First socio-economic study on the cyber security sector in Belgium

November 2022

Embracing technology
Embracing ambition

.AGORIA

CONTENTS

else, we will immediately match the price.
PeopleImages.com as part o
r exponentially. You will receive a receipt with a license.
age you wa

1/ FOREWORD

Dear reader,

As technology becomes more sophisticated, so do **cyber criminals and state-sponsored cyber actors**. They target every corner of the digital universe, from personal computers and online wallets to top-secret military intelligence – and everything in between. When they strike, they can impact multiple countries, economies, and millions of citizens all at once.

Therefore, our country must strengthen its digital resilience and lessen its dependence on products and services acquired outside Belgium and Europe. A **competitive cyber security sector** will allow us to keep up with all the changes in the field and anticipate threats. That requires a high level of expertise – not only in academia, but also in the public and private sectors.

The perception that cyber security is an overpriced and technical concern, is profoundly misguided. An increasing number of people and business leaders realise that, instead, cyber security provides an **opportunity** for both companies and citizens to take digitisation to the next level.

One data leak is enough to damage your customers' trust forever. One click in a phishing email is enough to lose your life savings. Consequently, an investment in cyber security means an investment in **business continuity and online safety**, a strong economy, and a secure digital life. All of these are key ingredients of 21st-century success.

But where do we start? More than ever, we need insights into the Belgian cyber security sector. That is why Agoria and its executive sponsors, the Ministry of Defence and the Centre for Cyber Security Belgium (CCB), conducted **the first-ever socio-economic study on the cyber security sector in Belgium**.

The study generated a wealth of information, which you can explore in the pages ahead, and presented **a unique opportunity**: with these findings, we can connect all layers of the cyber security ecosystem – from schools and governments to enterprises and customers – and make everyone realise the enormous potential of cyber security in Belgium.

We cannot let that potential go to waste. Cyber security embodies **the ultimate online protection** of our society and economy. Giving the sector our undivided attention is the least we can do in return.

Alexander De Croo,
Prime Minister of Belgium

Bart Steukers,
CEO Agoria

2/ EXECUTIVE SUMMARY

The global cyber security market is flourishing, constantly fuelled by technological innovations and the digital transformation of our daily lives from the pandemic era. The protection of online infrastructures and sensitive data has become a top priority for businesses and leaders around the world. After all, an investment in cyber security is **an investment in resilience, business continuity, and customer trust**. Excellent cyber hygiene enables organisations to comply with ever-tightening regulations and provides a solid shield against cybercrime.

Cyber security in Belgium

But what about the Belgian cyber security landscape? Is its digital autonomy strong enough to face cyber security challenges, now and in the future? Inspired by Australia's Cyber Security Sector Competitiveness Plan[1], Agoria and its executive sponsors found answers by conducting **the first-ever socio-economic study on the cyber security sector in Belgium**. The result offers **unique insights** into the Belgian cyber security sector as a whole, its (missed) opportunities, challenges and threats.

Key figures for the Belgian cyber security sector (2021)

441
Cyber security **companies**

€1.58 billion
Total cyber security **sales figure**

6,405 FTEs
Total cyber security **employment**

21.2%
Expected Compound **Annual Growth Rate** (2021-2025)

1,205
Cyber security **vacancies**

16.4%
Cyber security **export percentage**

All things considered, the sector has enormous potential, but is slowed down by multiple **challenges**. It needs mutual collaboration, a focused innovation capacity, a broader internal market, and an influx of investments and talented employees. Additional efforts are necessary to inform citizens, companies, and governments – and motivate their appropriate action.

Furthermore, the sector **fails to reach its target audience**. All too often still, managers and board members consider cyber security as a complicated technical issue with a hefty price tag – instead of an insurance against potentially devastating digital dangers. Consequently, most small and medium-sized enterprises (SMEs) only minimally integrate it into their risk-management policies – or not at all. That puts them below the **Cyber Security Poverty Line** (cf. section 4), meaning that their essential security capabilities, skills and services are insufficient.

[1] https://www.uastcyber.com/resources/sector-competitiveness-plan

Recommendations

On a strategic level, the cyber security sector is **incredibly important for our country**, its citizens, and the Belgian economy in general. It is time to recognise it as such and start managing it with the professionalism it deserves.

Both cyber security market expectations and European cyber regulations are becoming increasingly demanding. To cope with those requirements, Belgian cyber security organisations **need the capability to scale** in a supportive governmental and economic environment. That is why we have formulated five priority recommendations – clustered around three central themes – for the industry, government institutions, and all layers of the cyber security ecosystem.

Three themes, five recommendations

Development of talent and education curricula	1. Increase our country's overall capacity for higher cyber education, and spotlight cyber security careers
Awareness	2. Launch regional and national awareness campaigns, targeting management levels in the public and private sector, and the different governments 3. Inspire sector federations and governments to set a cyber security plan objective for 2025
Growth roadmap for the sector	4. Invite all regions and other stakeholders to consider supporting cyber start-ups and scale-ups 5. Promote export trade and facilitate foreign investments in Belgian cyber security skills and services

When properly executed, these recommendations will help the sector to grow and scale as needed, and **equip the Belgian cyber security sector for success**, so it can keep guarding our digital safety.

Moreover, we want to confidently position and profile Belgium as a haven for scalable innovative cyber security solutions, and establish **a cyber security powerhouse** in the heart of Europe.

Conclusion

The Belgian cyber security sector is one of our country's most valuable assets. Its growth rate is in the double digits, and it provides both an answer to global societal challenges and a key to further technological innovation. Only with more attention, focus and funding will it **reach its full potential**: protecting our governments, industries and citizens, and creating thousands of jobs and boosting our export trade along the way.

Therefore, we would like to invite all our partners and stakeholders to join forces and turn these objectives into reality. **Let's make it happen together.**

> The cyber security industry grows by double digits, and it won't slow down anytime soon. It is a great source of highly valuable jobs - exactly what we need to boost our economy

Jan De Blauwe
Chair, Cyber Security Coalition
COO and Managing Director, NVISO

3/ BACKGROUND

Before we dive into the numbers, let's define cyber security and contextualise its position in Belgium, the European Union and beyond. This chapter provides that background, including a high-level overview of the Belgian cyber ecosystem and its key players.

