

Philippe Massonet

Forging digital trust in the Age of AI

At the GRC: Be Connected! Lustrum event, Allan Boardman, an Independent Business Advisor with CyberAdvisor.London, 2023 ISACA Hall of Fame Inductee and seasoned professional with extensive experience in audit, risk, security, and governance, delivered a compelling presentation. He explored the transformative power of Artificial Intelligence (AI) within the industry and the significant opportunities and challenges it presents for GRC and security professionals. We sat down with Mr. Boardman to delve deeper into the key aspects of his presentation and gain further insights into this rapidly evolving landscape and the need for digital trust.

Your presentation highlighted that "The Age of AI has Begun...". What does this mean for you?

Allan Boardman: "I firmly believe that the development of AI is as fundamental as, or even more so than the creation of the microprocessor, the personal computer, the Internet, and the mobile phone. Entire industries are poised to be reoriented around it, and businesses will increasingly distinguish themselves by the effectiveness of their AI adoption. The public release of ChatGPT in November 2022 ignited a revolution. Since then, AI adoption has surged, and new competitors have emerged, most recently DeepSeek in January 2025. This feels like the most significant digital disruption of our era.

You also outlined several key risks and challenges. Could you highlight some of the most pressing concerns and how they should be mitigated?

Allan Boardman: "Well, there's quite a spectrum of risks organisations need to be mindful of. Forbes highlighted fifteen key risks, with the top three being a lack of transparency, bias

>>>

and discrimination, and privacy concerns. This indicates a clear need to develop AI in an ethical way proactively. Specifically, addressing various biases—whether they are gender, racial, socioeconomic, or content-related—is paramount for ensuring fairness and equality in AI outcomes. Building trust hinges on transparency, meaning clear visibility into the data used, the models employed, and the decision-making processes.

And then there's privacy, which is absolutely critical given the use of personal data by AI. This requires robust security measures to prevent breaches and unauthorised access. Even anonymised data can pose risks of re-identification, and AI tracking raises legitimate surveillance concerns. Furthermore, poor data handling can amplify existing biases and lead to discriminatory outcomes. So, in essence, organisations need to implement strong data protection measures, establish transparent consent protocols, and develop clear policies for how AI is used."

The spread of misinformation is increasingly prominent. What are your thoughts on these matters?

Allan Boardman: "This is a significant area of concern. The rapid spread of false information through AI can erode trust in media and institutions. AI can be used for manipulation, fraud, and even political interference, and deepfakes are often challenging to detect and verify. Developing advanced detection tools, promoting digital literacy, and enforcing stringent regulations are essential to combat this."

AI security risks also present unique challenges...

Allan Boardman: "Certainly. When we discuss security risks, organisations are navigating a complex landscape. We are talking about threats like data breaches, malware and hacking specifically targeting AI systems, exploitation of vulnerabilities within those systems, and adversarial attacks designed to manipulate AI inputs. And of course, there are insider threats, where individuals misuse AI capabilities. A particularly concerning area is what's called 'Shadow AI' – the unauthorized use of AI tools. This introduces a whole new set of risks, including potential data security breaches, compliance violations and intellectual property risks. To effectively mitigate these risks,

>>>

organisations must implement robust security protocols and maintain continuous monitoring. Furthermore, we're seeing the emergence of so-called jailbreaks with large language models, or LLMs. This is where users cleverly manipulate prompts to bypass the safeguards and content policies built into these models. These jailbreaking patterns are often shared widely on social media, which exacerbates the problem."

The legal and regulatory landscape surrounding AI is clearly in flux. What are some of the key approaches being taken globally?
Allan Boardman: "The legal landscape is indeed changing rapidly as regulators and lawmakers around the globe strive to keep pace with AI development. We are seeing three distinct approaches to regulating AI. The first one is a single risk-based law to regulate AI systems broadly, as seen in the EU, Canada, Brazil, and South Korea. The EU's AI Act, passed in March and approved in May 2024, is a prime example, focusing on managing risk from AI systems by classifying them into different risk levels with corresponding controls.

The second approach involves various narrow laws to regulate specific applications or domains of AI, which is the predominant approach in the US and China. In the USA, there is no single federal AI law, with regulations issued by different agencies depending on the sector. However, key laws like the National AI Initiative Act, the Fair Credit Reporting Act, the Americans with Disabilities Act are relevant in this respect.

Jailbreaking patterns are widely shared on social media, which exacerbates the problem.

The third approach is based on regulator-led initiatives supported by frameworks and strategies, as adopted by the UK, Australia, Singapore, and Japan. The UK, for instance, published an AI Strategy focusing on innovation and responsible development and is considering a legal framework for high-risk AI. Interestingly, India announced in late 2024 that it would not directly regulate AI but focus on voluntary codes instead."

Given these varying approaches and the inherent risks of AI, are there any established frameworks that organisations can adopt to manage these challenges effectively?
Allan Boardman: "Yes, there are certainly valuable frameworks available. The NIST AI Risk Management Framework (AI RMF 1.0) provides a comprehensive and flexible approach to managing risks associated with AI systems. It aims to foster trustworthy AI by focusing on ethical, reliable, and transparent development and deployment practices. Another important standard is ISO/IEC 42001:2023 – Information Technology – Artificial Intelligence Management System (AIMS). This provides guidelines for establishing, implementing, maintaining, and continually improving an AIMS. It is the world's first AI management system standard and offers valuable guidance for responsible AI adoption and governance."

The title of your presentation also mentioned the intersection of AI and cybersecurity, and the concept of digital trust. How do these elements connect?
Allan Boardman:" So, the question we need to ask ourselves is whether AI poses a threat or turns out to be an asset in cybersecurity.

>>>

AI offers immense potential for automated threat detection, rapid response and adaptive defence mechanisms, boosting security. However, we must address data quality, privacy, over-reliance on AI, and the danger of AI systems operating autonomously. Careful implementation is key to leveraging AI as an asset, rather than a threat, in cybersecurity.

As GRC professionals we all want to be building trustworthy systems and help organisations implement AI safely, securely, ethically and responsibly. Digital Trust encompasses the ability of people, organisations, processes, information, and technology to create and maintain a trustworthy digital world. ISACA, for instance, has developed a framework to develop such a digitally trustworthy ecosystem.

In the context of AI and cybersecurity, building digital trust requires prioritising governance and accountability, ensuring transparency and explainability of AI algorithms, and upholding data privacy and security. We cannot achieve this in isolation; collaborative engagement among industry, government, and academia is critical."

Could you provide some concrete examples of how AI is being applied in GRC?

Allan Boardman: "Certainly. In audit, AI use cases include fraud detection, risk assessment, ensuring regulatory compliance through automated checks, process automation, anomaly detection, continuous monitoring, and even automating the generation of audit reports. In cybersecurity, tools like Microsoft Security Copilot demonstrate how AI can assist with incident response by providing guidance and insights, threat hunting by analysing large datasets, intelligence gathering from various sources, providing policy insights and resolutions, automating tedious tasks, building queries and analysing scripts, and managing overall security posture. For risk management, AI can be used, among others, for risk identification through data analysis, predictive analytics to forecast future risks, automated monitoring of risk indicators, scenario analysis, ensuring regulatory compliance, and fraud detection."

What are your concluding thoughts for GRC professionals navigating this era of rapid AI advancement?

Allan Boardman: "My final thoughts echo the need to engage, embrace, and empower ourselves with AI. Generative AI offers extraordinary possibilities, but addressing the associated risks is crucial for building trust and ensuring a positive user experience. Regular updates and continuous monitoring of AI systems are essential for their effectiveness. Prioritising security and privacy is paramount to protect users and ensure compliance. Ultimately, balancing the benefits and challenges will enable the responsible and ethical use of AI. As others have noted, the internal audit profession, for example, is at a crucial juncture. We must embrace AI as both a catalyst and a tool to remain relevant and deliver strategic value in this ever-changing world. Therefore, I urge everyone to explore and embrace AI and feel empowered to supercharge their careers!"

AI: Empowering women or reinforcing bias?

With the rapid rise of technology, particularly artificial intelligence, a lot of new challenges are emerging. One critical issue is that AI systems are showing alarming signs of bias—reinforcing gender inequality in many areas. Cyber Security Coalition spoke about these important challenges with Mrs. Catherine Van de Heyning, Professor European Fundamental Rights at University of Antwerp, Public Prosecutor and Expert Advisory Committee UN Human Rights Council. She was one of the keynote speakers at the International Women's Day event co-organised by the Coalition and Women4Cyber Belgium and hosted at the Belgian Federal Public Service Economy in Brussels.

Let's start with a big question: do you think AI is good or bad in general, and more specifically for gender equality?
Dr. Van de Heyning: "I truly believe that AI has many benefits and offers huge possibilities to improve our lives. And not just in general or in a professional context, but for more empowerment and equality as well. There are tons of examples where AI has already generated more equality. One of my favourite projects is one of UNDP, which is called eMonitor+. Basically, it uses AI to promote information integrity and monitor the potential of conflict, considering violence against women and online violence. Another example are AI driven tools like the one Glassdoor is using to see whether there is real equal pay in vacancies."

