.AGORIA

Socio-economic study on the cybersecurity sector in Belgium – Second edition

October 2025

Table of contents

1. Foreword

Dear reader,

Since our last study in 2022, the **digital world** has evolved at an **unprecedented pace**. **Artificial intelligence** is now driving innovation across all sectors, creating new opportunities but also amplifying risks. **Cybercriminals** and **state-sponsored actors** are rapidly adopting AI to intensify their attacks, automate their deception techniques and bypass traditional defences. Combined with an **unstable geopolitical environment**, this makes **cyberspace a strategic domain** of our time.

No sector, no organisation, no citizen is immune. A phishing campaign can destroy a business. A manipulated dataset or algorithm can compromise production processes. And a targeted cyberattack can disrupt supply chains and critical infrastructure, with significant repercussions.

That is why **strengthening our digital resilience** is no longer a matter of choice, but a **necessity**. Belgium – and Europe as a whole – must foster a **competitive cybersecurity ecosystem** and ensure that we remain at the forefront. This requires **leading expertise**, not only in research, but also within our public institutions, private companies, hospitals and society.

Cybersecurity should not be seen as a cost, but as a **catalyst for trust, innovation and competitiveness**. In the face of threats, robust protective measures strengthen trust, attract investment and protect the digital lives of our businesses and institutions.

Based on the update of the first socio-economic study conducted in 2022 by Agoria, the Ministry of Defence and the Centre for Cybersecurity Belgium (CCB), the Cyber Business Group Cyber Made in Belgium (CMiB) of Agoria, in collaboration with Solvay Brussels School of Economics and Management (SBSEM) and Defence (Cyber Command), underscores the **dynamic growth of the Belgian cybersecurity sector**. Our conclusions highlight the sector's growing strategic importance, the challenges it faces and the opportunities available to Belgium to position itself as a **reliable and resilient digital economy in Europe**.

The Cyber Force is built on trusted partnerships and nationwide collaboration, engaging in academia, government, industry, and citizens alike. This collective effort with all cyber actors forms the backbone of our cyber resilience, enabling rapid innovation and robust capabilities. Through this unified approach, our nation stands among the most secure and least vulnerable in Europe.

Cybersecurity is the cornerstone of prosperity and sovereignty in this century. Focusing all our **attention and investment** on this sector is not only desirable, it is **imperative**.

Major-General Pierre Ciparisse
Belgian Defense Cyber Force Commander

Alex Driesen
Toreon Chief Executive Officer
CMiB Chairman

2. Executive summary

The cybersecurity market in Belgium is experiencing strong and steady growth. The rapid evolution of the threat landscape- driven by technological advances and geopolitical shifts- is fuelling demand for cybersecurity solutions.

Investing in cybersecurity means investing in resilience: every initiative, whether in the public or private sector, and whether from small businesses or large organizations, contributes to stronger online protection.

2.1 Cybersecurity in Belgium

This update of the socio-economic study on the cybersecurity sector in Belgium is an opportunity to monitor the evolution of this industry over the years.

Key figures evolution for the Belgian Cybersecurity sector

732
Cybersecurity **entities** in 2025
(+ 54% vs. 2021)

€ 2.61 billion
Total cybersecurity
sales figure in 2024
(+ 65% vs. 2021)

9.750 FTEs
Total cybersecurity
employment
(+ 52% vs. 2021)

15.9%
Expected compound
Annual Growth Rate
(2025-2030)

1.170
Cybersecurity **vacancies** in
the cybersecurity sector
(-3% vs. 2021)

22.1%
Cybersecurity
export percentage
(+ 35% vs. 2021)

2.2 Conclusions

These updated socio-economic numbers demonstrate the growth during the last 4 years. The **total cybersecurity sales figures has grown by nearly 65%**, from 1,58 billion in 2021 to 2,61 billion in 2024. New indicators point to continued growth in total cybersecurity sales, with the Agoria Study Centre calculating an optimistic annual increase of 15.9% from 2025 to 2030, based on Statista, Gartner, and IDC forecasts. A more likely outlook would be between 13% and 14%.

These growth numbers are reflected in the **increase of the number of entities and of the total cybersecurity employment** which grew from 6.405 in 2021 to 9.750 in 2025, while the number of cybersecurity vacancies **in the cybersecurity sector** remains relatively stable compared to 2021.

There were five recommendations around three themes in the socio-economic report in 2022 being the **development of talents and education curricula, Awareness** and a **growth roadmap for the cybersecurity sector**. Notably progresses have been observed thanks to fruitful collaboration between academia, federal, regional authorities, Defence and private sector. Still the five recommendations remains actual and will require additional efforts and investments in the coming years.

On a strategic level, cybersecurity is incredibly important for the **multi-layered resilience** at public, private organisations and all citizens levels.

With a double-digit growth foreseen in the 5 coming years, only more attention, focus and funding will allow Belgium to reach the capacity to protect its authorities, industries and citizens. These efforts will create thousands of jobs and reinforce Belgium nation status as the least vulnerable country in Europe as aimed by the Centre for Cybersecurity in Belgium in the "Cybersecurity Strategy Belgium 2.0 - 2021-2025" (CCB, 2021).

Miguel De Bruycker
Managing Director General,
Centre for Cybersecurity Belgium (CCB)

> *"Cybersecurity starts and ends with applying basic security measures."*

3. Cybersecurity landscape evolution

Before diving into the evolution of the cybersecurity socio-economic numbers of the cybersecurity sector in Belgium, let's look at the cybersecurity landscape evolution since 2022 globally, at the European level and in Belgium.

3.1 Cybersecurity in the world

Between 2022 and 2025, the World Economic Forum (WEF, 2024) shows a shift in cyber risks. Traditional threats like **ransomware** are now joined by **AI-driven dangers, supply chain issues, and rising geopolitical tensions**. Skills shortages and weaker resilience among small businesses is amplifying the problem.

Cybersecurity is a fast-growing sector, with spending expected to reach **$212 billion in 2025**, up from $188 billion in 2023 or +13%, (Gartner, 2024). Yet losses from cybercrime are much larger, projected at **$10.5 trillion annually**, up from $8 trillion in 2023 or +31%, (Cybersecurity Ventures, 2025).

AI is changing the game. The AI cybersecurity market, worth **$24 billion in 2023, $39,8 billion in 2025** and could exceed **$93,75 billion by 2030** (Altindex.com, 2025). While AI boosts defence, attackers use generative for phishing, malware, and deepfakes. Furthermore, the World Economic Forum observes that the **AI agents** in cybercrime has ramped up the threat level for business organizations (WEF, 2025). Combined with global talent shortages, this creates urgent need for stronger collaboration, fair access to resources, and resilient digital systems.

> *Cyber is not an isolated domain. We think cyberspace as a continuum from photon to disinformation. Protection of all Cyberspace layers is essential to guarantee the cyberresilience of our society.*

Major-General Pierre Ciparisse
Belgian Defense Cyber Force Commander

3.2 Cybersecurity in the European Union

Since 2022, the **EU has reshaped the cybersecurity legal landscape** with sweeping reforms. Network and Information Security 2 (NIS2) expanded sectoral obligations, Digital Operations Resilience Act (DORA) secured the financial system, and the Cyber Resilience Act (CRA) imposed rules for products with digital elements.

The Cyber Solidarity Act (CSA) created EU-wide response capacity, while the AI Act introduced risk-based governance for AI. Together, they raise resilience, accountability, and trust across Europe's digital ecosystems.

Major legal changes (since 2022):

- **NIS2 Directive (2023)** – Broader enforcement across 18 sectors, stricter incident reporting, management liability, supply chain accountability enforcement with heavy fines.
- **DORA (2022/2025)** – ICT risk management and operational resilience rules for financial entities, enforceable from January 2025.
- **Cyber Resilience Act (2024)** – Mandatory cybersecurity requirements for products with digital elements, including secured designs and updates.
- **Cyber Solidarity Act (2024/2025)** – EU-wide cyber crisis response, threat detection, and incident review capacity.
- **AI Act (2024)** – Risk-based framework for AI, banning harmful uses and imposing strict requirements on high-risk systems.

3.3 Cybersecurity in Belgium

3.3.1 Evolution of the cybercrime in Belgium

Belgium makes no exception; cybercrime is growing as in any other countries. Nevertheless, Belgium being located at a central point in Europe and hosting hosts the headquarters of the western military NATO as well as many European Union institutions, is one of the countries that cybercriminals are choosing to attack more than most. (VRT, 2024).