3.1. What is cyber security?

The Belgian Cyber Security Strategy 2.0 (2021)[2] defines cyber security as "the result of a set of security measures that minimise the risk of disruption or unauthorised access to information and communication (ICT) systems". This includes systems belonging to citizens, businesses, organisations and governments.

3.2. Context

3.2.1. Cyber security as a new global priority

In 2021, the global cyber security market was worth $139.77 billion. For 2029, its projected value is $376.32 billion – a Compound Annual Growth Rate (CAGR) of 13.4%[3]. According to the World Economic Forum's Global Risks Report 2022, business leaders and governments around the world have started to consider cyber security as **a top priority** in their national and international policies[4].

> Business leaders are defining new priorities, such as IT security strategies, data governance and user awareness
>
> **Danielle Jacobs**
> **Chief Executive Officer, Beltug**

Beltug, the Belgian association of CIOs and digital technology leaders, confirmed that worldwide trend in its **2022 Beltug Priorities Compass**[5]. More than 250 Chief Information Officers submitted their list of priorities, which resulted in the following top three:

1. ***IT security strategy***
2. ***IT security architecture***
3. ***Taking control of hybrid IT (on the premises and in the cloud)***

That level of attention is justified. In its State of the Union 2022, the European Commission estimated that **data breaches cost at least €10 billion per year**[6]. For attempts to disrupt internet traffic, that figure amounts to at least €65 billion.

Soon, customers themselves will ask companies to adhere to strict cyber security policies. Technological research and consulting firm Gartner predicts that businesses will face **increasing pressure** regarding their cyber security standards in the future[7]. When buying goods or services, customers will want to know for sure that their data will always be kept safe – and their trust intact.

[2] https://ccb.belgium.be/sites/default/files/CCB_Strategie%20 2.0_UK_WEB.pdf

[3] https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165

[4] https://www.weforum.org/reports/global-risks-report-2022/

[5] https://www.beltug.be/impact-item/les-priorites-des-cio-belges-et-de-leurs-equipes-la-gestion-des-donnees-et-les-defis-lies-a-larchitecture-informatique-et-a-la-cybersecurite-sont-des-priorites-absolues-pour-les-decideurs-tic/

[6] https://ec.europa.eu/commission/presscorner/detail/en/IP_22_5374

[7] https://www.gartner.com/en/doc/757928-predicts-2022-cybersecurity-leaders-are-losing-control-in-a-distributed-ecosystem

> The rapid convergence of IT and security operations drives the need for a strong Belgian cyber security ecosystem
>
> **Fabrice Wynants**
> **Global Director Cyber Security, Cegeka**

3.2.2. Cyber security in Belgium

Cybercrime incidents

In a resolution proposal against internet fraud, the Belgian Chamber of Representatives reported a total of 37,982 cybercrime incidents for the year 2021[8]. That equals **more than 100 cyberattacks a day**, a 37% increase compared to 2019. Almost 70% escaped prosecution.

Proximus' study 'How companies manage cyber security' (2021)[9] demonstrated that **cyberattacks surged during the COVID-19 lockdown**. Many companies were not prepared for hybrid working in terms of infrastructure, policies and training, which extended their digital vulnerabilities.

As a result, hackers launched **19% more phishing attacks** than ever reported before. In 2020, 42% of small and medium-sized enterprises dealt with a cyber incident. In 38% of the affected companies, it caused a business standstill. An alarming number, given that 50% of all organisations in Belgium and the Netherlands **do not have an active cyber security strategy**.

Furthermore, an analysis by Mastercard (2022) indicated that almost 1,000 Belgian businesses were the victim of a cyberattack in 2021[10]. **Priority targets** were the Belgian government (24% of all attacks) and financial institutions (21%). On average, those sectors encountered 50 to 70 cyberattacks per quarter.

In Agoria's study 'Cyber security in the manufacturing industry' (2021)[11], 48% of the respondents said that, in the event of a cyberattack, they would not know what to do or how to react appropriately.

Belgian cyber security policies: regional examples

On a regional level, several cyber security policies are already in place. Flanders, for example, follows the **Flemish Cyber Security Policy Plan**[12]. This policy has three components: international top research on cyber safety, enhanced cyber maturity for businesses, and more awareness and education regarding cyber safety.

In Wallonia, the new **'CyberWal by Digital Wallonia'** programme[13] unites more than 100 cyber security stakeholders. It builds on existing initiatives such as the **'Keep It Secure'** plan[14], which helps SMEs improve their cyber maturity, and the '**CyberExcellence'** research project[15], which wants to create tools and recommendations for a thoughtful, efficient and competitive cyber security strategy.

The Belgian cyber ecosystem and its stakeholders

In 2020, more than 97% of all Belgian companies were SMEs[16]. That particular labour market houses an intricate ecosystem of cyber security stakeholders. At the heart of the ecosystem is the **interaction** between two parties: cyber security suppliers and their consumers. That relationship is influenced by several entities, such as the federal and regional governments, cyber research and development, and the different cyber policies.

Both the interaction and its influencing entities are protected by a variety of national and international organisations, such as intelligence services and EU cyber agencies.

[8] https://www.dekamer.be/FLWB/PDF/55/2627/55K2627001.pdf

[9] https://cybersecurity.proximus.be/survey2021/research-report-cybersecurity

[10] https://www.mastercard.com/news/europe/en/newsroom/press-releases/en/2022/january/mastercard-reveals-record-levels-of-cybercrime-in-belgium-during-the-pandemic/

[11] https://www.agoria.be/fr/etude-Cyber-securite-dans-industrie-manufacturiere

https://www.agoria.be/nl/studie-Cybersecurity-in-de-maakindustrie

[12] https://www.vlaio.be/nl/begeleiding-advies/digitalisering/cybersecurity/vlaams-beleidsplan-cybersecurity