But AI is still doing more bad than good today for gender equality?
Dr. Van de Heyning: "Unfortunately, there is currently a decline of gender equality because of AI as well, and there are many examples of more violent behaviour against women and

>>>

girls because of AI. There are a few triggers to consider. The first one is bias. We're seeing it in the development of AI, from deepfakes to algorithms and voice cloning. AI tools are trained on data but when that data in research or our society is biased, then the output is biased as well. Moreover, even though there are more women working in the tech industry today, only about one out of five people working in AI are women and mostly not in a developer role. This does not mean that male developers actually want to have this bias, but the reality is that they are not always aware of it."

Can you give some examples of this bias?
Dr. Van de Heyning: "Look at AI that is being used in healthcare. We already know that in science, women's health has been under-evaluated, that some of the criteria that are specific to women have not been included in research and data. And that causes bias from the source. Fortunately, there are some incredibly good initiatives such as the Female Heart Hospital of the University Hospital in Antwerp that is really focusing on female heart problems. So, it's not just about the applications, it's also about ensuring that there is sufficient research and sufficient data out there about women.

Another example are the well-known AI image creators. We all love them because you can be so creative making cool new images for presentations, for example. And yet, most of these image creators are clearly biased. Ask for image of a judge, a CEO or construction worker and you will get a male in the majority of the image creators. If you ask for one of a cleaner or a teacher, you'll get a female. But it's also about the way they are portrayed, which is often in a very stereotypical or even downright sexist.

All these types of bias stimulate a certain perception of women. We all want to believe AI should be objective. And yet, some of these tools have been trained and retrained for years, they can be recalibrated, and recoded to make them search also for other data, but apparently that has not been done properly so far. From the start of the design that seems to have been disregarded."

Next to bias, what else is alarming you?
Dr. Van de Heyning: "One of the most problematic things is absolutely disinformation. AI is playing into that evolution, and in a gender-related way. We see examples of political opponents being sidelined for instance through deep fake interviews that never happened. Also, there are several AI bots now really pushing out specific information on gender. And of course, one of the very worrying trends is deep nuding, where AI is being used to portray women as if they were naked. In research from already two years ago, we found that more than half of the 15- to 25-year-olds knew about deep nudes, and 8 per cent had already made deep nudes. Thankfully, it is criminalized to disseminate these pictures due to new EU regulation and in Belgium it is also illegal to make them."

Are there any solutions out there to combat this?
Dr. Van de Heyning: "There are technical solutions, including those using AI. A tool like Alecto AI, for example, scans the internet for non-consensual intimate images in order to take them down. But now we already see fake accounts asking for nude images claiming that your image has been or will be disseminated, and they will help you prevent it. But indeed, we need to go a lot further and work towards an AI gender-based agenda."

What should such an agenda look like?
Dr. Van de Heyning: "First of all, we need to work on responsibility and awareness. Recently,

>>>

there was an AI summit in Paris, showing that a lot of nations are coming together and want change. And that can only be done with real responsibility. And this responsibility from the tech industry should be for the whole technology life cycle. So, not just when something goes wrong but also prevent it from going wrong. I think the only way you can do that is via liability and regulation.

Next, we need to implement gender-neutral by design. At the start of a design, companies need to think about gender neutral solutions that will avoid harm and are also not biased. Generating awareness for that is key, for example through bias training for employees, in particular for developers. We do need more female developers in the team, but we also need men to be conscious of their bias and its potential impact.

Finally, AI regulation is essential as well. In some parts of the world, they want to deconstruct regulations because they are bad for business. But we are Europeans. We have old houses, and we renovate them. We do fantastic things with our cities that have been there for centuries. And that's how we need to think about technology. Within constructs that are good for society, and certain regulation, you can be creative and safe at the same time."

How do you look at the future in these challenging and uncertain times?

Dr. Van de Heyning: "I am very convinced that we need a new agenda. I believe there is really a potential new era for Europe, because we will have the opportunity to create and market new products that are not harmful, and people can trust. Of course, funding from the EU, governments and companies is necessary to fuel this innovation, but now is the time to fill the gap for people looking for alternatives. At the same time, we can also have an agenda where we foster, where we mentor, where we include a more unbiased workforce to create the AI of the future. Even if there are many challenges ahead, today can be a restart for Europe, a restart for Belgium to think differently about technology."

Building resilience in a world where cyber criminals are using AI

As the Cyber Security Coalition marked its 10th anniversary, Kathryn Hedley, Certified SANS Instructor and Director and Digital Forensic Specialist at Khyrenz Ltd., took the stage to reflect on two decades of cyber security evolution and what lies ahead. Kathryn sees resilience not just as merely defensive: "We will also need to adapt and thrive in an increasingly complex threat landscape."

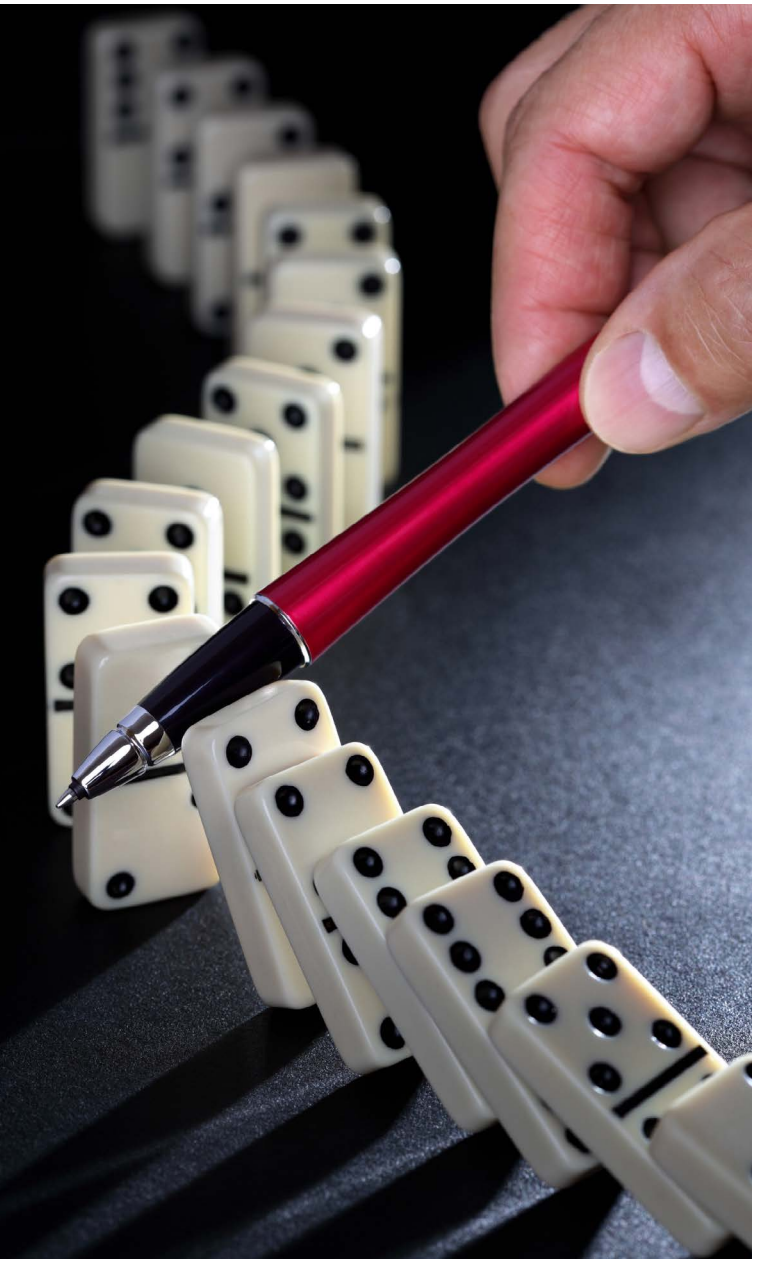
Our ability to detect, respond and adapt determines the impact.

The challenge of authenticity

Hedley walked the audience through the radical shifts in digital forensics over the last 20 years. "When I started, we analysed single systems, such as computers that contained just a few hundred gigabytes of data. The main cases involved credit card fraud and copyright infringement. Fast forward to today, and we're dealing with globally distributed networks, sophisticated botnets, and cyber criminals who no longer leave behind easy-to-trace footprints."

She highlighted the rise of ransomware, deepfakes and AI-generated cyberattacks. Attackers are leveraging encryption, anonymisation techniques and anti-forensic methods to cover their tracks. "We've entered an era where cyber criminals are erasing logs, manipulating timestamps, and leaving minimal forensic evidence," she warned.

>>>



One of the most pressing concerns, according to Hedley, is the growing difficulty in distinguishing reality from manipulation. "Deepfake technology and AI-generated content are making it harder to verify authenticity. This is already affecting legal cases, intelligence gathering and even everyday communications," she noted.

Hedley shared an example of AI-generated images that misrepresented the age and identity of an individual, emphasising how these tools could be weaponised. "This is not a problem for the future… it's happening now! Cyber security professionals must develop new verification methods to counteract digital deception."