The number of attacks is raising sharply from about 100 per day in 2023 to **275 attacks per day** during the first quarter of 2025 or an increase of 165 % in less than three years (Check Point Software technology, 2025). This is confirmed by the number of reported incidents to the authorities. The Centre for Cybersecurity Belgium received on average of **45 incidents per month** mainly on critical systems since the introduction of the NIS2 legislation. 80% more compared to the period between August 2023 through September 2024 (CCB, 2025a).

> *As cross-border trust erodes, cybersecurity becomes a vital differentiator - for our industry, our exporters, and our country. Opportunity to shape Belgium's reputation as the place where trust is built in.*

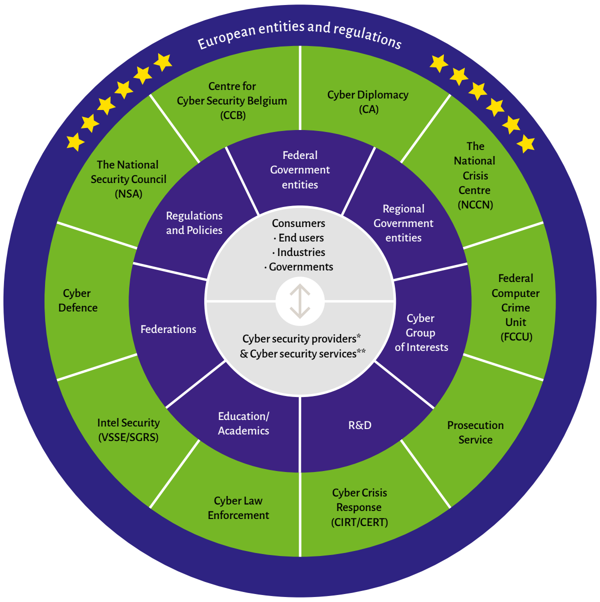
Alex Driesen
Chief Executive Officer, Toreon
Chairman, CMiB

No less than **one in four Belgian companies (25%) was the victim of a cyberattack in 2024** (Proximus, 2025). At the same time, nearly three-quarters (71.4%) of the Flemish companies state that their company is well protected against cyber-attacks. This indicates **an overly optimistic perception of cybersecurity maturity** given that a significant proportion of Flemish companies still lack a basis for management procedures and technical measures, (VLAIO, 2025).

3.3.2 Evolution of Belgian Cybersecurity ecosystem

Since 2022, Belgium's cybersecurity ecosystem has evolved into a well-coordinated, multi-layered network of public and private actors. For instance, the **Centre for Cybersecurity in Belgium (CCB)**, operating as **CERT.be** and the **National Cybersecurity Coordination Centre (NCC-BE)**, translated the **NIS2** EU Directive in national law and leads national implementation of NIS2, manages incident reporting, provides threat intelligence, and ensures alignment with EU cybersecurity initiatives.

The Belgian cyber ecosystem and its stakeholders


European entities and regulations
Centre for Cyber Security Belgium (CCB)
Cyber Diplomacy (CA)
The National Crisis Centre (NCCN)
Federal Computer Crime Unit (FCCU)
Prosecution Service
Cyber Crisis Response (CIRT/CERT)
Cyber Law Enforcement
Intel Security (VSSE/SGRS)
Cyber Defence
The National Security Council (NSA)
Federal Government entities
Regional Government entities
Cyber Group of Interests
R&D
Education/ Academics
Federations
Regulations and Policies
Consumers
· End users
· Industries
· Governments
Cyber security providers*
& Cyber security services**

In 2025, Belgium took a bold step by establishing the **Cyber Force,** expanding the Cyber Command initiative across the entire Defense organization and officially recognizing cyberspace as an operational domain.

Private sector major stakeholders—including the **Belgian Cyber Security Coalition, Agoria**, and the **Cyber Made in Belgium** (CMiB) members drive innovation for example in the field of ICS/OT, deploy services such as **Cyberstart** (Agoria, 2023), **Cyberboost** (Agoria, 2024) or **Cyber Risk Scan** (Agoria, 2025), and participate in collaborative EU projects such as CyberHub.

Many public–private initiatives are taking shape. For instance, **CMiB4Defence** strengthens collaboration between Belgian Defence and industry. Another example is the contribution of CMiB members to the 2025 Cyber Fundamentals® frameworks update on top of the next CCB national strategy.

Public awareness and resilience are reinforced through campaigns like Safeonweb.be, national exercises, and national events such as **BE-CYBER** organised by the Belgian Cyber Security Coalition and **Cybersec Europe** fairs.

> *A strong cyber industry in Belgium makes our society more resilient in this digital age.*

Wouter Vandenbussche
CyberSec Service Lead
Proximus NXT

In 2024, 99,7% of the companies in Belgium were SMEs (CSIPME, 2025). Considering this fact, Belgium has implemented numerous initiatives to enhance cybersecurity among SMEs, focusing on practical support, awareness, and guidance.

To name a few examples, one can highlight the Centre for Cybersecurity Belgium (CCB) awareness and guidance initiatives for SMEs through **Cyber Fundamentals**® Small and Basic. These frameworks were launched in 2023 along with Cyber Fundamentals® Important and Essential. New versions are expected in October 2025. Moreover, online resources like **Safeonweb.be**, helping also smaller organizations implement basic cybersecurity measures.

The federal initiative **Ma PME Cybersécurisée/ Mijn zaak cyberveilig** launched in 2023 aiming at helping SMEs to better secure their business against cyber-attacks. At regional level, **co-financing for cybersecurity advisory** services in Flanders (Cybersecurity verbetertrajecten) and in Wallonia (Chèques-entreprises cyber securité) are also contributing to develop further resilience in SMEs.

Together, these institutions and initiatives **form a robust ecosystem** balancing governance, operational readiness, and international coordination.

3.3.3 Cybersecurity education

In 2022, Agoria estimated that the number of open vacancies in the Cybersecurity sector was around 1.200 and approximately 4.000 in all Belgian sectors (Agoria, 2022). Nevertheless, the needed workforce estimated for the Belgian overall sectors its number is still set at **6.190 cybersecurity team shortages in 2025** (ICS2, 2024).

To meet that demand, **the cyber education has a crucial role to play**. The number of formal and non-formal curricula has increased during the last years in Belgium. Agoria has inventoried around 100 cybersecurity curricula during the summer 2025.

In the list of cybersecurity education programs established by the CCB (CCB, 2025b) there are **50 academic programs identified** (+13,6% since 2024) amongst which 25 are masters, 21 are bachelors, 4 are specializations in cybersecurity offered by formal institutions.

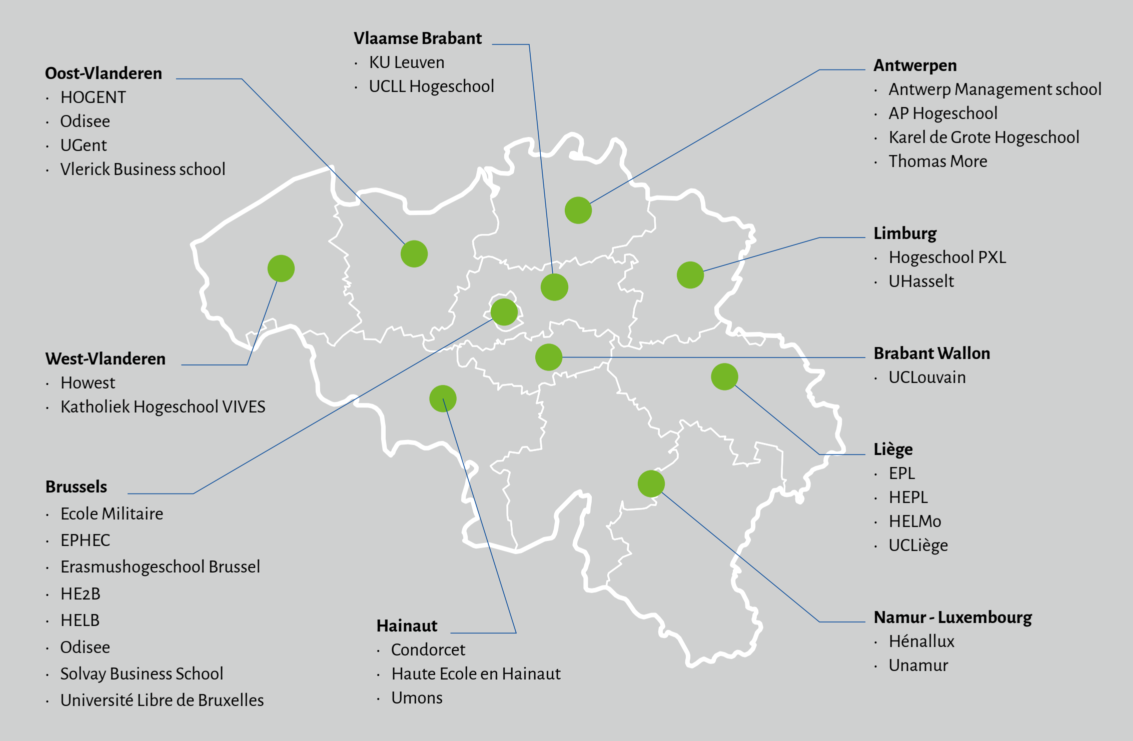


Illustration: Overview of the main academia offering cybersecurity curricula – in alphabetic order (CCB, 2025b).