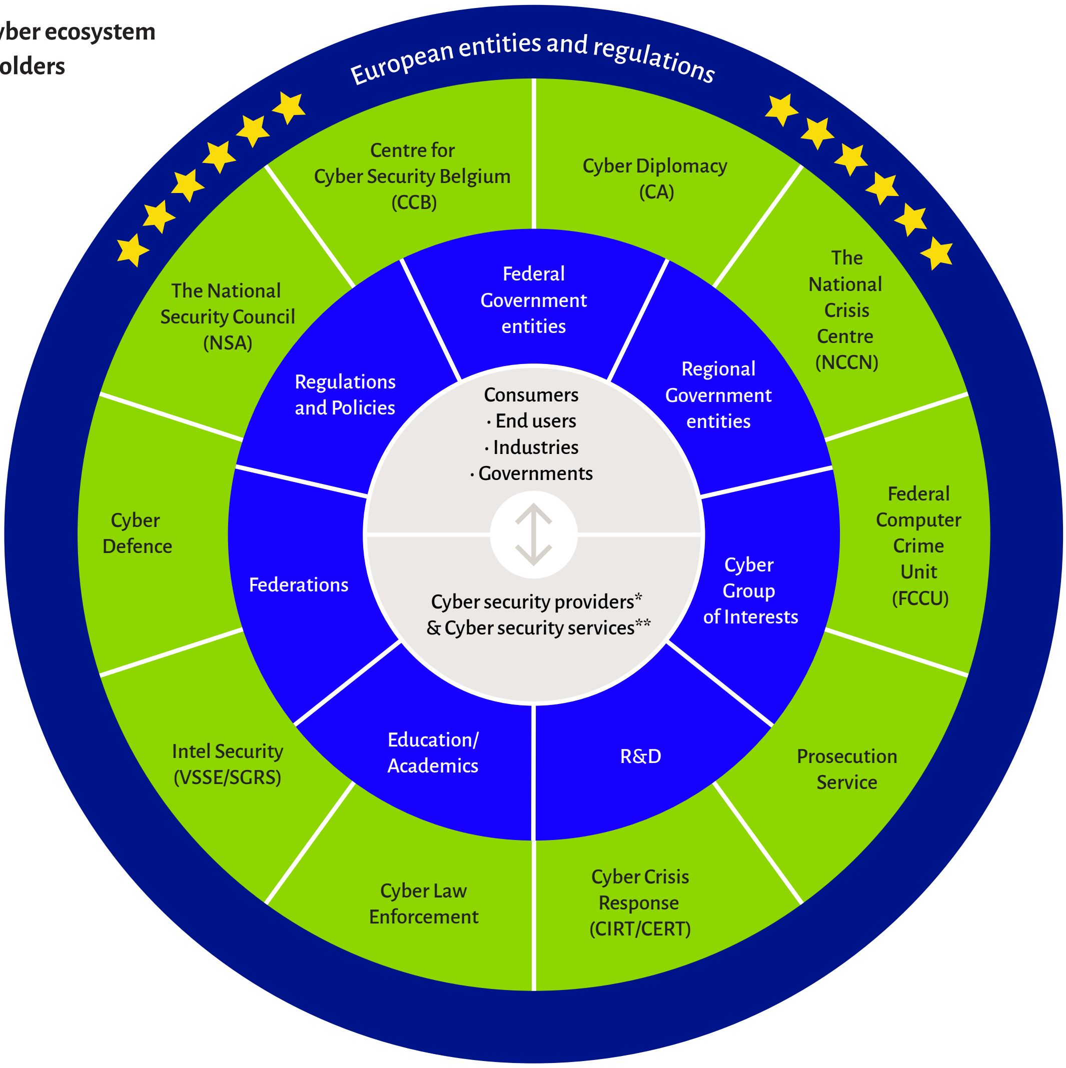
[13] https://cyberwal.be/

[14] https://www.digitalwallonia.be/fr/publications/keepitsecure/

[15] https://www.digitalwallonia.be/fr/publications/cyberexcellence-projet-recherche-cybersecurite/

[16] https://www.hrzkmo.fgov.be/; https://www.csipme.fgov.be/

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**

We categorised the Belgian cyber security providers and their offered services as illustrated below. For the classification of the particular services, we used the CyBOK taxonomy (cf. section 4). While the exact terminology is up for debate, the overview does highlight the diversity of the cyber market.

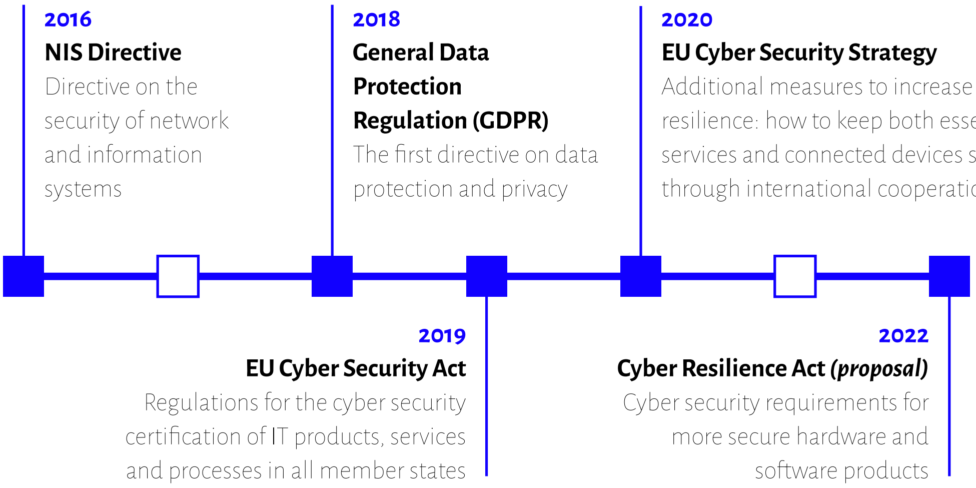
Cyber security providers and services

* Cyber security providers	
Generalists	Organisations that offer multiple cyber services
Consultants	Consultants regarding cyber security services
Integrators	Organisations that integrate products and components in industrial environments
Specialists (Pure players)	Organisations that focus on one specific cyber domain
Specialists (Niche players)	Organisations that focus on one specific sector or vertical (e.g., telecom, public services, insurance)
Training, education and certification entities	Organisations that mainly offer cyber education and certifications
Innovators	Start-ups and scale-ups that focus on an innovative product or service

** Cyber security services
Consulting and audits
Certification and accreditation
Security products (SW, HW, SECaaS, Insurance)
Security solutions (Integrations & Engineering)
Managed security services (Monitoring, Detection & Response)
Forensics and incident handling (CIRT, CERT)
Security training, education and certification
Research, development and innovation

3.2.3. Cyber security in the European Union

As illustrated by the (non-exhaustive) timeline below, the European Union has considered cyber security a top priority for quite a few years now.