Building resilience: a proactive approach

While the cyber security landscape is evolving rapidly, Hedley offered a structured approach to strengthening resilience. "Cyber attacks are inevitable, but our ability to detect, respond and adapt determines the impact." She outlined 4 key strategies:

- **Forensic readiness:** Organisations must ensure they have the right data logging, storage and retrieval systems in place before an incident occurs.
- **Continuous monitoring:** Cyber security is no longer about reacting to attacks but actively hunting for threats within networks.
- **AI-driven defence:** While attackers leverage AI, defenders must do the same by integrating AI-driven detection and response mechanisms. However, we must continue to validate our tools to ensure precise detection of threats and minimize false positives.
- **Cyber crisis simulation:** Just as fire drills prepare for emergencies, companies should conduct regular cyber security simulations to refine their response strategies.

Kathryn Hedley concluded with a call for stronger collaboration across industries. "The difference between us and cyber criminals is that they operate in silos while we work together. We share intelligence and resources. That's our advantage, and we must continue to leverage it."

Theme 4

Building a post-quantum future

Marc Delincé

“A post-quantum transition is more than just software being replaced”

To safeguard our way of life and work, we must make post-quantum cryptography a priority now. Addressing the challenges of this transition will require large-scale awareness efforts around its impact and implications. Marc Delincé and Lorenzo Bernardi, respectively Senior Advisor and Head of Security Services at NRB, stress the importance of collective intelligence and knowledge sharing.

In a world where data is the core of nearly every process or competitive advantage, encryption is the backbone of its functionality. “It’s everywhere: from internet protocols, critical infrastructure and banking systems to blockchains,” says Delincé. “However, most companies remain insufficiently aware of this. Given that a significant portion of classical encryption will become breakable in the quantum era, it is more crucial than ever to focus on raising awareness around the issue today.”

‘Harvest now, decrypt later’

Quantum physical principles such as superposition and entanglement are leveraged by quantum computers, which manipulate quantum effects to decipher complex optimisation and situational problems that classical computers can’t efficiently handle. As a result, they are expected to be able to cause a ‘crypto-crash’ within the next decade. “Enormous investments are being made in the quantum race, especially in China,” says Delincé. “It is essential to emphasise that this means the threat is actively taking shape.”

Bernardi builds on this point: “Attackers are already thinking in terms of ‘harvest now, decrypt later’: storing encrypted traffic they intercept today to decrypt it when the hardware is available.” This is why both believe intelligence agencies around the Western world are setting openly aggressive deadlines for emergency and transition plans

>>>


Lorenzo Bernardi

towards post-quantum cryptography. “In this context, we see that Belgium, which by virtue of its role as the host country for the historic Solvay Conferences, can be considered as a catalyst of quantum physics,” says Delincé. “Private and semi-public collaborations such as Quantum4Belgium, Quantum Circle and the Cyber Security Coalition are taking action, consciously - and rightly - to accelerate the pace,” Delincé continues.

In this context, post-quantum cryptography (PQC) is increasingly coming to the fore. “These are cryptographies based on different mathematical principles, and do not require a quantum computer,” says Delincé. “They do however have practical implications, including larger keys, more bandwidth and more CPU. In practice, companies will always face a trade-off between how far they want to go and where they want to add this different layer of encryption. Furthermore, the fact that the organisation is paying today against a future incident is quite abstract, which makes it difficult to build a business case.”

Crypto-agility

In other words, this is also a matter of infrastructure, an area in which NRB, as a leading player in Belgium’s IT sector, delivers end-to-end IT solutions and services. “A PQC transition is a multi-year process. It’s about more than just replacing software; sometimes, it’s a matter of hardware too,” Bernardi explains. “Companies that are waking up to our interconnected reality must not only adapt their own environments based on a thorough inventory, but also involve other partners in their ecosystem. Consequently, there will always need to be hybrid modes to bridge this gap. This all requires time, skills and budget.”

Such initiatives, which must be laid out in a context- and company-specific roadmap, should ultimately lead to crypto-agility. For NRB, this is not just a buzzword but a principle. To create a legacy for tomorrow, a governance structure must be established that can be continuously updated. “Collaboration and knowledge sharing are essential to achieve our goals. In addition to the Quantum Circle, the Belgian Cyber Security Coalition, which focuses on collective intelligence and resilience through concrete issues and experiences, is a very relevant platform. L’union fait la force,” says Bernardi.

Belgium can be considered as a catalyst of quantum physics.

Successfully addressing this massive security challenge requires near-immediate efforts to foster a culture where security in the quantum world is viewed as a dynamic system. “In addition to early awareness and clear roadmaps focused on mutual collaboration, training – both in education and especially ongoing professional development to build up the muscle memory of those working on the ground – is absolutely essential,” Delincé concludes.

“Post-quantum is, above all, an opportunity to get our house in order”

Building on the awareness that Belgium will need to catch up significantly in the coming years when it comes to quantum, Jan Sonck founded the Quantum Circle two years ago. The initiative’s significant traction shows that mindsets are maturing and, according to Jan, 2026 will be a tipping-point year.

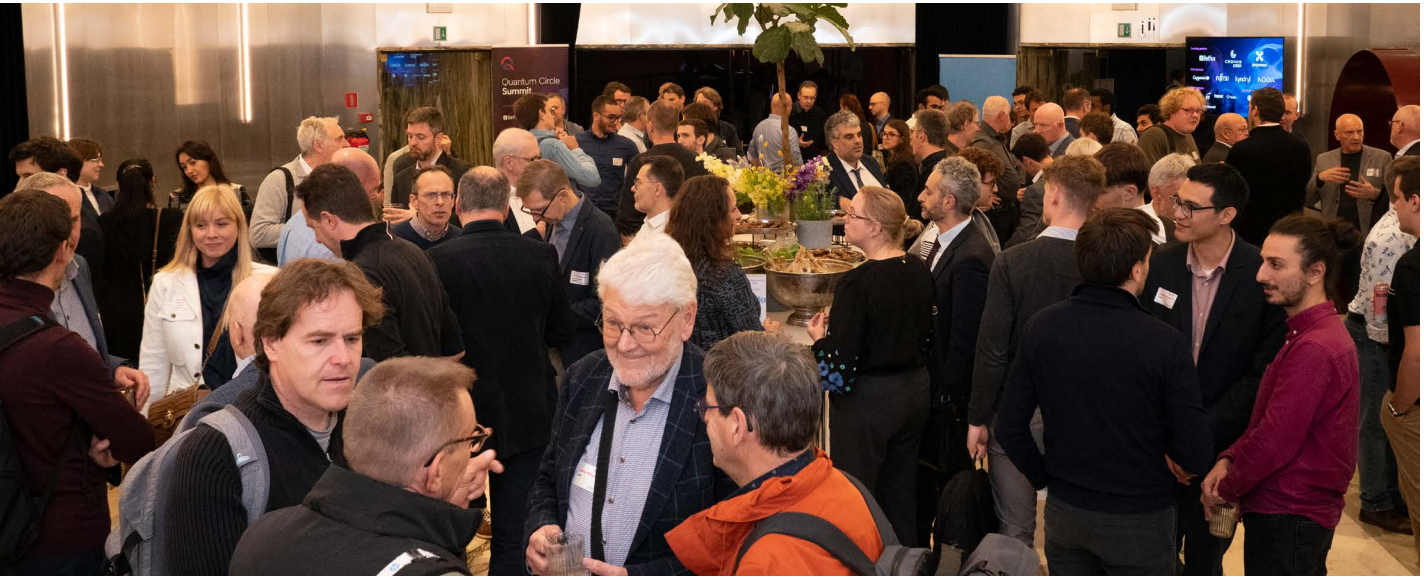
“Since we first launched the Quantum Circle in Belgium, we have built up a core group of around fifteen active ‘doers’, a wider circle of some 200 interested parties, an online platform with roughly 250 profiles from about 100 organisations, and a newsletter reaching approximately 750 contacts,” Sonck explains. It’s a strong start, fuelling far-reaching ambition. “We want to be a lever that lifts Belgian companies and public authorities from asking ‘what is quantum?’ to asking ‘which concrete use case should we tackle, and when?’”

That shift, he believes, is exactly what the post-quantum security discussion needs right now, especially considering the widespread misunderstanding about the urgency. “Since it’s generally assumed that the first generation of powerful quantum computers will arrive within eight to twelve years, and migration is expected to take four to five, many decision-makers conclude there’s still plenty of time,” he says. “That’s a shame because they will miss out on the current momentum, which is brimming with opportunities.”

Act now, or miss the opportunity

Sonck therefore argues for a different way of looking at post-quantum cryptography (PQC). “PQC isn’t just an answer to a future threat, it’s an opportunity to get our house in order today,” he states firmly. The way organisations approach the broader cybersecurity challenge of PQC offers a powerful illustration of why this matters. Anyone who wants to take PQC seriously must first understand where cryptography actually lives: in an inventory

>>>



of keys, certificates, protocols, applications and dependencies. Next comes the often-underestimated step of data classification and a clear understanding of data flows. “Only once those steps have been completed can you assess where current security falls short and where ‘crypto-agility’ is lacking,” Sonck adds.