> *Only when every member of the workforce is empowered through cybersecurity training, embraced by a strong cyber culture and supported by digital inclusion, can we build a truly resilient and cyber safe world.*

Saskia Van Uffelen
Manager Future workforce
Agoria

The learning programs remains evenly distributed across all regions with 20 programs in Flanders, 19 in Wallonia, 11 in the Brussels region and are available in several languages 19 programs are proposed in English, 17 in French and 14 in Dutch.

In the report of the cybersecurity skills needs for Belgium (CyberHub Belgium, 2024a), the analysis of the programs shows that the **learning programs cover the 12 roles** defined in ENISA's ECSF competency framework (ENISA, 2022).

On the cybersecurity vocational training courses side, although it is difficult to compare the evolution of the offering due to a lack of references, one can estimates that the offering has grown in recent years.

In the non-exhaustive inventory compiled by Agoria in the summer of 2025, Agoria identified **more than 40 vocational training courses** offered by formal and non-formal institutions. These courses can last from a few days to several months, be classroom-based or online, and even be part of a programme combining work and study.

In a study conducted by VLAIO (VLAIO, 2025), **42,8% of the companies surveyed assert that lack of employee awareness is the greatest cyber risk to their company**. Training or activities for employees can reduce this risk, but adoption is still lacking in more than half of companies). This percentage, which is almost identical to what was observed in 2022, shows the importance of continuous learning and education.

> *Intensive cybersecurity training is essential due to fast-evolving threats, gaps in new employees' skills, and risks from changing business processes.*

Georges Ataya
Academic Director,
Solvay Brussels School of Economics and Management

4. Cybersecurity sector evolution since 2021

4.1 State of the cybersecurity sector in Belgium

4.1.1 Quantitative results

Thanks to the results of the survey executed in 2025, based on an inventory realized between March and August 2025 of entities active in the cybersecurity sector, we can give an accurate overview of the Belgian cybersecurity landscape and compare with the results of the survey executed in 2021.

The Belgian cybersecurity landscape

441
Cybersecurity **entities** in 2021

732
Cybersecurity **entities** in 2025 (+ 54%)

€ 1,58 billion
Total sales figure in cybersecurity in 2021

€ 2,61 billion
Total sales figure in cybersecurity in 2024 (+ 65%)

€ 600 million
Total value added in cybersecurity in 2021

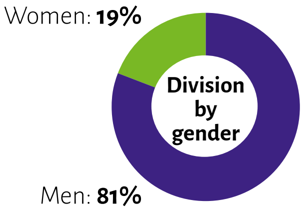
€ 915 million
Total value added in cybersecurity in 2024 (+ 52,5%)

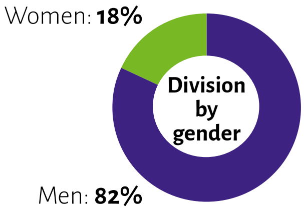
0.10 %
of the Belgian GDP in 2021

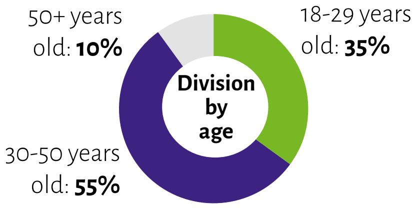
0.15 %
of the Belgian GDP in 2024 (+ 50%)

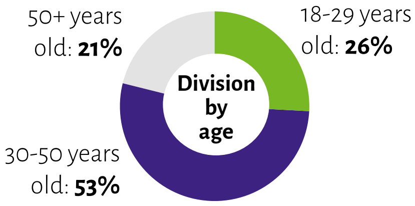
6.405 FTEs
Total employment in cybersecurity in 2021

9.750 FTEs
Total employment in cybersecurity in 2025 (+ 52%)

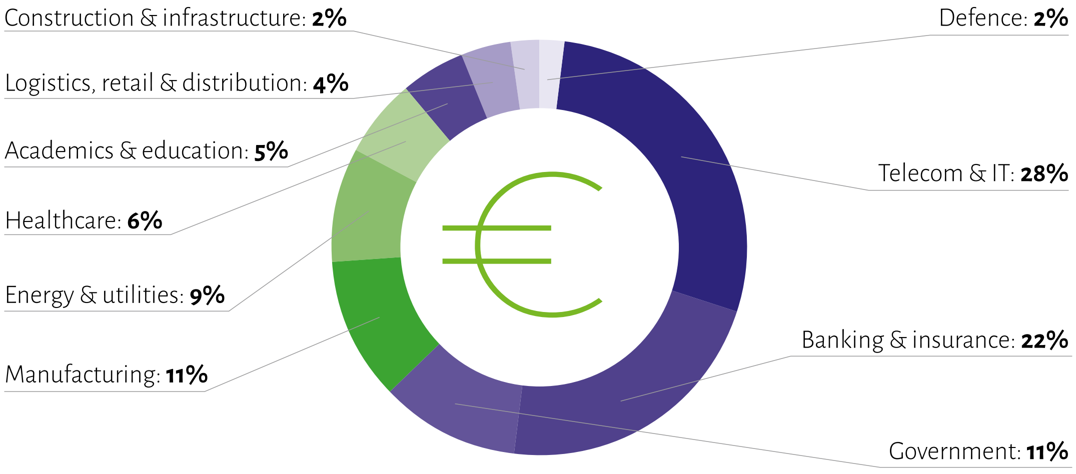








Most important sectors where cybersecurity sales figures are realised



1.205

Total number of vacancies in the cybersecurity sector in 2021

→

1.170

Total number of vacancies in the cybersecurity sector (-3%)

16%

Vacancy rate cybersecurity sector which is much higher than:
Vacancy rate **Belgian IT sector: 9,1 %**
Vacancy rate **Belgian economy: 5%**

→

12,4%

Vacancy rate cybersecurity sector which is much higher than:
Vacancy rate **Belgian IT sector: 5,3 %**
Vacancy rate **Belgian economy: 3,9%**

16,4%

Export percentage in 2021 (+ 35%)

→

22,1%

Export percentage in 2025 (+ 35%)

42%

Doesn't export at all in 2021

→

75%

Doesn't export at all in 2025

Regional distribution

Entities active in the cybersecurity sector by region:

Cybersecurity entities based in:	**Cybersecurity entities**	**Cybersecurity sales figures (2024)**	**Cybersecurity employees (in FTE)**
Brussels	173 (23,6%)	€ 0, 52 billion	2.800
Flanders	396 (54,1%)	€ 2, 01 billion	6.485
Wallonia	163 (22,3%)	€ 0, 08 billion	465
Belgium	**732**	**€ 2,61 billion**	**9.750**

Considerations based on the updated numbers

The Belgian cybersecurity sector is demonstrating strong and steady growth. Both total sales and added value figures confirm that the sector is expanding faster than the broader Belgian market. Cybersecurity, which once represented only 0.1% of Belgium's GDP, now accounts for 1.5% - a remarkable 50% growth.

> *True cyber resilience will come from continuous improvement, bridging IT and OT, and securing every layer of society.*

Bart Van den Branden
Head of Product Management Security
Cegeka

The telecom and IT industries, along with the banking, insurance, academic, and education sectors, are growing at an even quicker pace than the overall market. The cybersecurity market itself continues to expand rapidly and is expected to sustain this momentum over the next five years.