2016
NIS Directive
Directive on the security of network and information systems

2018
General Data Protection Regulation (GDPR)
The first directive on data protection and privacy

2020
EU Cyber Security Strategy
Additional measures to increase cyber resilience: how to keep both essential services and connected devices safe through international cooperation

2019
EU Cyber Security Act
Regulations for the cyber security certification of IT products, services and processes in all member states

2022
Cyber Resilience Act *(proposal)*
Cyber security requirements for more secure hardware and software products

ENISA

The EU Cyber Security Act (2019) gave more resources to **ENISA**, the European Union Agency for Cyber Security[17]. The organisation is now permanently charged with the EU's cyber security policy and supporting all members with its implementation.

Investments and initiatives

With several investments, the European Union wants to make its **digital transition safe, secure and permanently protected** against threats.

For instance, cyber security is a fundamental part of the post-pandemic Recovery Plan for Europe, Horizon 2020, the Connecting Europe Facility (CEF), the Digital Europe Programme (DIGITAL), and InvestEU. In the near future, the Centre for Cyber Security Belgium (CCB) will serve as one of the Union's 27 National Coordination Centres (NCC), responsible for the supervision of cyber security investments, and as Belgium's National Cyber Security Certification Authority (NCCA).

Furthermore, the EU aims to **inform the public** and **nourish talent development**. Those ambitions have given rise to initiatives such as ENISA's Cyber Security Month campaign (every year in October), which Agoria supports for the Belgian market, and the annual European cyber security challenge, which encourages students to pursue cyber security careers. The European Commission has also developed the European Cyber Security Atlas, which visualises the Union's cyber security expertise.

> Tax shelter for the cyber security industry could be a catalyst for cyber resilience
>
> **Sebastien Deleersnyder**
> **Co-Founder and Chief Technology Officer, Toreon**
> **Cyber Security Personality of the Year 2022**

[17] https://www.enisa.europa.eu/

4/ THE CYBER SECURITY SECTOR REPORT

After a brief discussion of the study's objective and methodology, this chapter will review the most remarkable quantitative and qualitative research results. We will conclude the report by referencing the need for a new strategic growth framework, before summarising the overall outcome of the study, and sharing the sector's own outlook for 2025.

4.1. Objective

Until now, all available information on the Belgian cyber security landscape has turned out to be either incomplete or not fully up to date. Thorough **research was necessary** to adequately depict the current state of the cyber security sector in our country. This study endeavoured to unearth those essential numbers (quantitative component) and insights (qualitative component), and use them to specify recommendations for the sector's advancement.

As the first of its kind in Belgium, it lays the **foundation** for future in-depth investigations into the opportunities and challenges of the Belgian cyber security sector.

4.2. Methodology

In order to adequately represent the Belgian cyber security sector, we chose to incorporate a quantitative and a qualitative component in our research. We translated that dual approach into a survey (quantitative) and interviews with major stakeholders (qualitative).

4.2.1. Quantitative component: survey

The questionnaire comprised **nine quantitative questions**[18] 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 (cf. below), employees, open vacancies, and the diversity of its workforce in terms of age and gender.

Solvay Brussels School of Economics & Management (SBS-EM)

We asked four SBS-EM students to identify and map out all companies that offer cyber security solutions, services and products in Belgium. Their **resources** included, but were not limited to, LinkedIn, Google Jobs, Nomios, EDITx, 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 cyber security activities in our country.

After inspection and correction of all data by Agoria's **Study Department** and the **CMiB (Cyber Made in Belgium) Study Task Force** (a division of the Agoria Cyber Business Group), the final list comprised 441 companies. All of these were invited to fill out the survey.

Eventually, after verifying all submitted answers, the survey yielded **79 completed forms**. The results were divided by region and by company size.

As a whole, the sample corresponds to 17.9% of the Belgian cyber security population, 50.6% of the total cyber security sales figure, and 50.7% of the sector's total cyber security employment. This representation allowed us to confidently **extrapolate** their results to the entire cyber security population in Belgium.

[18] *https://online.agoria.be/cyber/cyber_overview.pdf*

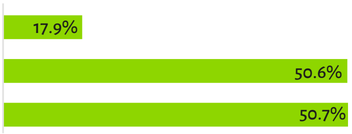
Sample size

79 respondents

of the Belgian cyber security companies

of the total cyber security sales figure

of the total cyber security employment

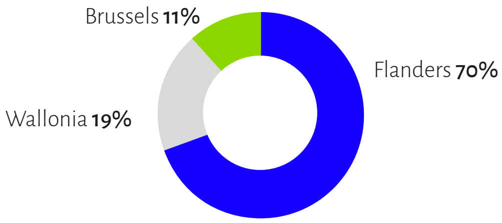


Division by region

Flanders: 55 respondents

Wallonia: 15 respondents

Brussels: 9 respondents



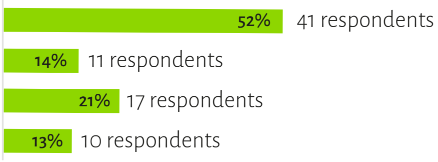
Division by company size

0-49 employees

50-99 employees

100-499 employees

500+ employees



4.2.2. Qualitative component: interviews

Between May and July 2022, we conducted around **30 interviews,** all of which consisted of **five open-ended questions**[19]. The interviewees represented important, high-level cyber security stakeholders in our country.

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 cyber security sector more competitive.

4.2.3. Taxonomy

Throughout the study, we used the open-source CyBOK taxonomy (the Cyber Security Body of Knowledge)[20] [21]. This classification **organises cyber security activities into five categories** by means of an accessible vocabulary. This classification organises cyber security activities into five categories by means of an accessible vocabulary, as summarised in the table below. For a more detailed infographic on each category, go to section 7.