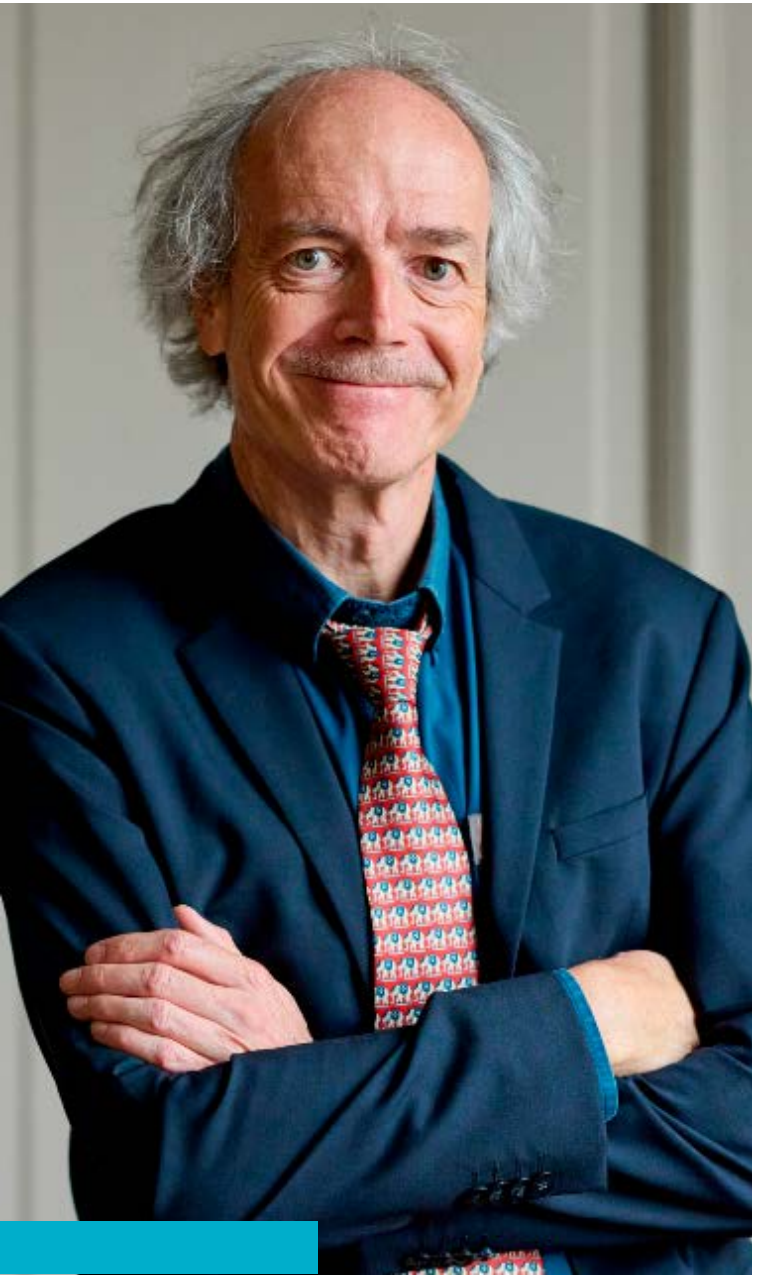
In large organisations, this is not a minor technical project but rather a broad clean-up of IT and security: areas that have been neglected for far too long, often until something goes wrong. Tackling the exercise in phases keeps costs under control while simultaneously building market pressure. Sonck draws parallels with how ESG has been used in recent years: as a procurement lever to systematically set requirements for suppliers and make post-quantum readiness a standard condition in renewal cycles.

What matters most, however, is avoiding a ‘wait-and-see’ attitude. “You can compare it to how we consider gas as a heating source in homes. If you’re building a new house today and still opt for gas ‘just to see where we are in 10 years’, you’re taking a predictable risk. You know the context is changing, so you’re better off designing with the future in mind,” he explains. “In practice, we still find plenty of examples of this wait-and-see attitude. Just look at the European car industry, which is actively putting the brakes on electrification.”

Tipping-point year 2026

Thus, the Quantum Circle’s ambition extends far beyond the security narrative. “We start from three broad domains: quantum computing, quantum communication and quantum sensing. Security doesn’t actually fall under these,” he says. At the same time, the community cannot and will not ignore the many questions surrounding post-quantum cryptography, which is why he believes in a strong synergy between the Quantum Circle and the Cyber Security Coalition.

Intensive collaboration is sorely needed in Belgium, as it faces a real gap. “We’re a country of SMEs, which puts us at a disadvantage. Multinationals’ quantum teams are often located outside our borders, and the expertise is ‘in the cloud’ of the parent company. On top of that, unlike Europe’s leading countries, we lack national plans and investment programmes.” Despite this — or perhaps because of it — Sonck expects 2026 to be a tipping-point year. “Very concrete use cases provide compelling evidence with remarkably strong persuasive power.”



“The transition to quantum-safe communication needs to start today”

A world without cryptography is unthinkable in our digitalised society. While Belgium possesses strong academic expertise in this field, this is no guarantee for a worry-free future. New technologies, such as quantum computers, could potentially undermine all we have relied on for years. Professor Bart Preneel (KU Leuven) illuminates the challenges, and sees a crucial role for the Cyber Security Coalition.

Cryptography is the technology that shields information and makes it accessible only to those with the correct key. It secures online transactions and identity checks, protects medical records, and ensures that software updates are safely implemented. “Because cryptography is so omnipresent, the impact when security fails is significant,” says Professor Preneel. The greatest challenge ahead comes from quantum computers. “They will bring life-saving breakthroughs in fields like medicine, but at the same time, they pose a threat to our digitalised society.” Millions of applications are at risk of becoming vulnerable in the future. “Much of cryptography is based on mathematical problems that quantum computers could quickly solve,” Preneel explains. Although the breakthrough of quantum is not imminent, vigilance is already necessary. “Sensitive information intercepted today could be cracked in 15 or 20 years. That’s why governments and organisations must take action now: map out processes, identify quick wins, and create a migration plan. Because a software migration can take many years.”

Strong in knowledge, not yet in policy

In the field of cryptography, Belgium has an edge over other countries, thanks to its renowned research institutions. From the first chip cards to the Advanced Encryption Standard (AES), our academics have made significant contributions to the security of many systems. “Belgium continues to play

>>>

a key role in the research into algorithms that can be used in quantum computers," Preneel states. "Thanks to our unique culture of collaboration and decades of investment in academic research, our country remains a cryptography pioneer."

However, strong expertise alone will not suffice to overcome all the challenges; we also need clarity on how far we are willing to go in controlling and protecting our data. "Many governments want to access encrypted information in order to fight crime and terrorism. But this carries a risk: once you create backdoors, you undermine the entire system's security. This has already been proven multiple times." Professor Preneel believes that Belgium is too ambivalent in this regard: "Many of our businesses and organisations are highly vulnerable and not agile enough. We need to act now and make the necessary preparations."

The power of collaboration

Collaboration is crucial for this shift, because companies and governments cannot achieve the transition to post-quantum cryptography on their own. "Here, the Cyber Security Coalition can play a critical part," highlights Preneel. Within the Coalition's Cryptography Focus Group, knowledge and experiences are shared, whitepapers are published, and presentations are given to help businesses develop their own strategies. "By doing so, we put issues on the radar, increase awareness, and develop tools that translate new regulations into practice. This is essential because the transition won't happen on its own: it will take time, money and collective efforts."

The topic will only become more important in the coming years. "Apart from the challenges that quantum raises, investing in your own security remains crucial. The damage after an incident is always greater than the investment needed to prevent it." Preneel concludes with a clear message for policymakers: "Ensure more coherent regulations, because today it's a tangled mess. Only by continuing to invest and improving collaboration can we secure our digital future."

Post-Quantum Cryptography: It's time to act!

Quantum computers are no longer science fiction-they're becoming a reality. While they promise breakthroughs in fields like medicine and logistics, they also pose a serious threat to today's encryption systems. Algorithms like RSA and ECC, which protect our emails, financial data, and digital identities, could be broken by quantum machines. Post-quantum cryptography is our defence. It's a new generation of encryption algorithms designed to withstand both classical and quantum attacks.

These algorithms are built on hard mathematical problems that even quantum computers struggle to solve. The urgency is real: attackers can "harvest now, decrypt later", meaning data stolen today could be decrypted in the future once quantum capabilities mature. That's why organisations must start transitioning now—before it's too late. Post-quantum cryptography isn't just a technical upgrade. It's a strategic move to safeguard digital trust in the quantum era.

Theme 5

Cyber-ready, AI-smart, and inclusive

“We need a fundamental cultural shift within SMEs”

Whilst cyber threats are continuously evolving, it is essential for SMEs to grasp the urgency of cybersecurity. For Hugues Mertens, founder of About IT and active for over a decade in supporting SMEs through their digital transformation, cybersecurity forms the backbone of every organisation, regardless of its size. “SMEs have no choice but to regularly invest in updates and new systems.”

Although Belgium has made significant strides in cybersecurity in recent years, many SME leaders still struggle with a degree of naïveté. “The CEO of a small company still often says: ‘We are too small; hackers won’t target us.’ But that is a fundamental misconception,” Mertens explains. “Cybercriminals do not only target large corporations; every organisation is a potential target. When an attack does occur, the consequences can be devastating. The damage extends beyond financial losses - it affects trust, reputation, and even the continuity of the business.”