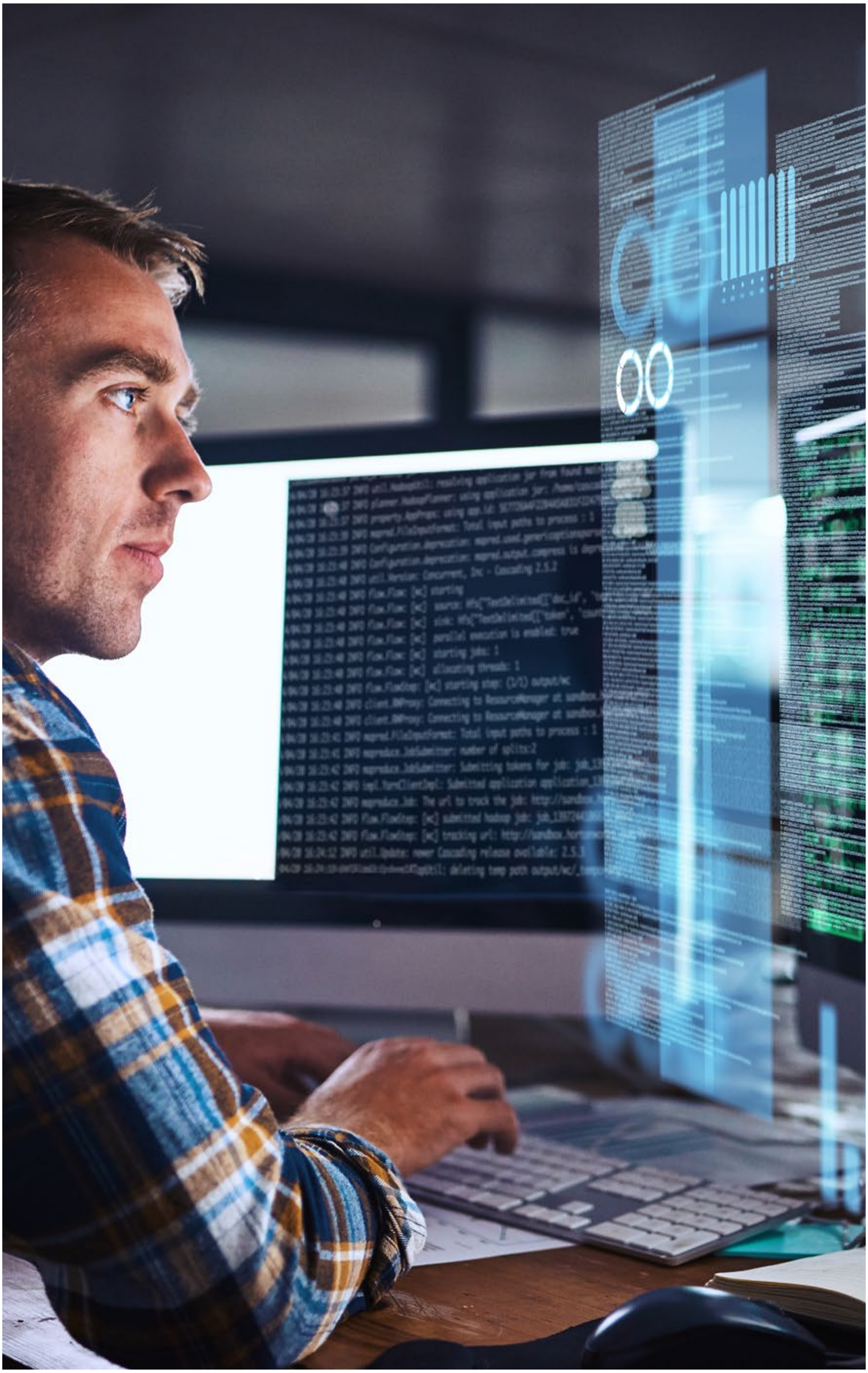
However, some structural challenges remain. The **share of women in the cybersecurity workforce has remained relatively stable**, highlighting the need for initiatives that improve both the attractiveness of the field and awareness of career opportunities. At the same time, **the sector is maturing:** the proportion of professionals aged 50+ has doubled from 10% in 2021 to 21% today, while the share of younger professionals (18–29 years old) has declined from 35% to 26%. The 30–50 age group remains stable.

Talent shortages also continue to put the market under pressure. Although the total number of vacancies has stabilized, the vacancy rate in cybersecurity (12.4%) remains well above both the IT sector (5.3%) and the national average (3.9%).

Finally, **exports are gaining importance**. The share of exports has risen from 16.4% in 2021 to a projected 22.1% in 2025, driven mainly by larger companies. While 42% of the entities weren't exporting at all in 2021, this percentage has increased to 75%. This may potentially be linked to raise of very small businesses.

> *The cybersecurity landscape demands more than just defences, it requires a proactive, intelligence driven approach that anticipates and mitigates risks before they materialize. Known the unknown to build a safer digital society.*

Hans Stevens
Head of Trusted Solutions
Orange Cyberdefense Belgium



4.1.2 Qualitative results

The qualitative results are extracted from the 6 open questions which were part of the survey. They can be **summarized** in the following areas:

Cyber poverty in SMEs

Multiple respondents reported that many SMEs face an alarming state of **cyber poverty**, as limited awareness of digital risks often leads them to underestimate the importance of cybersecurity.

> **The Cybersecurity Poverty Line**
>
> **The Cybersecurity Poverty Line** (CPL) is the point at which an organization lacks the minimum resources (money, staff, tools, or skills) needed to protect itself from common cyber threats.
>
> If an organization is below this line, it cannot afford or sustain even the basic level of cybersecurity practices; if it is above the line, it can at least cover the essentials.

The **cost of a cyber security incident can often amount to hundreds of thousands or even millions of euros** (CCB, 2021a), while proactive measures like an incident response plan or cyber insurance significantly reduce both financial impact and recovery time. It underlines that being prepared can make the difference between an incident a company survives and a crisis that threatens its continuity. Unfortunately, with investment priorities directed toward immediate business growth, **cybersecurity is frequently pushed aside**, leaving these companies vulnerable to increasing cyber threats.

Rapid evolution of the cyber landscape

The cyber threat landscape is evolving at an accelerating pace, with increasingly sophisticated attacks outpacing organizations' ability to adapt their defences. This rapid evolution of the technology landscape increases complexity and uncertainty, making proactive and adaptive risk management essential.

While this rapid evolution is perceived as a threat, it is also a source of opportunities for companies active in delivery cyber solutions to their clients. For example, **AI poses a significant challenge in cybersecurity**, enabling attackers to automate, scale, and refine their methods at unprecedented speed. At the same time, it offers MSSPs a powerful opportunity to deliver smarter, faster, and more cost-effective protection for their clients.

Kurt Ceuppens
Chief Executive Officer
NVISO

> *“The cybersecurity industry is expanding at a pace that significantly outstrips the economic growth of Belgium. With strong contributions from industry, academia, and government, Belgium is uniquely positioned to make cybersecurity a cornerstone of our economy and our future. So let's seize this opportunity.”*

Some respondents mentioned that the **growing convergence of IT and OT** has heightened the importance of protecting operational technologies, as cyberattacks on these systems can **directly disrupt critical** infrastructures and industrial processes. To illustrate this evolution, "killware" or lethal cyberattacks in the health sector require organizations to treat OT, IoT, and IT as one challenge.

Likewise, some respondents reported that the new geopolitical situation and the EU regulations (NIS 2 DORA, CRA, ...) are also **creating opportunities** on the cyber market. The same observation was reported in relation to defence-related opportunities.

Persistent lack of awareness

Respondents report that SMEs managers and their employees often lack awareness of cyber threats because of limited budgets, fewer dedicated IT staff, and **the misconception** that attackers primarily target larger organizations.

For organisations subject to NIS2, management awareness is improving due to legal requirements, but business priorities still overshadow the urgency of investments and actions.

Cyber education as a solution for skills gap

Not surprisingly, all respondents reported that they are having difficulty recruiting new talents.

One of the often-mentioned ways for closing the skills gap is more advanced coordination between companies and academia, both formal and non-formal. It is important to underline that the course offering is not in adequation with the markets needs. It has to cover a wider range of cybersecurity specialities. It should be not limited to producing pen testers or SOC analysts.