Standards such as CyBOK and SFIA (Skills Framework for the Information Age)[22] are currently not used consistently in Belgium. Therefore, we applaud the initiative of the Flemish government to start using CyBOK for the classification of, among others, the course offerings of the **Flemish Cyber Security Policy Plan**.

CyBOK Taxonomy: benefits *

1. **By the community for the community**
2. **Developed by 115 world experts**
3. **International effort**
4. **21 knowledge areas**
5. **Free to use for everyone**

Courtesy of Helen Jones (CyBOK)

The CyBOK categories and their subdivisions

CyBOK categories

Systems security	Securing data treatment processes, e.g., internal data storage and user permissions
Software and platform security	Maintaining the resilience of software, computing platforms and applications, e.g., the integrity and privacy of data
Infrastructure security	Protecting networks and hardware against intrusion
Human, organisational and regulatory aspects	Preventing (un)intentional user mistakes through awareness and enforcement of in-house cyber security policies
Attacks and defences	Testing the internal cyber defence lines (ethical hacking) and patching up any vulnerable spots

[19] *https://online.agoria.be/cyber/cyber_overview.pdf*

[20] *https://cybok.org/*

[21] *Agoria already uses the CyBOK taxonomy for the Agoria Connect tool, which allows companies to get in touch with cyber security organisations and discover their services. For more information, please check agoriaconnect.be.*

[22] *https://sfia-online.org/en https://skillsbeam.io/*

4.3. State of the cyber security sector in Belgium

4.3.1. The numbers: quantitative results

Thanks to the results of the survey, we can now – for the very first time – give an accurate overview of the Belgian cyber security landscape.

The Belgian cyber security landscape (2021)

441 companies active in cyber security

€1.58 billion

Total sales figure in cyber security

€600 million

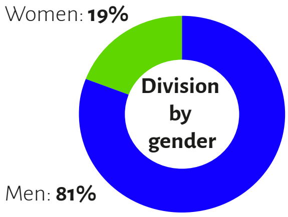
Total value added in cyber security

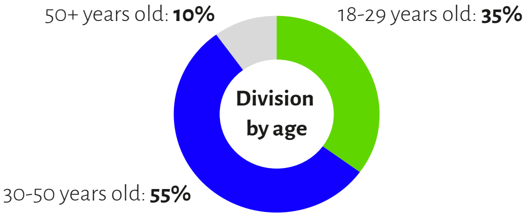
0.1%

of the Belgian GDP

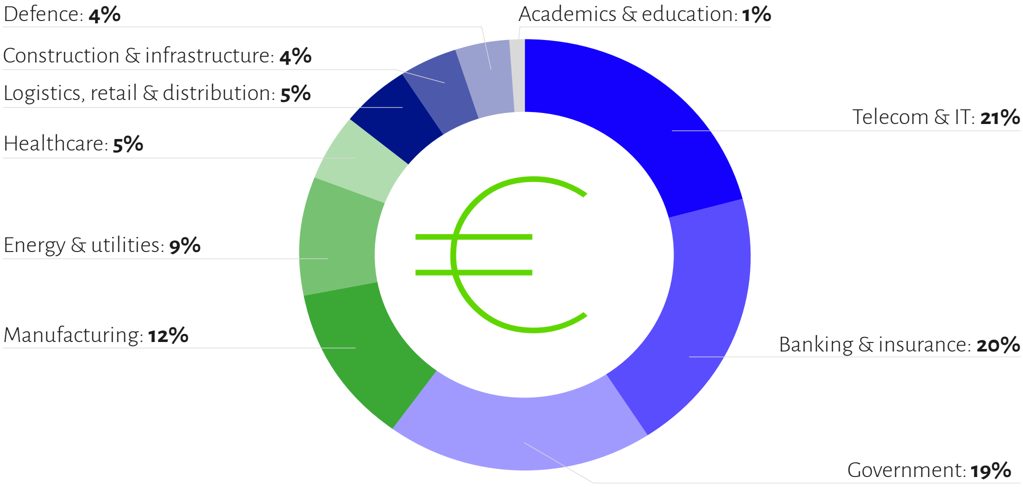
6,405 FTEs

Total employment in cyber security





Most important sectors where cyber security sales figures are realised



1,205

Total number of vacancies in the cyber security sector

16%

Vacancy rate cyber security sector which is much higher than:
Vacancy rate **Belgian IT sector: 9.1%**
Vacancy rate **Belgian economy: 5%**

16.4%

Export percentage

42%

doesn't export at all

Companies active in cyber security by region

	Cyber security companies	Cyber security sales figure	Cyber security employees (in FTE)
Brussels	102 (23%)	€0.18 billion	1,740
Flanders	233 (53%)	€1.33 billion	4,210
Wallonia	106 (24%)	€0.07 billion	455
BELGIUM	**441**	**€1.58 billion**	**6,405**

A limited workforce

There are 1,205 vacancies in the cyber security sector – a vacancy rate of 16%. The need for cyber skills is not limited to that industry, though. Other industries, such as the banking sector, defence, and the public authorities, show **a significant demand for cyber security professionals** as well. All in all, we estimate that the Belgian labour market currently offers 4,000 open cyber security vacancies.

Bridging that gap will be challenging. While there are job opportunities aplenty, there is simply **not enough talent available**. Moreover, qualified and talented employees might not be drawn to the sector due to lack of awareness, a language barrier or unrecognised international degrees.

> The need for gender balance is evident in all sectors. In cyber security, however, that need is an urgent one, due to the enormous competence gap created by the digital transformation

Anett Mádi-Nátor
President, Women4Cyber Foundation

Limited exportation and a focused market

On average, export trade accounts for **16.4%** of the total sales figure across Belgian cyber security companies. No fewer than 42% of cyber security organisations in our country have no engagement in export trade at all.

The majority of **cyber security demand** in Belgium is claimed by just four economic sectors. Together, telecom and IT (22%), the banking and insurance sector (20%), the government (19%) and manufacturers (12%) make up 73% of the sector's customers. Other divisions show significantly lower cyber security needs.