Technological Debt

At the same time, Hugues Mertens notes positive developments in Belgium. The cybersecurity ecosystem is stronger than ever. Organisations such as the Cyber Security Coalition, the Centre for Cybersecurity Belgium (CCB) and Agoria contribute to a joint effort to address cyber risks. Through this collaboration between public and private actors, Belgium is better equipped than many other countries. “Yet today, it is still not enough. The success of this effort depends on the engagement of all players, including smaller businesses, and therefore the SME landscape,” he adds.

According to Mertens, SMEs must become more conscious of their accumulated technological debt. “Many companies still operate with outdated systems that are inefficient but also extremely vulnerable to attacks,” he says. “Consider, for example, aging servers or the lack of a coherent cloud strategy.”

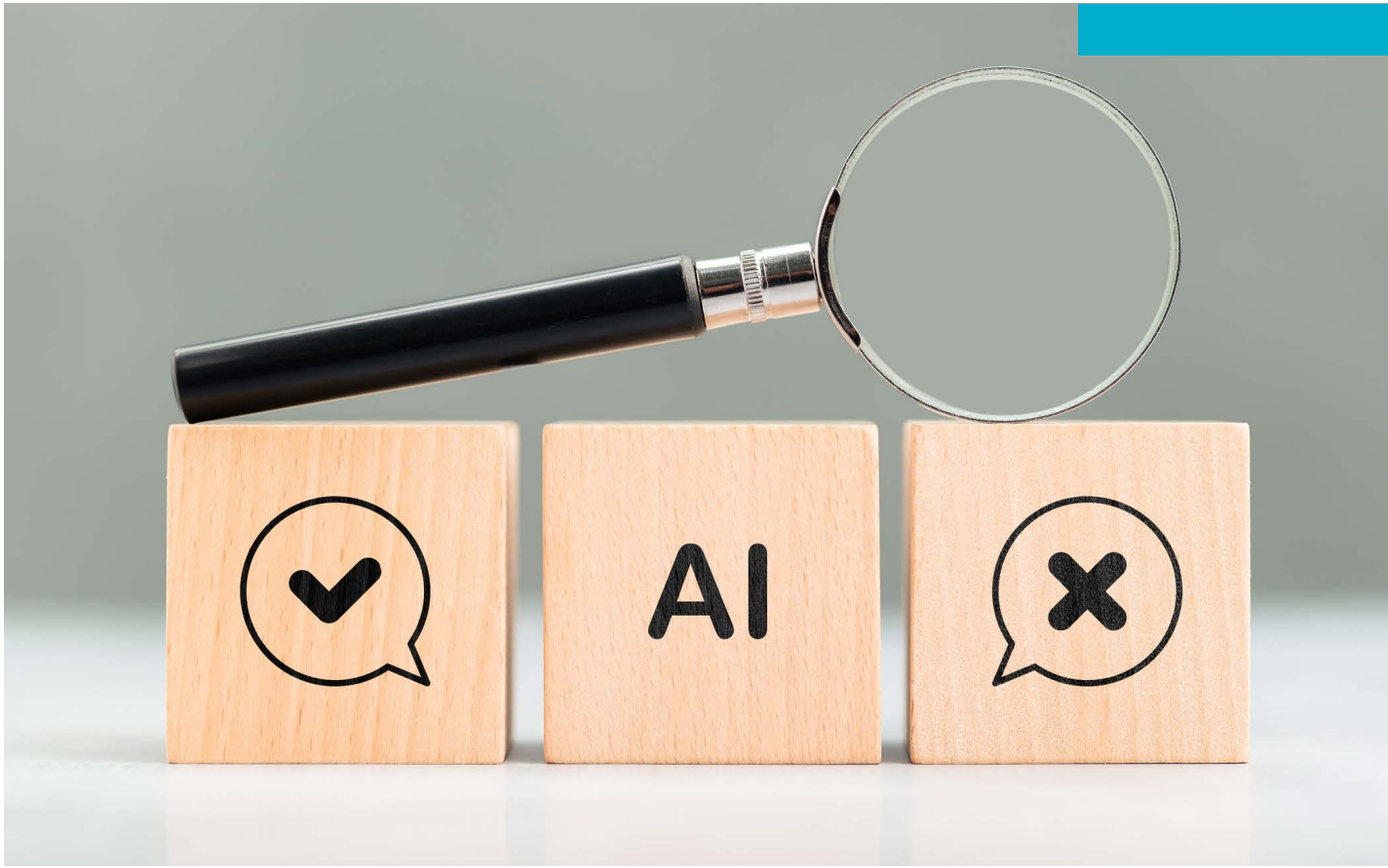
>>>

This outdated technology represents a significant threat to the organisation's security. "In short, investing in technology and cybersecurity is not a luxury, but a necessity. SMEs have no choice but to regularly invest in updates and new systems. Only by doing so can they avoid falling behind competitors who are actively modernising. The AI revolution of recent years illustrates this point better than anything else."

Digital Resilience

The cyber expert emphasises the need for a fundamental cultural shift within SMEs. "Many companies still view cybersecurity as a technical issue confined to the IT department. But cybersecurity must be embraced throughout the organisation, from management to operational staff. Governance and management decisions should guide technological implementation, not the other way around. Only in this way can a company effectively defend itself against the ever-growing threats of the digital world."

"The future of SMEs depends more than ever on their digital resilience. It is essential that they not only maintain their technology but also foster a culture of preparedness and a continuous drive for improvement.



Cybersecurity should not be seen as an additional cost but as an undeniable long-term investment."

Professional guidance, Hugues Mertens' core business at About IT, is therefore more relevant than ever. Frameworks and guidelines set by organisations like the CCB provide a critical starting point, but to translate these measures into practical, operational actions on the ground, expert support is indispensable. "We feel this every day in the enthusiastic responses from our clients," Mertens concludes.

“AI will become a core competency for students in every field”

As AI becomes an integral part of our daily lives, the need to understand and critically assess AI technology is more pressing than ever. For Bruno Dumas, professor at the University of Namur and researcher in Artificial Intelligence, fostering AI literacy among students is key to prepare them for the future of work.

According to Dumas, AI literacy is more than just understanding how AI systems work. It’s also recognising their potential and limitations. As he explains, “It’s about equipping students with the tools to understand AI systems, how they work, and how they impact various sectors. This is crucial because AI is already integrated into classrooms, industries and daily tasks.”

A university-wide course

To address this, he and his colleagues at the University of Namur developed a course that introduces AI to third-year students from all faculties, ensuring that everyone — from humanities majors to scientists — has the opportunity to learn about AI and its applications. “We wanted to show students that AI is a field that can be applied across various disciplines, from medicine to biology, from law to social sciences,” he explains. “The course covers the basics of AI, its strengths, weaknesses and potential. But most importantly, it emphasises critical thinking about how it works.”

“The Namur Digital Institute (NADI) has been working on AI for many years, but at the same time, we’ve always approached it in as interdisciplinary a way as possible. That approach is clearly reflected in how the course is structured. Moreover, the relatively small scale of our university works to our advantage, as it allows us to implement changes across all curricula,” he continues.

The course has been well-received: hundreds of students enrolled in the first year, demonstrating the growing interest in AI

>>>

literacy. “We’re now reaping the rewards of the groundwork we laid,” says Dumas. He stresses that AI literacy is essential for understanding not only the capabilities of AI but also its limitations. “AI systems such as large language models (LLMs) generate responses based on probability, not logic. It’s crucial for students to understand this in order to recognise the potential risks of AI, such as its tendency to ‘hallucinate’. While many students are aware of this, gaining a deeper understanding of how these mechanisms work is something they find extremely valuable. The same applies to ethical considerations such as privacy or bias.”

The growing AI divide

On a societal level, Dumas is most concerned about the growing divide between those who are familiar with AI and those who are not. “Today, we are widening a gap that could create an unequal playing field in society, where only the ‘initiated’ benefit from AI’s capabilities. But even more importantly, this could create a divide between those who understand the ethical and societal implications and those who don’t,” he warns.

It was his interactions with the business world in particular that made him realise this divide is already part of daily life. “AI is often introduced into large companies without considering how it will be used,” Dumas says. “We see cases where companies buy AI systems, but employees are left wondering how to implement them effectively.”

Therefore, when looking ahead, Dumas sees AI education evolving in both scope and depth. “In the next five to ten years, I picture AI becoming a core competency for students in every field of study. AI literacy will be as fundamental as knowing how to use a computer,” he predicts. In such a future, he believes that AI literacy cannot be achieved by academia alone.

Collaboration between universities, public sector institutions and private companies will be essential to ensure that everyone has access to AI education.

Collaborative initiatives that bring together diverse stakeholders to share knowledge and resources thus offer the key. “We need to create opportunities for knowledge sharing, so that all sectors can work together to build a future where AI is understood and used responsibly,” Dumas concludes.

Diversity and cybersecurity: stronger together

Digital transformation and cybersecurity dominate the agenda in most organisations, yet inclusion often lags far behind. For Tamara Eelsing, Diversity Manager at Brussels' public transport operator STIB-MIVB, the three are inseparable. "For many, diversity is still a blind spot. But it is a strategic necessity, especially in sectors where the talent shortage is biting hard."