Several respondents mentioned the **importance of diversity at large** (women, upskilling, etc.) as well as the **need to introduce cybersecurity concepts very early** in the school curriculum, including for children.

Cooperation Public/Private

While the CCB has consolidated its position of leading governmental organisations in Belgium, respondents to the survey mention that SMEs should be even **more financially supported by the authorities** through the NCC-BE program.

Some respondents emphasize **the importance of collaboration** between the private and public sectors, particularly through increased information for companies about the importance of cybersecurity and priority given to **national and sovereign** solutions during purchasing processes.

4.2 Outlook for 2026 to 2030

4.2.1 Economic trends

The total Belgian cybersecurity **Sales figure** was set at **1.6 billion for 2021**. The same figure is at **2,61 billons for 2024** (+ 65% in 4 years).

According to a calculation of the Agoria Study Centre based on the survey results and the predictions from Statistica, Gartner and IDC, the Belgian cybersecurity market is expected to burst again in the coming years. The total cybersecurity sales figure should **be more 2 times higher in 2030 compared to the 2025** with a **Compound Annual Growth Rate (CAGR) of 15.9%** calculated by the Agoria Study Centre based on Statista, Gartner and IDC predictions even if a more likely outlook would be between 13% and 14%.

> *With the rapid evolution of artificial intelligence and the rising threat of hostile nation-states, it's crucial for the industry to reinforce and for the public and private sectors to work closely together. By creating a robust and resilient ecosystem, we can strengthen national cybersecurity.*

David Vanderoost
Chief Executive Officer
Approach Cybersecurity

4.2.2 Technological trends

The rise of Artificial Intelligence has already a dual effect on the cyber security sector. **Defensive AI** uses artificial intelligence to protect and defend against cyber threats, while **offensive AI** applies it to launch or enhance attacks. Both defensive AI and offensive AI will continue to rapidly evolve in a continuous cycle, with each advancement in attack capabilities driving stronger defences, and each new defence prompting more sophisticated attacks.

Whenever quantum computing will become a reality, it will be capable of breaking today's encryption methods, requiring companies to rethink cybersecurity and transition to **quantum-resistant protections**.

The big challenge for companies will be that moving to quantum-resistant encryption will take time, money, and major changes to their systems.

The **space sector**, which is now an essential sector in the NIS2 Directive, faces systemic cyber risks linked to the complexity of global supply chains and geopolitical tensions. The uneven resilience of actors and the rapid adoption of emerging technologies such as AI and quantum technologies (Quantum Key Distribution - QDQ) create additional vulnerabilities.

4.2.3 Regulatory trends

The NIS2 Directive and the Cyber Resilience Act (CRA) are complementary EU regulations that enhance cybersecurity in the European Union, with NIS2 focusing on the resilience of critical entities and their supply chains, and the CRA mandating cybersecurity for products with digital elements. Both regulations introduce increased obligations for risk management, incident reporting, and security updates throughout the product lifecycle, creating a comprehensive framework for digital security across the EU.

With the NIS2 directive translated into the Belgian law (entered in force in October 2024), the focus turns to putting the rules into actions

> *Space is a critical vector of necessary services for our society: we cannot secure earth without securing space.*

Matteo Merialdo
Director, Technology and Innovation
Nexova

5. Follow-up on of the 2022 report recommendations

Theme 1: Development of talents and education curricula

Recommendation 1
Increase our country's overall capacity for higher cyber education, and spotlight cybersecurity careers.

As already indicated in this report, the number of formal and non-formal curricula has increased during the last years in Belgium. Agoria has inventoried around 100 cybersecurity curricula during the summer 2025.

The **Belgian Cyber Security Coalition**, which has celebrated its 10th anniversary in 2025, counts, throughout its 12 focus groups, 18 academic institutions as members along with private companies and public institutions

In parallel, **Cyber Made in Belgium (CMiB)**, has created in 2022 a **focus group**, called **CMiB4Talent**, dedicated to the development of cybersecurity skills and the promotion of cybersecurity awareness. CMiB4Talent, supported by Agoria, brings together no fewer than 120 participants representing a complete triple helix comprising private, public and academic institutions and major organisations such as the Defence and Police forces.

Amongst the initiatives undertaken by CMiB4Talent, it is worth mentioning the **'A Day in the Life of' sessions for students**, led by cybersecurity experts. Overall, throughout its activities, we observe **an increasing of interest and participation of students** towards CMiB4talent events and initiatives.

Noëmie Honoré
Associate Partner, Global Cybersecurity Lead Belgium & Luxembourg, Wavestone

> *In Belgium, despite numerous initiatives, the proportion of women in cybersecurity has slightly shifted from 19% to 18%, even as demand for talent increases. Progress is slow, so it is essential that men and women work together to highlight opportunities, share their experiences and welcome more women into the field.*

Beyond facilitating communication between academia and industry, numerous initiatives are being undertaken to address the talent gap and increase the quantity and quality of the curricula offered.

An initiative worth mentioning is aimed at **better training human resources managers** and recruiters so that they can identify cybersecurity candidates' **potential** by looking beyond criteria such as individual **certifications**.

Rosetta Stone

The Rosetta stone is CMiB4Defence project co-initiated between the private sector and the Belgian Defense Cyber Force project supported by CMiB4Talent with the objective to reduce the talent gap for both stakeholders. It aims at being the foundation for facilitating the **collaboration between the market needs and the academia curricula offering**, while facilitating recruiters work and supporting NIS 2 compliancy.

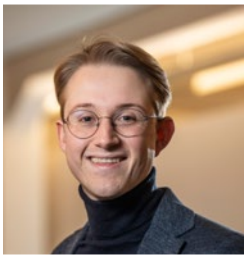
The language used to discuss cyber work and skills requirements is inconsistent. This hinders the nation's capacities to identify skills gaps and prepare the pipeline for the future cyber talents

The Rosetta stone is unifying the language of multiple worldwide skills frameworks (ECSF, NICE, SFIA and DCWF) using the 12 European Cybersecurity Skills Framework (ECSF) roles defined by European Union Agency for Cybersecurity (ENISA) as reference.

Jan De Blauwe
Chair of the Board
Belgian Cyber Security Coalition

> *"That is the value of our partnership with Agoria: a multiplier - by uniting industry voices with the Coalition's cross-sector platform, we strengthen resilience and Belgium's economy where it counts: in people, processes and technology."*

Since 2024, Agoria, in collaboration with Solvay Brussels School of Economics and Management and Howest, leads **CyberHub Belgium**, a three-year project funded by the European Commission, to address the shortage of cybersecurity professionals by fostering collaboration and innovation.



> *“Cybersecurity should be an integral part of our culture, taught at all ages. Only through this effort will society truly become resilient.”*

Gert-Jan Wille
Cybersecurity Venture Lead
Howest University of Applied Sciences

Future Workforce

The Agoria Future Workforce initiative aims to boost companies' competitiveness by supporting them in **attracting, developing, and retaining talents**, while also preparing their workforce to meet future demands and challenges.

The program uses **data** to forecast skills requirements, link different **talent pools**, and boost people's employability through upskilling. Its purpose is to prepare individuals for careers in ICT, cybersecurity, AI, and other digital sectors, helping address the shortage of specialists while also enhancing overall digital competence.

On the diversity side, since 2019 **Women4Cyber** promotes, encourages, and supports the participation of women in cybersecurity by fostering a more gender-inclusive community. The foundation has grown significantly internationally and counts currently 33 national chapters.

> *“Cybersecurity starts with people. At Women4Cyber Belgium, we foster a trusted community built on support, personal growth, and diversity.”*

Leila Abajadi
Chairwoman,
Women4Cyber Belgium

Women4cyber Belgium, officially launched in 2024, has 10 Board Directors, including women in senior positions at the CCB and the European Commission, as well as men from the Belgian Cybersecurity Coalition, Agence du numérique, Agoria, ...

Part of its activities, Women4Cyber Belgium is proposing mentoring program, scholarship training for women and young ladies.

It also worth mentioning **Women in Tech Belgium** and **SheLeadsTech Belgium** which communities that empower and support women's growth, leadership, and visibility in the Belgian tech industry.

Theme 2: Awareness

Recommendation 2

Launch regional and national awareness campaigns, targeting management levels in the public and private sector, and the different governments.