> Addressing the cyber security challenge is one of the main prerequisites for the successful adoption of 5G use cases and the further digitalization and competitiveness of our industries

Olivier Bruyndonckx
Vice President Customer Success Cloud and Network Services, Nokia

Strong emphasis on one cyber security domain

When aligned with the CyBOK taxonomy, the sector's current services mostly cover **infrastructure security** (37%). The other four pillars (systems security, software and platform security, attacks and defences, and human, organisational and regulatory aspects) are more equally divided, representing between 13% and 17% of the Belgian cyber security sales figure.

4.3.2. The insights: qualitative results

In the interviews, several stakeholders shared similar insights into the most prominent opportunities and challenges of the cyber security sector.

Fragmentation and misconceptions

Multiple interviewees remarked on the **lack of cooperation** between the different layers of the Belgian cyber ecosystem. Both the federal government and its regional counterparts assume specific cyber security responsibilities. As a result, the coordination of cyber security policies, research projects and initiatives is often fragmented.

Moreover, the cyber security sector's reputation has been harmed by misconceptions and **a general lack of awareness**, especially among SMEs. After all, cyber security measures are often considered a costly and complicated issue. Board members and managers rarely realise that it is an investment in business resilience, integrity and customer trust – and a crucial protection against potentially disastrous intrusions.

> Many small and medium-sized businesses view cyber security as a cost, not a benefit
>
> **Kurt Callewaert**
> **Valorisation Manager Digital Transformation, Howest**

Cyber poverty in SMEs

Numerous stakeholders mentioned the alarming cyber poverty in the infrastructure of our country's SMEs. Fuelled by the abovementioned misconceptions, many companies reserve just a minimal spot for cyber security in their overall risk management. Some don't even include it at all. With cyberattacks becoming increasingly effective, this neglect poses an **immense danger** to our economy and the trustworthiness of the digital marketplace.

> Every day,
> we see that most Belgian SMEs
> are still below the cyber poverty line
>
> **David Vanderoost**
> **Chief Executive Officer, Approach Belgium**

The Cyber Security Poverty Line

The Cyber Security Poverty Line (CPL), also known as the security poverty line, is used to divide organisations into two categories: those that can achieve a mature security position, and those that fail to do so – often due to insufficient financial or human resources. The concept was originally coined by Wendy Nather, Head of Advisory CISOs at Cisco, in 2011.

Cyber security education for everyone

As mentioned earlier, the Belgian labour market currently offers a total of ca. **4,000 open cyber security vacancies**. To meet that demand, more investments in cyber security education are needed.

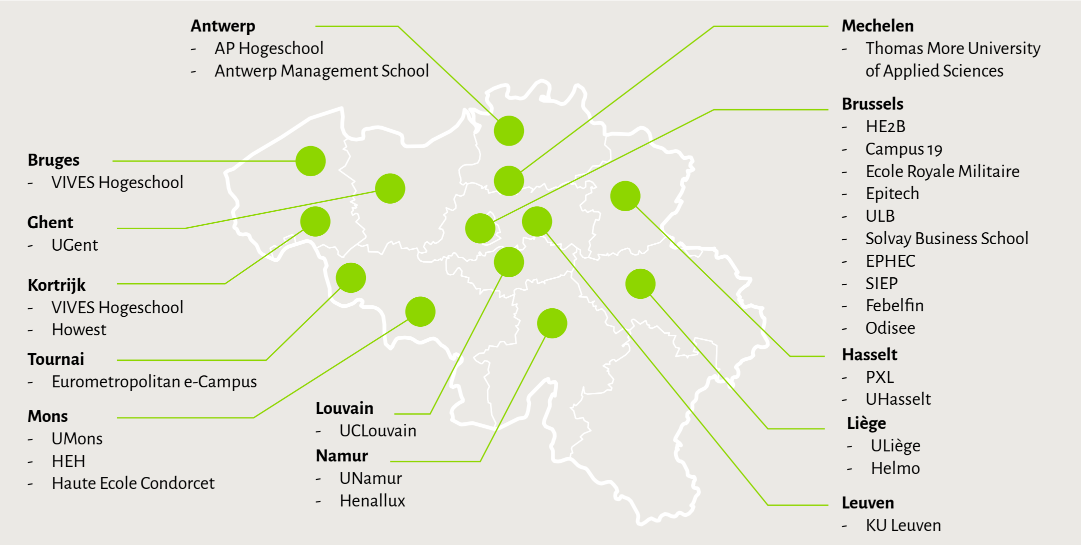
However, certain cyber security skills are more in demand than others. In order to gain more insights, we used the AI-based TechWolf tool to analyse current cyber security job vacancies and indicate the **most sought-after cyber security skills** in Belgium, the European Union and around the world.

The most sought-after skills in cyber security job vacancies[24]

Belgium	EU	Global
1. Network Security	1. Cyber Attack	1. Information Security
2. Information Security	2. Information Security	2. Cyber Attack
3. Network Architecture	3. Security Engineering	3. CISSP
4. Network Monitoring	4. Security Threats	4. Network Security
5. Problem Management	5. SIEM	5. Security Engineering
6. TCP/IP	6. Vulnerability Management	6. Security Controls
7. Incident Response	7. CISSP	7. Incident Response
8. VPN	8. Incident Response	8. Vulnerability Scan
9. Network Security Tools	9. Network Security	9. Computer Science
10. IPS	10. Vulnerability Scan	10. Web Security

How can aspiring cyber security professionals in Belgium acquire those skills? The map below visualises their options. Recent additions include KU Leuven's Master of Cyber Security, Howest's Advanced Cyber Security Postgraduate Programme, and the Haute Ecole Condorcet's Master in Networks and Computer Systems Security.