With around 10,000 staff, STIB-MIVB is one of the capital's largest employers. Roles span everything from drivers and engineers to back-office staff and IT specialists. And Tamara's responsibilities are just as wide-ranging: shaping strategy, supporting managers, running awareness campaigns, and acting as a bridge between staff, unions and leadership.

Gender imbalance and the cybersecurity parallel

Despite years of effort, the employment gender gap at STIB-MIVB remains all-too evident. "On average, only 12% of our staff are women, and for technical roles that drops to barely 2%. Persistent stereotypes are part of the reason, along with practical barriers such as working in shifts, which is hard to balance with family life," Tamara explains.

It is a challenge that feels familiar in cybersecurity and other STEM fields. "The parallels are obvious. These sectors are still overwhelmingly male, and we have to work doubly hard to attract women, and, more importantly, to keep them." One striking initiative is the Our jobs have no gender campaign, with photos of employees posing alongside their daughters and other female relatives, to show that technical careers are open to everyone.

>>>

Promise and pitfalls

The technology angle becomes even sharper when artificial intelligence (AI) enters the picture. AI can support HR tasks such as screening CVs, but the risks are significant. “AI learns from data, and data nearly always contains bias. If most cybersecurity experts are men, an algorithm could conclude that men are automatically more successful. That further entrenches stereotypes.”

But AI can also uncover hidden talent. US researcher Vivienne Ming, for instance, used algorithms to identify the most active contributors to open-source projects, regardless of their qualifications. That brought to light expertise which would otherwise have gone unnoticed. For Tamara, the lesson is clear: “We should use AI smartly, but never trust it blindly. Human checks are essential if we want to tackle systemic bias.”

The cyber challenge for public transport

STIB-MIVB is facing major technological shifts, including automating its metro trains, electrifying its bus fleet, and rolling out digital tools for its passengers. As a result, the network is more reliant than ever on digital systems. “Cybersecurity is absolutely critical. Our systems must be reliable and above all safe, for the hundreds of thousands of passengers we carry each day.”

Human checks are essential if we want to tackle systemic bias of AI.

In practice, this means operating in tightly controlled environments and restricting the use of generative AI tools, especially where sensitive data is concerned. But the company is also looking forward: AI could help analyse CCTV footage or plan maintenance more effectively, for example. “Imagine being able to spot risky behaviour on a platform before something serious happens. If AI can pick up those warning signs, we can intervene faster and prevent accidents. That kind of innovation can make a huge difference, for both passengers and staff.”

Diversity Charter Belgium: a starting point for business

Tamara also sits on the advisory board of Diversity Charter Belgium, launched in June 2023. The charter is designed for organisations taking their first steps into diversity. “For companies without a dedicated diversity manager, it offers an accessible entry point: they can learn from each other, share best practices, and find the support they need to get started.”

For members of the Cyber Security Coalition, the charter has particular value. “It proves that inclusion isn’t a side issue. It is a way to accelerate innovation and tackle the shortage of digital skills head-on,” says Tamara.

Diversity, AI and cybersecurity are increasingly intertwined. For Tamara, the bottom line is simple: “We need to stay alert, challenge our processes, and seize every opportunity. That’s the only way to be truly cyber-ready, AI-smart and inclusive.”

Theme 6

Belgium's Cyber Security Awards

Cyber Security Personality of the Year

The fifth edition of the Cyber Security Awards honoured the most inspiring and influential professionals in Belgium's cybersecurity landscape. Ann Mennens, CyberAware Programme Manager at the European Commission, was awarded the 2025 Cyber Security Personality of the Year Award. In her current role she is raising awareness about cyber security, training people, communicating about it at the European Commission. As a leading voice, she has driven numerous projects at both national and European levels, consistently advocating for the inclusion and empowerment of women in cyber. Her unwavering commitment, outstanding leadership and her ability to inspire change make her a true role model for a safer, more inclusive digital future.

VIDEO

CISO of the Year

Philippe Cornette, Group CISO & Chief Enterprise Compliance Officer IT at John Cockerill, was awarded the 2025 CISO of the Year Award. The jury praised his exceptional achievement in elevating cybersecurity standards worldwide. Operating in a complex, multidisciplinary and multinational environment, Philippe established a global security baseline for John Cockerill within just five years. His direct engagement with teams and close collaboration with the Board exemplify the impactful leadership that sets him apart.

Philippe Cornette: I was genuinely surprised to have been named CISO of Year. I didn't expect it at all, as there were so many great candidates, whom I know personally. The cybersecurity community in Belgium is small, so we often cross paths. It's an honour, and it has already opened new opportunities to speak at events and share my experience.

Can you tell us a bit about your career path?
I've been in IT for more than 35 years. I started at AT&T, then worked for Swift and ING, mainly in IT infrastructure, security and fraud prevention. Back then, we didn't talk about cybersecurity. It was security, backups and disaster recovery. In 2019, after several years as an independent consultant, I joined John Cockerill to help define its cybersecurity strategy. I proposed a strategy, and was asked to stay to implement it. Five years later, I'm still here as Group CISO.

What makes John Cockerill's cybersecurity landscape so challenging?
It's a remarkably diverse company. We operate in defence, energy, hydrogen, services and heavy industry, across more than 30 countries.

>>>

Each business has its own risks and regulatory obligations: CMMC for the defence sector, NIS2 for manufacturing, and GDPR and other frameworks across multiple industries. For its size, John Cockerill is extremely complex, and that's what makes the job so fascinating.

How do you deal with the growing number of cybersecurity regulations?
I call it a tsunami of legislation. On the positive side, regulation helps less mature sectors catch up. But it's hard to keep pace. I maintain a world map with more than 300 cyber-related laws, and it keeps expanding. Europe and the US are dense, but Asia, Africa and Latin America are catching up fast.

What types of cyber threats concern you most today?
For an engineering company like ours, protecting intellectual property is as critical as defending against cybercriminals. It's not only about ransomware or data theft, we also face risks of industrial espionage from competitors and even friendly nations. Safeguarding our know-how is a strategic priority.

How do you see the role of AI in cybersecurity?
Artificial intelligence is both an opportunity and a risk. In our Security Operations Centre, AI helps us analyse billions of events that humans could never process manually. But we must use it wisely. If AI starts learning from AI, we could lose human expertise. We need to ensure knowledge transfer so the next generation can still grow into experts.

What about the human factor?
This remains an important issue. Despite training and monthly phishing simulations, people still click where they shouldn't. Awareness is a constant effort. The challenge is to make initiatives engaging and relevant, not just another mandatory e-learning exercise.

What keeps you motivated after such an extensive career?
I love what I do, and I don't plan to stop anytime soon. I still test new tools and local AI models at home: that keeps me sharp. This award is not only for me, but for the whole team at John Cockerill. Cybersecurity is, above all, a collective effort.

Young Cyber Security Personality of the Year

Digital transformation and cyber resilience dominate the agendas of many organisations, yet the field of cryptography often receives far less attention than it deserves. For Sarah Ampe, EY Belgium Digital Risk Manager and recently named Young Cyber Security Personality of the Year, this is precisely the domain that is becoming increasingly critical, as the pace of change forces organisations to think differently and, above all, think ahead.

Sarah's interest in cybersecurity began while she was pursuing her mathematics degree, during which her Bachelor's thesis introduced her to the world of cryptography. This proved to be a turning point. Although she went on to specialise in the discipline, she felt she lacked a clear view of how cryptography was applied in real-world environments. That question ultimately led her to EY, where she discovered a setting in which technical expertise, governance and organisational complexity come together. "Strong cryptography only works when the systems around it evolve as well," she explains. "Technology on its own is never enough."

Her decision to step fully into the field, however, was shaped by an unexpected encounter. While exploring her first professional opportunities, Sarah attended an EY event where women working in cybersecurity spoke openly about their experiences. "I had been to many recruitment fairs, but I tended to meet almost exclusively men," she recalls. "That never bothered me, but hearing the sector described through women's perspectives was refreshing. It gave me a different sense of what a career in cybersecurity could look like."

The incident offered her practical insights as well as reassurance: this was a domain in which diverse profiles could thrive. "It convinced me, because I suddenly saw a sector in which I could grow."

>>>

Evolving at unprecedented speed

At EY, Sarah quickly saw how rapidly cryptographic standards are shifting and how demanding this is for organisations. One of the most significant impending changes is the reduction of certificate lifetimes, which will decrease from one year to just 47 days. A process that once required annual attention will soon need to be managed every few weeks. "Automation becomes essential in such cases," she notes. "The real challenge is thus not the technology itself, but understanding your environment: knowing where cryptography sits within your systems, how components connect, and what happens when standards change."

The emergence of post-quantum cryptography is adding another layer of urgency. Many organisations still view it as a distant concern, but Sarah believes this is a misplaced assumption. "New cryptographic algorithms already exist. They have been tested, standardised, and are ready for broader adoption. Waiting until quantum computers pose an immediate threat is not a strategy. Preparing now will prevent a frantic and disruptive transition later."

Social awareness

Although cryptography is her technical foundation, Sarah views cyber resilience far more broadly. She is committed to making digital skills accessible to wider communities, including giving workshops to children and volunteers at a Digipunt in Roeselare, supporting individuals who struggle with everyday digital tools.