The Centre for Cybersecurity Belgium (CCB), through Safeonweb has created national several campaigns such as an **anti-phishing campaign** in 2023 a campaign promoting the use of **2 factor authentication** and, is launching a campaign dedicated to the **prevention of investment fraud** in October 2025. The campaigns use to be relayed by the Belgian Cyber Security Coalition and Agoria to its members.

> *"Cybersecurity is a must to safeguard Belgian competitiveness; resilience, awareness, and automation are now essential."*

Stijn Van Impe
Global sr. Director cybersecurity solutions
Unisys Belgium

At the regional level, VLAIO, for the Flemish audience, and Walhub, for the French speaking audience, proposes since 2023, through a partnership with Sirris and Agoria, a free awareness e-Learning program for Flemish entrepreneurs and SMEs Program called **Cyberstart** (Agoria, 2023). It is a weekly e-tutorials with tips, tools, and a concrete step-by-step plan to improve their cyber resilience.

Flanders hosts several **noteworthy cybersecurity-related events** and initiatives throughout the year—especially in 2024–2025—targeting different audiences from SMEs to government IT officials.

Wallonia hosts **"Cyberweek"**, an annual cybersecurity awareness week is organized by Cyberwal by Digital Wallonia and partners. It offers events conferences, live demonstrations, communication campaigns, and more.

Brussels also ran a **Cyberweek 2024**, focusing on AI and cybersecurity, organized by Digitalcity.brussels.

Besides Cyberstart, AGORIA has developed two other free, bilingual (NL/FR) tools dedicated to supporting SMEs in their journey towards resilience by adopting cyber hygiene: **Cyberboost** (Agoria, 2024), an online boot camp consisting of five modules and 15 hours of training, and **Cyber Risk Scan** (Agoria, 2025).

The introduction of the **NIS2 law** has also greatly contributed to raising awareness among decision-makers thanks to the new obligations imposed on its members in terms of cyber risk awareness.

Recommendation 3

Inspire sector federations and governments to set a cybersecurity plan objective for 2025.

In 2022, 53% of the companies surveyed by Proximus (Proximus, 2022) had cybersecurity strategy in place. In its recent report, Proximus indicates that between **73 and 74% of the companies surveyed have cyber strategy** covering prevention and detection, which represents an increase of approximatively 21% in three years (Proximus, 2025).

This level remains relatively low, especially when considering that only 39% of the large companies have implemented a cybersecurity incident response process with high confidence of their ability to recover from cybersecurity incidents. Concerning SMEs, this confidence reaches 48% thanks to their higher flexibility to develop a robust strategy. (Proximus, 2025)

> *Cybersecurity is, above all, about resilience - protecting our economy and essential services for citizens. Achieving resilience requires investing in training people and working together across private, public, and educational sectors to stay ahead of evolving threats.*

Lorenzo Bernardi
Head of Security Services & CSO
Network Research Belgium (NRB)

To increase of the number of companies having a cyber security strategy, **Agoria** has developed a tool called **Cyber Risk Scan**, based on the Cyber Fundamentals® Basic of the CCB, allowing companies to create a cyber strategy by answering a questionnaire **covering 13 key security measures** (Agoria, 2025).

Why a cybersecurity strategy help an SME stand out?

Cybersecurity risks also arise when attackers exploit their victims' supply chain vulnerabilities. Due to failures in the implementation of security measures by third parties, hackers can potentially compromise all of a company's networks and operations. It is essential, that SME executives recognize their critical role as suppliers in the supply chains of companies regulated under NIS2.

Having a clear cybersecurity strategy is no longer optional for SMEs—it is essential. It strengthens resilience, protects sensitive data, ensures compliance, and safeguards trust. Beyond defence, it creates competitive advantages, positioning SMEs as secure, reliable, and preferred partners.

The goal of this recommendation being to increase the cyber resilience of the Belgian ecosystem, numerous initiatives are now available for free to support companies in the development of their cybersecurity strategies.

To name a few, we can mention **Cyber threat Alerts, Safeonweb Browser Extension** or **Quick Scan Report** proposed by the CCB (CCB, 2025c) or the SME-focused tool QuickScan proposed by the FPS Economy (FPS Economy, 2025).

Theme 3: Growth roadmap for the sector

Recommendation 4

Invite all regions and other stakeholders to consider supporting cyber start-up and scale-ups.

Cybersecurity start-ups and scale-ups can leverage federal initiatives such as the **tax shelter**, which attracts private investment, and **IP support** to protect algorithms, software, and patents. In addition, **entrepreneurship project calls** often provide opportunities to fund cybersecurity awareness and innovation projects

Created in 2021, the **National Cybersecurity Coordination Centre Belgium** (NCC-BE / CCB) can support cybersecurity start-ups and scale-ups by connecting them to EU funding, international research collaborations, and investment opportunities, strengthening their growth. (CCB, 2025d)

> *“Staying ahead in Cybersecurity requires deep technical expertise and continuous innovation.”*

Bart Preneel
Full professor, Head of research group COSIC
KU Leuven

At the regional level, Cybersecurity start-ups and scale-ups in Brussels benefit from **hub.brussels** through its incubators and accelerators, which provide coaching, workspace, and mentoring.

Additional project calls allow cyber companies to position their solutions around **resilience, digital sovereignty, and impact entrepreneurship**. Similarly, **Innoviris** supports ambitious cyber ventures with funding schemes such as the **Innovative Starters Award**, innovation vouchers, and project calls that foster R&D in cybersecurity.

In Flanders, **VLAIO** offers targeted support for cybersecurity companies aiming to grow and internationalise. Its **Schaalklaar subsidy** helps innovative cyber firms scale, while **Scaleup Flanders** and dedicated **R&D funding** provide the resources needed for rapid expansion and cutting-edge innovation.

Wallonia's **Agence du Numérique** plays a central role through the **Digital Wallonia strategy**, where cybersecurity is a key priority. Initiatives such as **Cyberwal by Digital Wallonia**, launched in 2022, encourage cyber start-ups and scale-ups to innovate and expand, while programs like **Espace Public Numérique** contribute indirectly by supporting digital inclusion and cybersecurity awareness.

Recommendation 5

Promote export trade and facilitate foreign investments in Belgian cybersecurity skills and services.

There are initiatives to promote export at the federal and regional levels, as well as private level.

As already mentioned above, the **National Cybersecurity Coordination Centre Belgium (NCC-BE / CCB)** plays a key role in connecting Belgian cybersecurity organisations to European opportunities by coordinating EU funding programmes strengthening their competitiveness in global markets. (CCB, 2025d)

> *True cyber resilience will come from continuous improvement, bridging IT and OT, and securing every layer of society.*

Steven Vinckier
CEO
Spotit

In Brussels, **hub.brussels** helps cybersecurity companies internationalise through training, coaching, and support with export procedures. Its global network of trade and economic attachés provides market intelligence and facilitates connections with potential buyers worldwide. (hub.brussels, 2025)

In Flanders, **FIT – Flanders Investment & Trade** provides sector-specific support to cybersecurity firms. Its dedicated ICT Welcome Team facilitates foreign investments while assisting local companies with export planning, international networking, and scaling abroad. (FIT, 2025)

In Wallonia, the **AWEX – Wallonia Export & Investment Agency** actively promotes the region's cybersecurity excellence abroad. Through trade missions, international representation, and partner matchmaking, it helps cyber companies expand their global reach. (AWEX, 2025)

With the support of the CMiB members and partners being public institutions, academia or private companies, **Agoria** ensures presence to several international trade shows dedicated to cybersecurity. To name of few, we can mention presence at the Forum INCYBER (FIC) in Lille, where more than 180 Belgian delegation representatives showed up at the Belgian booth in 2024, at the Cybersec Netherlands in Utrecht and Nexus in Luxemburg.

Moreover, Agoria and some of its CMiB partners are actively involved in **relationship with various embassies**, such as Japan, USA, Canada or Poland and has taken part to international visits such Cyber Defence day in Estonia, Campus Cyber in France or CyberHubs meeting in Lubijna aiming at fostering European synergies.