Overview: main schools that offer cyber courses (excl. online programmes)



Antwerp
- AP Hogeschool
- Antwerp Management School

Bruges
- VIVES Hogeschool

Ghent
- UGent

Kortrijk
- VIVES Hogeschool
- Howest

Tournai
- Eurometropolitan e-Campus

Mons
- UMons
- HEH
- Haute Ecole Condorcet

Louvain
- UCLouvain

Namur
- UNamur
- Henallux

Mechelen
- Thomas More University of Applied Sciences

Brussels
- HE2B
- Campus 19
- Ecole Royale Militaire
- Epitech
- ULB
- Solvay Business School
- EPHEC
- SIEP
- Febelfin
- Odisee

Hasselt
- PXL
- UHasselt

Liège
- ULiège
- Helmo

Leuven
- KU Leuven

Source: Data Gathering by Solvay & Agoria (2022)

> Offering cyber security knowledge at the earliest stages of education is a must to strengthen the cyber skills profiles on the Belgian market
>
> **Michael Boeckx**
> **Chief Security Officer, NRB Group**

[24] https://techwolf.ai/

While this non-exhaustive illustration shows that cyber security is fundamentally integrated into our **academic environment**, the interviewees agreed that additional training programmes are necessary to keep cyber security professionals' expertise up to date. Continuous knowledge sharing is essential to provide them with the right tools to protect our critical assets and digital privacy in an increasingly connected world.

That is not just true for higher education. Several stakeholders confirmed that **organisations and governments** should equally expand their (online) course libraries to keep their employees' and security risk managers' know-how up to date. They must comprehend and reinforce their cyber hygiene to comply with the increasingly stringent EU regulations.

Lastly, awareness should also spread to all **citizens**, even those who are not active in the cyber security sector. Every citizen should understand digital risks and how these relate to their online responsibilities. Even the bare minimum of cyber knowledge could inform them how to responsibly use and secure their own digital space, and how to safely buy goods and services online.

> As an academic player, we have a social responsibility to contribute to any cyber resilience initiatives
>
> **Fabian Restiaux**
> **Head of the Applied Sciences and Technology Department, Hénallux**

Therefore, the interviewees proposed to **incorporate notions of cyber security** in different segments of our educational system, from primary schools to secondary schools right through to our universities and beyond. Closing cyber security knowledge gaps should be a top priority for the industry, governments and educational institutes.

4.3.3. A new strategic socio-economic framework

All interviewees agree that Belgium, with its multilingual and international character, is poised to become a cyber security hotspot in Europe. However, achieving such **a strong cyber security culture** calls for a new strategic socio-economic framework.

We need to strengthen our infrastructures, perfect and share our knowledge, and increase our scaling capacity. That will allow us to keep up with technological developments and formulate the right responses to emerging threats.

> Belgium has all it takes to become a Cyber Security and Data Protection Valley
>
> **David Dab**
> **National Technology Officer, Microsoft**

Boosting awareness and talent was a recurring theme in the qualitative interviews, but **other solutions** were voiced as well. In order to grow the cyber security sector, we don't just need to recognise its strategic importance and educate our society. Several interviewees stated that we have to stimulate the internationalisation of our cyber security organisations for exponential growth. Others expressed the need for more coordination between regional and federal initiatives, and a proper strategic roadmap for the sector as a whole.

If we fail to do so, our cyber security position will remain **vulnerable and highly dependent** on other countries, such as the United States and China. Also, it is hard to ignore that cyber threats are progressively driven by geopolitical motives, and not just financial gain. Some interviewees feared that, if we are poorly prepared, large-scale cyberattacks could wreak havoc on our essential services, such as our banking system or electricity distribution. The public could lose faith in the opportunities and benefits of the digital environment and its applications. The consequences for our economy would be absolutely disastrous. After all, the CCB is quite clear in its predictions regarding the biggest threats for our population and economy:

Belgium's biggest threats in the future[25]

Cyber crime	Foreign military and intelligence services	Hacktivism	Cyber terrorism
Abusing computers and networks (and the data they store) for financial gain	Using cyber security knowledge to economically damage other countries, and undermine their stability and overall defences	Online breaking and entering to promote political, social or religious ideologies	Performing violent cyber activities to cause fear and intimidation

> As clearly stated by NATO and the EU, the current geopolitical context forces us more than ever to dramatically strengthen the cyber resilience of our society

Major General Michel Van Strythem
Commander Belgian Cyber Command, Ministry of Defence

© Pierre-Yves Thienpont

4.4. Research results: summary

This study combined quantitative and qualitative research to paint **a truthful picture of the cyber security sector in Belgium**.

Firstly, 79 **survey respondents** reported numbers that implied many opportunities for growth. An influx of new talent will enable the sector to decrease its vacancy rate, boost its export percentage and diversify its products and services.

Secondly, **interviews with major cyber security stakeholders** indicated a strong need for awareness and training. More efforts are needed to inform both companies and citizens about the strategic importance of cyber security. A new strategic socio-economic framework will allow us to reinforce our defences, eliminate cyber poverty, and to better prepare cyber security professionals for future threats.

[25] *https://ccb.belgium.be/sites/default/files/CCB_Strategie%20 2.0_UK_WEB.pdf*

All in all, Belgium needs more tools and support to build on its steady starting position and establish a stronger and more scalable cyber security culture.

> Procurement laws for public contracts should be adapted, so cyber security SMEs can compete with giant service providers and create the necessary local ecosystem
>
> **Georges Ataya**
> **Chief Executive Officer, Ataya & Partners**

4.5. Outlook for 2025

According to the survey results, the sector's hopes and dreams for the future burst with optimism. When comparing their prospects with 2021, Belgian cyber security companies expect that their total cyber security sales figure will be 2.15 times higher in 2025; **a Compound Annual Growth Rate (CAGR) of 21.2%**. Fortune Business Insights has predicted a global CAGR of 13.4% by 2029[26].

> Belgium has all the assets to become a European frontrunner, but only if we accelerate talent development and strengthen our competitiveness
>
> **Filip Verstockt**
> **President, CMiB**
> **General Manager, Orange Cyberdefense Belgium**

That optimism fits in perfectly with the Cyber Security Strategy's prime objective to make Belgium **one of Europe's least vulnerable countries** in the cyber domain by 2025.