Her encounters there leave a lasting impression. People overwhelmed by digital parking systems, eID software or essential online services often feel powerless. "Digitalisation should never exclude people," she says. "Those who struggle with digital platforms face not only frustration but also increased vulnerability to fraud. When talking about cyber resilience, this group must be part of the conversation."

A new priority

Sarah observes that many Flemish companies encounter the same obstacle: they lack a clear view of the cryptographic systems they are using and the potential impact of upcoming changes. Without that insight, it becomes difficult to set priorities or build a realistic roadmap. Automation remains a stumbling block, even though it will soon be unavoidable. Preparing for quantum-resistant cryptography, she adds, should become a standard element of long-term planning. Not as a response to fear, but as a sign of maturity.

She considers the role of the Cyber Security Coalition particularly valuable in this context. For Sarah, its strength lies in creating a trusted space for sharing experiences and learning from one another. The guidelines and frameworks developed within the Coalition offer practical support that organisations can apply immediately. "Many companies face similar challenges," she explains. "The Coalition enables them to address them collectively and to build maturity more quickly."

New talent and broader perspective

For young professionals, especially women, Sarah has a clear message. She sees how often strong talent underestimates itself and allows opportunities to pass by. "You don't need to have a perfect answer to everything before you begin," she says. "Don't let yourself become your own barrier."

With her award, she hopes to keep two themes firmly on the agenda: the need for a strategic, forward-looking approach to cryptography, and the importance of embedding digital inclusion in every conversation about cyber resilience. "We move forward only when everyone can participate, organisations and citizens alike. That is the foundation of genuine digital security."

Cyber Security Researcher of the Year

2025 Cyber Security Researcher of the Year Prof. Dr. Peggy Valcke, full professor of Law at KU Leuven's Centre for IT & IP Law (CiTiP), views the award as recognition of the importance and added value that lawyers bring to technological research projects. "More than ever, I am convinced that collaborating with technical profiles is incredibly enriching for lawyers, and vice versa," she says.

Peggy Valcke's primary motivation in applying for the award was to highlight the work of her research group, she explains. "It's not always easy for legal researchers to hold their ground in projects focused on technology development. They often have to fight for a place at the table, both during the funding application process and throughout the research phase, to convince others of their value."

"Yet interdisciplinarity is more crucial than ever in such projects," she continues. "AI, for instance, is by its nature an interdisciplinary field. The same goes for cybersecurity, which involves much more than just technical security. Lawyers clearly have a vital role to play. While this may lead to longer development processes, it ultimately results in better outcomes. As the African proverb says: 'If you want to go fast, go alone. If you want to go far, go together'."

This approach has long been the norm at CiTiP. "Very few of our projects focus solely on legal issues, which has proven to be a fruitful course. One clear example is the Data Protection Modelling Framework (DPMF), developed with our colleagues at DistriNet. It enables software engineers to accurately represent the who, what, why and how of data processing operations in accordance with the GDPR, and was recognised as a best practice in the new ISO/IEC standard 27564 on the use of models for privacy engineering. We're quite proud of that," she says.

>>>

A sense of disdain

Within Belgium, she sees that the added value lawyers bring is generally well-recognised, which she attributes in part to the Cyber Security Coalition. "They consistently emphasise the importance of interdisciplinarity and have fostered a culture around it within our ecosystem. In other European countries, this recognition is less common. In EU projects, for example, we sometimes have to work harder to convince technical project partners of our value, and in some cases there's even a sense of disdain towards the work of lawyers."

It's a regrettable attitude that goes against the broader societal trend that is emerging.

"In recent years, the democratic legislator has made it clear that technological developments can only move forward if they take certain values and principles into account, from the early design phase. To ensure this, a level playing field with binding measures—including security, data protection and ethics-by-design obligations—has been developed."

"That's why I am more convinced than ever that the collaboration between technical profiles and lawyers is incredibly enriching for both. Seeing so many of our legal researchers being eagerly recruited today reassures me I'm not alone in this belief. Moreover, in my role as BIPT Board member, which I have held since early 2024, I experience every day the importance of open collaboration across disciplines and profiles. This award serves as further confirmation of my conviction," she concludes.

Privacy Professional of the Year

This year's Privacy Professional of the Year is Nathan Vanhelleputte, Head of Digital Compliance Office at Bnode (formerly Bpostgroup). He received the award for his strategic integration of data protection policies, which demonstrated that compliance and privacy are not obstacles but enablers that contribute to innovation and growth.

What led you to your current role at Bnode?
Nathan Vanhelleputte: I have a legal background and over the years specialised in privacy law and the complex legislation regarding data protection. In 2021, I had the opportunity to become the Data Protection Officer at Bnode, which at the time was in the midst of a digital transformation. I saw this as an opportunity to leverage my experience and help a large organisation prepare for the future.

Why are you passionate about privacy? What keeps it interesting for you?
What drives me most is the profound impact that technology can have on people's daily lives. For me, privacy is not a standalone domain. I try to keep in mind the broader picture: how technology influences our society and how can it be used to improve our lives and our economy. Data protection plays an important role in this, but it's not a goal in itself. It needs to contribute to this broader vision, in particular how we can use technology responsibly to ensure we maximise its benefits while not losing sight of the potential risks.

Is personal data protection under more pressure currently?
Yes, absolutely. The pace at which technology evolves brings new opportunities but also new threats, and currently we are also seeing the geopolitical situation becoming increasingly complex. We must constantly ask ourselves how we can better defend our organisations against these threats, both on a technical and a strategic level. For example, how can we at Bnode strengthen our digital infrastructure while also complying with regulations and meeting evolving customer expectations?

>>>

How does Bnode protect its customers' personal data?
I can't reveal a lot about that, but I can say that we do everything possible on a daily basis to protect our customers' data. It's a process that never stops and requires striking the right balance between being compliant and providing quality service. This means we constantly assess risks and set priorities. We implement the rules in a way that not only protects us and our customers, but that also enables us to continue to grow.

How do you ensure that privacy and data protection remain a top priority in the organisation?
We actively engage with management on an ongoing basis, to ensure that compliance is seen not just as a requirement but as an integral part of our business strategy. By ensuring that everyone, from top management to the operational teams, understands why we do what we do, we can create a culture where being compliant is second nature.

What does the Privacy Professional of the Year award mean to you?
This recognition is a confirmation that we are on the right track at Bnode. The hard work of my team is being recognised, and that motivates us to do even better and come up with solutions that go beyond what is expected of us. Stagnation is never an option. There is always room for improvement.

Finally, where do you see the biggest challenges in data protection and privacy today?
Regulations are becoming increasingly complex and we must ensure these rules remain feasible for businesses. Look at the GDPR: compliance is compulsory but for many companies, even after seven years, it's still unclear what the rules actually mean and what is expected of them. There is a need for a simpler and more practical framework that also leaves room for innovation. This will enable us to respond more quickly to the changing technological and geopolitical landscape.

Theme 7

Community life

Aftermovies

10th Anniversary Celebration

GRC: Be Connected! Fifth edition

Solstice Event@Mastercard

BE-CYBER Event - Coffee edition

Cyber Security Awards Fifth edition

Photo galleries

10th Anniversary Celebration

International Women's Day 2025

GRC: Be Connected! Fifth edition

Application Security

Solstice Event@Mastercard

Meet & Greet event

BE-CYBER Event - Coffee edition

25 Years of Cyber Justice

Cyber Security Awards Fifth edition

Publications

10th Anniversary Celebration

IT Value Creation in the (Central) Government

Cyber Security Survey Belgium 2025

White Paper – Preparing for the Quantum Era

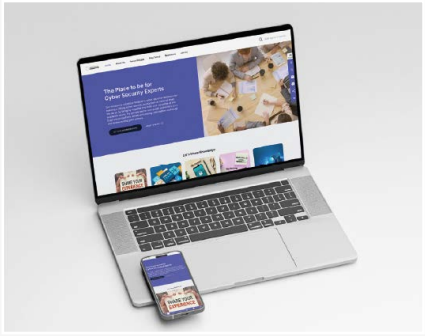
About the Coalition

About the Coalition

The Cyber Security Coalition is a non-profit association (ASBL/ VZW) that provides a neutral, non-commercial forum where cyber security professionals can freely exchange in confidence. The Coalition is a member-funded initiative.

The membership fees cover the operating costs and deliverables, such as awareness campaigns, information kits or the publication of guidelines. All member organisations are represented in the General Assembly.

Stay informed



visit our website
www.cybersecuritycoalition.be

subscribe to our newsletter
CyberPulse

follow us
LinkedIn: **Belgian Cyber Security Coalition**
Spotify of ApplePodcast: **cybertalk-nl / cybertalk-fr**

Colophon

The Cyber Security Gazette is a creation of the content company, commissioned by the Cyber Security Coalition.

Editors: Björn Crul, Roeland Van Den Driessche, Bavo Boutsen, Frank Simkens, Jo De Brabandere and Anse Keisse

Editor-in-Chief: Cathy Suykens

Photography: iStock, archives

Design: Bruno Jacques

Cyber Security Coalition
Stuiversstraat 8
1000 Brussels
info@cybersecuritycoalition.be
www.cybersecuritycoalition.be
Release Date : January 2026

Our board


Georges Ataya, Vice Chair


Fabrice Clément


Phédra Clouner, Vice-Chair


Jan De Blauwe, Chairman


Karine Goris


Xavier Paulus


Bart Preneel


Nathalie Ragheno


Catherine Van de Heyning


Saskia Van Uffelen


Stéphane Vince


Séverine Waterbley

Our operations team

From left to right:
Pascal Champagne, Henk Dujardin, Cathy Suykens, Christian Mathijs, Guy Hofmans.