6. Key takeaways

- **Total cybersecurity revenue rose** from €1.58 billion in 2021 to €2.61 billion in 2024 (+65%), while **employment increased** from 6,405 to 9,750 FTE (+52%)
- The rise of artificial intelligence is already having a dual effect on cybersecurity, with defensive **AI used for protection and offensive AI used for attack**, while the advent of **quantum computing** will challenge current encryption methods and require a transition to quantum-resistant protections.
- Belgium still faces an estimated **shortfall of 6,190 cybersecurity specialists**, even as the entry into force of the NIS2 Directive and the Cyber Resilience Act increases capacity requirements, with a greater focus on the specific needs of critical infrastructure and defence.
- It is important to emphasise that **academic provision is not perfectly aligned with market needs**. It often covers certain specialisms too narrowly, whereas the sector requires a much broader range of skills and in greater numbers.
- Despite numerous initiatives, the **proportion of women in cybersecurity has barely changed**, falling from 19% to 18%, which shows that progress remains slow and that pressure must be maintained to attract more diversity to the sector.
- **Trusted partnerships**, both in Belgium and internationally, form the foundation of our cyber resilience and inspire us to innovate together.

> *"The potential for Belgian industry goes far beyond cybersecurity alone. Counter-drone solutions include an offensive, cyber-mindset approach."*

Lt-Gen Michel Van Strythem
former Cyber Commander,
Chief Innovation Defense and head of Task Force Drone.

7. Acknowledgements

We sincerely thank our executive, financial, and CMiB sponsors whose support made this research possible. Their commitment has enabled us to build a strong foundation for future growth and success in cybersecurity.

We are deeply grateful to the companies that participated in the survey. Their valuable insights allowed us to present an accurate picture of Belgium's cybersecurity sector.

Trusted partnerships are critical

We can thank and mention the valuable ongoing national trusted partnerships:

- With **Defense** within the CMiB4DEF focus group reinforcing the collaboration between the private sector and the Cyber Defense needs,
- With **CCB** about the opportunity to contribute to the national cybersecurity strategy, the Cyber Fundamental® 2025 and promotion of the national awareness campaign 'safeonweb'.
- With Belgian **Cyber security coalition** demonstrates the power of collaboration in strengthening Belgium's digital resilience. By combining Agoria's industry reach with the Coalition's cross-sector expertise, we amplify awareness, foster trust, and accelerate the adoption of best practices across businesses of all sizes.

By pooling our networks and expertise, we make it easier for organisations to learn fast, comply smartly and invest where it matters.
Finally, we warmly thank the **Howest Hogeschool** and **Solvay Brussels School of Economics & Management** for the long-standing and fruitful collaboration with Agoria across numerous joint projects, and especially for its role in mapping and gathering the data at the core of this report.

Executive partners

(In alphabetic order)

- Agoria/Cyber Made in Belgium (CMiB)
- Belgian Defense Cyber Force
- Belgian Cyber Security Coalition
- Centre for Cybersecurity Belgium
- Howest Hogeschool
- Solvay Business Scholl of Economics and Management
- Women4Cyber

Financial sponsors

(In alphabetic order)

- Approach Cyber, Cegeka, Nexova, Network Research Belgium (NRB), Nviso, Orange Cyberdefense Belgium, Proximus, Toreon, Spotit and Unisys

Surveyed companies

(In alphabetic order)

- Aikido Security, Apogado, Approach Cyber, Axians Belgium, AXS Guard - Able, BV, B12 Consulting, Briol & Partners, Centran, Cheops Technology NV, CREIT, Cresco, Cyber Praxis, Cyen, ACOServices, DigiSôter, DigiTribe, e-BO Enterprises, Easi, Easiance, Elimity, Emmera SRL, Ernst & Young Advisory Services, Global Cyber Alliance Belgium, Guardsquare, Inetum Belgium, Innocom, ITNM BV, LuxTrust S.A, Matias Consulting Group (MCG), mobco, Naval Group Belgium, NET-measure, Nokia Bell, Nomios Belgium, NPS Consult Group, Network Research Belgium (NRB), Nviso, Office-IT, Orange Cyberdefense Belgium, OutKept, Ozoos, PeopleWare, Proximus NXT IT, Refracted Security, Safran Aero Boosters, Scalable Solutions, Sealed, Secure Code, Warrior, Secutec, Smart Business Partner (former NRC Benelux), Soterics, Spotit, Sword Integra , Synergit, Technifutur, Telenet Business, Telespazio Belgium, Toreon, Uniwan.be, van der Maren

Contributors

At Agoria

- Study Department, Marketing & Communications, Senior Management & Board of Directors.
- More specifically Stanislas Van Oost, Patrick Slaets, Ann Peeters, Eric Van Cangh, Saskia Van Uffelen, Christophe Vantongelen, Cassylinne Mees, Myriam Gillisjans and Jan Gatz.

At Solvay

- Georges Ataya, Erlind Shalaj, Elies Bortolin

External support

- Manuel Gonzalez Peña – Kyrielle

8. Methodology

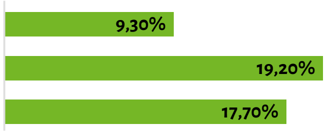
To adequately represent the Belgian cybersecurity sector, we chose to incorporate quantitative and qualitative components in our research. We translated that dual approach into the survey with quantitative questions and open qualitative questions.

Quantitative survey component

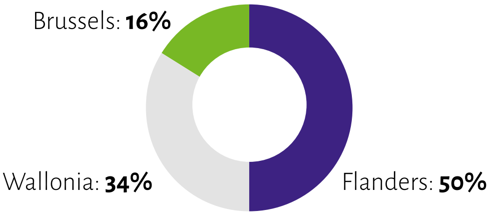
The questionnaire comprised **ten quantitative questions** that inquired about the companies' sales figures, expected sales figures in 2025, the markets in which they operate, export ratio, activities in the five CyBOK fields (see below), employees, open vacancies, and the diversity of its workforce in terms of age and gender.

Sample size

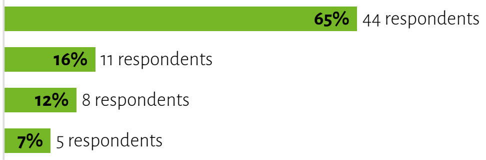
68 entities
of the Belgian cybersecurity companies
of the total cybersecurity sales figure
of the total cybersecurity employment



Division by region
Flanders: 34 respondents
Wallonia: 23 respondents
Brussels: 11 respondents



Division by company size
0-49 employees
50-99 employees
100-499 employees
500+ employees



Qualitative component

The survey conducted during the 2025 summer contained six open-ended questions. The questions focused on the sector's knowledge gap, the biggest challenges and threats, key opportunities, industry recommendations, and advice (directed to policymakers) on how to make the Belgian cybersecurity sector more competitive.

Study process

We asked Solvay Brussels School of Economics and Management students to identify and map out all companies that offer cybersecurity solutions, services and products in Belgium. Their resources included, but were not limited to, LinkedIn, various Agoria partners, the Belgian Cyber Security Coalition, the European Cyber Security Organisation (ECSO), the Agence du Numérique (AdN), Flanders Innovation & Entrepreneurship (VLAIO), the Association of Flemish Cities and Municipalities (VVSG), and exhibitors at events such as Cybersec Europe and the Belgian Cyber Security Convention.

All data were then classified according to a fixed framework that contained the company's name, VAT number, postcode, website, type (e.g., consulting agency, vendor, etc.), and a comment section detailing the company's cybersecurity activities in our country. The final list comprised 732 entities (companies and organisations). All of these were invited to fill out the survey.

Eventually, after verifying all submitted answers, the survey yielded 71 completed forms representing 68 entities. The results were divided by region and by company size.

The sample corresponds to 9,3% of the Belgian cybersecurity population, 19,2% of the total cybersecurity sales figure, and 17.7% of the sector's total cybersecurity employment. This representation allowed us to confidently extrapolate their results to the entire cybersecurity population in Belgium

Taxonomy

We used the open-source CyBOK taxonomy (CyBok, 2021). This classification organises cybersecurity activities into five categories (systems security, Software and platform security, infrastructure security, human, organizational and regulatory aspects, attacks and defences).

9. References

- **Agoria. (2022) Whitepaper: First socio-economic study on the cyber security sector in Belgium**
  https://www.agoria.be/en/services/expertise/digitalisation/cybersecurity/whitepaper-first-socio-economic-study-on-the-cyber-security-sector-in-belgium

- **Agoria. (2023) Cyberstart**
  https://www.agoria.be/cyberstart or https://www.agoria.be/cyberstart/fr

- **Agoria. (2024) Cyberboost**
  https://www.agoria.be/cyberboost/fr or https://www.agoria.be/cyberboost/nl

- **Agoria. (2025) Cyber Risk Scan**
  https://www.agoria.be/fr/services/expertise/digitisation/cybersecurity/le-nouveau-cyber-risk-scan-aide-les-entreprises-a-decouvrir-leurs-vulnerabilites-numeriques or https://www.agoria.be/nl/diensten/expertise/digitalisering/cybersecurity/nieuwe-cyber-risk-scan-helpt-bedrijven-hun-digitale-zwakke-plekken-blootleggen

- **CCB. (2021) Cyber Security Incident Management Guide**

- **CAltindex. (2025) AI Cybersecurity Market to Quadruple and Hit a $133 Billion Value by 2030**
  https://altindex.com/news/ai-cybersecurity-to-surge

- **Awex. (2025)**
  https://www.awex-export.be/fr/accueil

- **CCB. (2021) Cybersecurity Strategy Belgium 2.0 2021-2025**
  https://ccb.belgium.be/sites/default/files/2024-10/CCB_Strategie%202.0_UK_WEB.pdf

- **CCB. (2021a) Cyber Security Incident Management Guide**
  https://cybersecuritycoalition.be/wp-content/uploads/cybersecurity-incident-management-guide_EN.pdf

- **CCB. (2025a) Largest cyber security operation ever in Belgium: 2410 organizations from critical sectors take action**
  https://ccb.belgium.be/news/largest-cyber-security-operation-ever-belgium-2410-organizations-critical-sectors-take-action

- **CCB. (2025b) Cybersecurity education in Belgium**
  https://ccb.belgium.be/school/cybersecurity-education-belgium

- **CCB. (2025c) Safeonweb @ work**
  https://atwork.safeonweb.be/

- **CCB. (2025d) National Cybersecurity Coordination Centre Belgium (NCC-BE)**
  https://ccb.belgium.be/ncc

- **CyberHub Belgium. (2024) Cybersecurity Skills Needs Analysis report Belgium**
  https://cyberhubs.eu/resource/cybersecurity-skills-needs-analysis-in-belgium/

- **Conseil supérieur des indépendants et des PMEs. (2024) Rapport annuel 2024**
  https://www.csipme.fgov.be/_files/ugd/aabb75_18c81a29144e4481a056449419923b8c.pdf

- **Check Point Software technology. (2025) The state of cyber security 2025**
  https://www.checkpoint.com/security-report/

- **CMiB. (2025) Cyber Made in Belgium (CMiB)**
  https://www.agoria.be/en/themes/business-groups/safety-security-defence/cyber-made-in-belgium-cmib/cyber-made-in-belgium-introduction

- **Cybersecurity Ventures. (2025) Cybercrime to Cost the World $10.5 Trillion Annually By 2025**
  https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

- **Cybok. (2021) Introduction to CyBOK Knowledge Area Version 1.1.0**
  https://www.cybok.org/media/downloads/Introduction_v1.1.0.pdf

- **ENISA. (2022) European Cybersecurity Skills Framework Role Profiles.**
  https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles

- **FIT. (2025) Invest in Flanders**
  https://invest.flandersinvestmentandtrade.com/en/sectors/digital-industry

- **FPS Economy. (2025) Quickscan**
  https://mijnzaakcyberveilig.be/ or https://mapmecybersecurisee.be/

- **Gartner. (2022) 3 Planning Assumptions for Securing Cyber-Physical Systems of Critical Infrastructure**
  https://www.gartner.com/en/articles/3-planning-assumptions-for-securing-cyber-physical-systems-of-critical-infrastructure?

- **Gartner. (2025) Gartner Forecasts Worldwide End-User Spending on Information Security to Total $213 Billion in 2025**
  https://www.gartner.com/en/newsroom/press-releases/2025-07-29-gartner-forecasts-worldwide-end-user-spending-on-information-security-to-total-213-billion-us-dollars-in-2025

- **hub.brussels. (2025) Support for internationalisation**
  https://info.hub.brussels/en/guide/growing-your-business-export/support-internationalisation

- **ICS2 ((ISC)²). (2024) global Cybersecurity workforce Prepares for an AI-Driven World**
  https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study

- **Proximus. (2022) The impact of cybersecurity on companies in the Benelux**
  https://cybersecurity.proximus.be/research-report-2022/results

- **Proximus. (2025) In the crosshairs: 6th Annual Cybersecurity Survey Results**
  https://nxt.proximus.be/cybersecurity_report_en

- **VLAIO. (2025) CS barometer**
  https://www.vlaio.be/nl/nieuws/helft-vlaamse-bedrijven-2024-slachtoffer-van-cyberaanval

- **VRT. (2024) Cyber-attacks on the rise, Belgium an increasingly popular target**
  https://www.vrt.be/vrtnws/en/2024/11/26/_cyber-attacks-on-the-rise-belgium-an-increasingly-popular-tar/

- **WEF. (2024) Global Cybersecurity Outlook 2024**
  https://www.weforum.org/publications/global-cybersecurity-outlook-2024/

- **WEF. (2025) AI agents: the new frontier of cybercrime business must confront**
  https://www.weforum.org/stories/2025/06/ai-agent-cybercrime-business

Cyber Made in Belgium executive partners

Cyber Made in Belgium financial sponsors

(In alphabetic order)

Disclaimer

Agoria makes every effort to collect and share qualitative and up-to-date information, but cannot guarantee the full accuracy or completeness of the information provided. This information is in no way intended as personalised legal or other advice. Agoria disclaims any responsibility for the content of the report or the use that might be made of it. The reader or user is also aware that this information is subject to change without notice.

DF 82/06
DX 01/87
YU 07/26

About Agoria

Technology federation Agoria unites more than 2,250 Belgian businesses, 70% of which are SMEs. Together, they represent approximately 340,000 employees. They all have one ambition in common: strive for progress in the world, through the development or application of innovative technologies.

Agoria, which counts 200 employees, aims to connect all those inspired by technology and innovation, increase their success, and shape them in a sustainable way. Its service focuses on digitisation, the manufacturing industry of tomorrow, talent policy and training, market development, regulation, infrastructure, climate, environment and energy.

Cyber Made in Belgium (CMiB), an important subdivision of Agoria, represents 120 entities specialising in cyber security and promotes a dynamic ecosystem that provides solutions and services through close collaboration with academia, the public sector, government and security organisations such as the Ministry of Defence and the Police.

Find out more at agoria.be/en/cmib

About Solvay Brussels School of Economics and Management

Solvay Brussels School of Economics and Management, part of Université Libre de Bruxelles (ULB), is a leading European institution recognized for its excellence in business, economics, and management education.

Solvay Business School combines rigorous academics with strong corporate ties to foster innovation, entrepreneurship, and leadership across a wide range of international programs. Supported by vibrant research and Brussels' role as a European hub, it prepares students to excel in dynamic global markets.

Find out more at solvay.edu

About the Ministry of Defence

The Belgian Ministry of Defence has created the Belgian Cyber Force to defend military weapon systems and support operations against cyber threats. It constitutes a rapidly expanding civilian and military environment that creates close synergies with the public and private sectors, industries and academia. The Cyber Capacity houses experts in every cyber security domain imaginable, but also – and this is unique in Belgium – experts in offensive cyber operations.

Together with various national and international stakeholders and with the academic, industrial and non-profit sectors, the Belgian Cyber Force works every day to support Belgian cybersecurity.

Find out more at www.mil.be

About the authors

Eric Van Cangh
Senior Business Group
Leader Digital

+32 492 23 24 34
Eric.VanCangh@agoria.be

Stanislas Van Oost
Senior Cyber
Security consultant

Stanislas.vanoost.ext@agoria.be

Patrick Slaets
Senior Expert
Studies Centre

+32 497 27 76 48
patrick.slaets@agoria.be

Georges Attaya
Academic
director

gataya@solvay.edu

Embracing technology
Embracing ambition

.AGORIA

Agoria means progress through technology. We are paving the way for all technology-inspired companies in Belgium pursuing progress internationally through the development or application of innovations and which, together, represent some 324,000 employees. We are proud that more than 2,000 member companies trust in the three pillars of our services: consulting, business development and the creation of an optimal business environment. Follow us on **www.agoria.be** and **https://X.com/agoriafr**.

www.agoria.be