Our members

PRIVATE

Accenture - BNP Paribas Fortis - Cronos Security - ING Belgium - KBC Group - Mastercard - Proximus - SWIFT

2dehands/2ememain - AboutIT - AG Insurance - Ahold Delhaize Global Tech BV - Allen Overy Shearman Sterling (Belgium) LLP - Approach Cyber - Ataya & Partners - AXA Belgium - Banque Nationale de Belgique - BDO - Belfius Bank - Belgian Mobile ID - itsme - Byblos Bank Europe SA - Capyx - Cegeka Groep NV Certi-Trust - CETIC - Colruyt Group Services - Computacenter NV - Corilus NV - Cranium Belgium NV - Crelan - Cresco - Crimson7 - Cyber Security - Management - Defend-OT - Delaware - Devoteam - DigiTribe - DNS Belgium - Doccle BV - EASI SA - Ebo-enterprises - Elimity - ESET Belux - E-Solutions - Ethias - Euranova - EURid - Euroclear - Exclusive Networks BeLux BV - Expertware Belgium srl - EY Advisory Services BV - Fox&Fish Cyberdefense - Guardiant Cyber - INNOCOM - Intigriti - Isabel NV/SA - Jarviss - Klarrio - KPMG Advisory cvba - L&S Registered Auditors - Liedekerke Wolters Waelbroeck Kirkpatrick - Link2Trust - Maiky (Security Service Layer bvba) - Marsh - Microsoft NV - Miris - Multitel - Netskope - Nexova Cyber SA - Nextensa - NOBI - NPS Consult - NRB - NVISO Belgium SRL - Orange Belgium - Orange Cyberdefense Belgium nv - Palo Alto Networks Belgium B.V. - PeopleWare n.v. - Persistent Security Industries - Pluxee - Psybersafe - PwC Enterprise Advisory BV - SAI vzw - Secudea - Secure Code Warrior - Secutec bv - Sirius Legal - Sirris - Solvay - Sopra Steria - Takto - Telenet BV - Thales Group Belgium - The Bayard Partnership - The Key 2 IT - Toreon BV - Trend Micro Belgium - Trustbuilder - UCB - Uniwan - Vanbreda Risks & Benefits NV - VDK Bank - Wavestone Belgium NV/SA - Yoursciencebe - Zetes Belgium

PUBLIC

Agence du Numérique - ASTRID - Banque Carrefour d'Echange de Données (BCED) - Belgian Defense - Belnet - BelV - BIPT-IBPT - C.R.E.G. - Centre for Cyber Security Belgium - CPAS Bruxelles - Enabel - European Commission - FIA-FAI - Flanders Investment & Trade - FOD Justitie/ SPF Justice - FOD/ SPF BOSA - FOD/ SPF Economie - FOD/ SPF Foreign Affairs - FOD/ SPF Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu - FOD/SPF Financiën - Finances - FOD/ SPF Sécurité sociale - GBA- APD - IBZ/ SPF Intérieur - Idelux Développement (Association intercommunale pour le développement économique durable de la province de Luxembourg) - IMIO - Irisnet - Paradigm - Parlement Wallonie - Province de Hainaut - Province de Namur - RVA-ONEM - SCK-CEN (Belgian Nuclear Research Centre) - STIB-MIVB - VDAB - Vlaamse Landmaatschappij - Vlaamse Overheid - VRT - YPTO N.V. (NMBS-SNCB)

NON-PROFIT

Landsbond der Christelijke Mutualiteiten - Flux50 - International Post Corporation (IPC) - Isaca Belgium - Quantum Circle - Shield vzw

Our members

ACADEMIC

Antwerp Management School - EE-Campus (Eurometropolitan e-Campus) - Henallux - HOGent - HOWEST University of Applied Sciences - ICHEC Brussels Management School - KU Leuven - PXL Hogeschool - Solvay Brussels School of Economics & Management - SyntraPXL vzw - Technofutur TIC - Thomas More - UCL - UGent - ULB - Université de Namur - Vives University College - VUB - Vrije Universiteit Brussel

FEDERATION

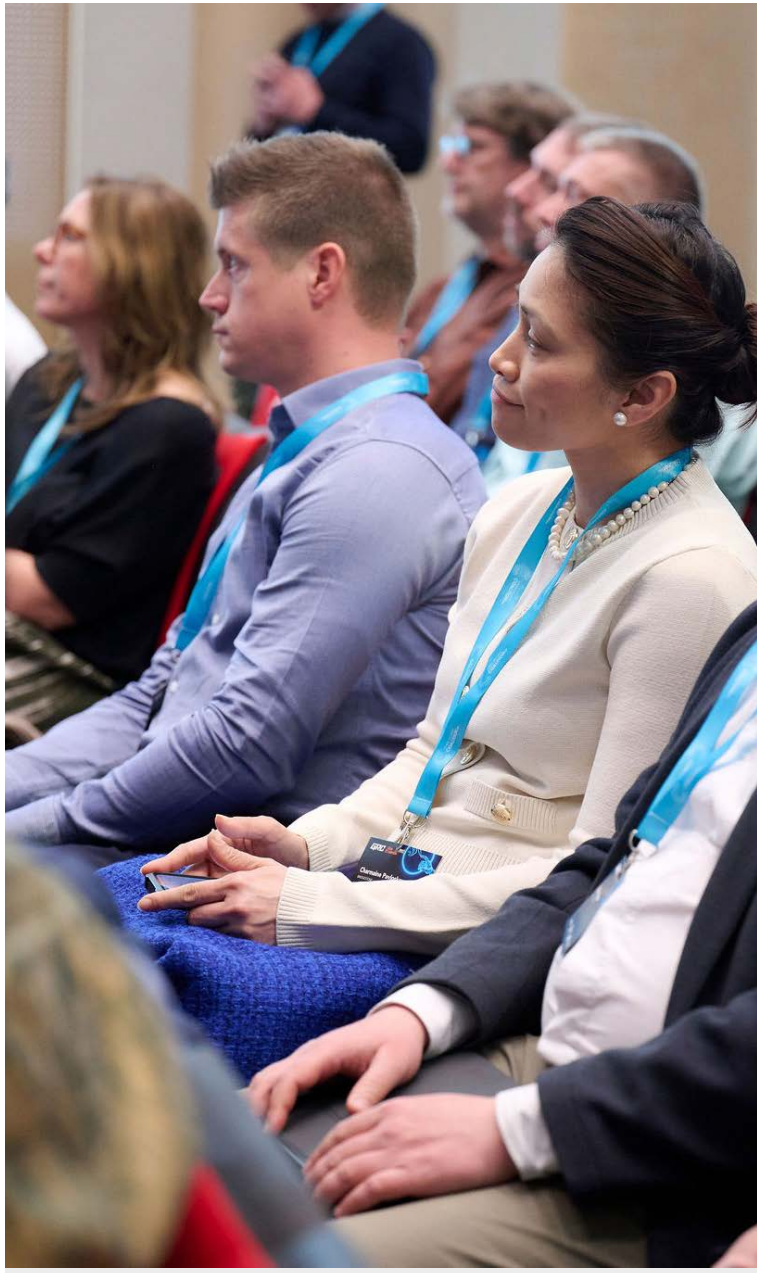
AGORIA asbl - Assuralia - Beltug - FABA - Febelfin vzw/asbl - FEDNOT - FEVIA VZW - HRZKMO / CSIPME - LSEC Leaders in Security - Santhea - Synergrid - VBO-FEB vzw/asblVives University College

HEALTHCARE

AZ Delta - AZ Groeninge - AZ Maria Middelares - AZ Oudenaarde vzw - AZ Rivierenland - AZ Sint-Jan - AZ Sint-Lucas Brugge - AZ Turnhout - AZ Vesalius - Azorg - Broeders van Liefde - Brugmann CHU/UVC - CHU Saint-Pierre - Clinique Saint Jean - Clinique Saint-Pierre Ottignies - Cliniques Universitaires Saint Luc - EpiCURA - GPN SON - Grand Hôpital de Charleroi - Hôpitaux Iris Sud - Iris Ziekenhuizen Zuid - HUB - Imelda Ziekenhuis - Jan Yperman Ziekenhuis - Jessa Ziekenhuis - Korian Belgium - Nexuzhealth - UZ Leuven - VITAZ - ZNA (Het Ziekenhuis Netwerk Antwerpen vzw) - ZOL

ASSOCIATE MEMBERS

Brasseur Pepijn - Clarence Pinto - Gunther Penne - Iva Tasheva - Jaroslav Remen - Jeroen Hoof - Leila Abajadi - Matthias Neuville - Meenakshi Sundaram - Nathalie Claes - Olivier De Visscher - Patrick Bochart - Paul Rollier - Ruben Tronçon - Sam Van Hauwaert - Shreeji Doshi - Veerle Peeters



Special thanks to our premium members