Belgium's six strategic objectives for 2021-2025[27]

- Strengthen our digital environment and increase overall trust in its safety
- Provide computer users and administrators with the right knowledge
- Protect the country's Organisations of Vital Interest from all cyber threats
- Respond swiftly and efficiently to cyber threats
- Improve public, private and academic collaborations
- Show commitment on an international level

[26] https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165

[27] https://ccb.belgium.be/sites/default/files/CCB_Strategie%20 2.0_UK_WEB.pdf

5/ RECOMMENDATIONS

Based on the quantitative and qualitative results of our research, we have formulated **five recommendations**, clustered around three themes. When properly executed, they will help the Belgian cyber security sector to meet the ever-changing market demands and regulations, to scale in a supportive environment, and to keep citizens and businesses safe in an increasingly connected digital atmosphere. All these recommendations are in line with the Belgian Cyber Security Strategy 2.0 and with the cyber security objectives set out in the National Pact for Strategic Investments (2018)[28].

Theme 1: Development of talent and education curricula

Recommendation 1

Agoria recommends to increase our country's overall capacity for higher cyber education, integrate cyber security into every level of our educational system, promote cyber careers, attract more women to the sector, and add cyber jobs to the list of 'bottleneck professions', as specified by VDAB, Actiris, Le Forem, our regional employment agencies, and competence centres.

In the fight against cybercrime, **competent cyber security specialists** are our most powerful weapons. Therefore, we need to attract new talent and nurture the skills of all current cyber security employees. New recruitment methods and improved remuneration will be necessary to make the sector stand out in the war for talent.

Sharing knowledge is a fundamental part of that process. We need to provide schools with information materials to encourage young people to pursue a STEM career (Science, Technology, Engineering and Mathematics). With further investments in R&D, educational institutions can spread knowledge, conduct high-level research[29], and provide the most relevant courses. Both the public and private sector should offer **high-quality training** to their security managers, enabling them to detect and handle threats with up-to-date expertise.

Other examples include Massive Open Online Courses (MOOC) and a national strategy to grow the cyber security workforce through tailor-made training, in tune with vital trends and developments in the field.

Illustration: cyber security heatmap

In the United States, CyberSeek has developed a heatmap that visualises cyber security supply and demand for all 50 states, including all the sector's job openings. A similar tool for our country could help us gain more insights into the available job opportunities, and points of weak or strong representation in the landscape.

Theme 2: Awareness

Recommendation 2

Agoria recommends evaluating whether its planned 'Roadshow for Leaders' awareness programme can be expanded into regional and national campaigns, targeted at management levels in the public and private sector, and the different governments. Those campaigns would aim to educate the audience by means of an accessible vocabulary, incite them to take action and increase their business' cyber resilience, and prepare them for upcoming EU cyber regulations.

[28] *https://www.npsi-pnis.be/nl/cybersecurity*

[29] *https://cybersecurity-research.be/*

Boards and executive committees are increasingly aware of cyber risks. However, they mostly talk about the potential threats, instead of the business opportunities. That is why Agoria has launched the 'Roadshow for Leaders' programme in Belgium

Vincent Defrenne
Vice President, CMiB, and Director Cyber Strategy, NVISO

Recommendation 3

Agoria recommends that sector federations and governments become inspired by Agoria's own commitment "to secure that 95% of all their member companies have a cyber security plan in place by 2025" [30] and will set a similar objective. This recommendation is officially supported by The Federation of Enterprises in Belgium (VBO/FEB).

Internet users have **a shared responsibility**: making sure that the Web remains a safe place to exchange data. Therefore, everyone needs to know how to treat personal and business data responsibly, wherever they are, and how to efficiently address security problems.

Let's build a trustworthy Internet, together

Miguel De Bruycker
Managing Director, Centre for Cyber Security Belgium (CCB)

Awareness campaigns without jargon or buzzwords are required to **educate the public, business leaders and governments** about the impact of cyber hygiene on business resilience, customer trust, and their overall safety in the digital landscape. Such initiatives are needed to bridge the current knowledge gaps and feed better-informed preventive measures against cyber threats, which will reinforce our digital resilience even further.

Meanwhile, the CCB will keep communicating with governments, media and relevant security agencies about emerging threats and how to respond to them. Its **Online Cyber Security Reference Guide** will continue to help organisations evaluate and/or implement a proper cyber security plan.

Theme 3: Growth roadmap for the sector

Recommendation 4

Agoria recommends inviting the regions and other involved stakeholders, as part of their Industrial Policy, to consider increasing support for cyber start-ups and scale-ups. That would enable those companies to boost the development of scalable innovative cyber security solutions, and to execute or strengthen projects such as the Cyber Green House and the 'CyberWal by Digital Wallonia' programme.

[30] *https://technologyforabetterworld.be/en*

Belgium needs to strengthen its digital autonomy. An advanced cyber capacity, more secure infrastructures, and state-of-the-art protection techniques will **limit our vulnerabilities and dependence** on other countries. This requires commitment and resources from all stakeholders involved.

> It is our moral obligation to increase the cyber resilience of our society. Security incidents at companies below the Cyber Poverty Line can have far-reaching consequences for the entire ecosystem
>
> **Wouter Vandenbussche**
> **Solution Lead Security & Service Intelligence, Proximus**

Without such a commitment, we are unable to **fortify our digital defence lines**. Cyber security start-ups and scale-ups need accelerated investments to rapidly detect and anticipate threats, to keep up with the evolutions in their field (and inevitable new threats), and to focus on their own scalable, innovative solutions.

> During our most recent strategic review, we confirmed and reinforced the importance of cyber security. Therefore, the Federal Holding and Investment Company will continue to invest both directly and indirectly in the Belgian cyber ecosystem
>
> **Leon Cappaert**
> **Investment Manager, Federal Holding and Investment Company (SFPI-FPIM)**

That level of support will show **trust** in the safety of digital products and applications**, boost economic growth**, and make **customers feel protected** during their online movements and actions.

Investment example: the Cyber Green House

As highlighted in the Belgian Cyber Security Strategy 2.0, the Cyber Green House will provide a modern innovation centre, where cyber security professionals will be able to test new solutions and business models in a controlled environment. It is one of many initiatives that aim to give the cyber security sector a well-deserved, necessary boost.

Investment example: the Cyber Testing & Certification Lab

The Ministry of Defence, and the Royal Military Academy in particular, are building the Cyber Testing & Certification Lab for the evaluation of cyber security products and services in the context of scientific and technological research. In the long run, the lab will support companies in their ambition to market certified cyber security products.

Recommendation 5

Agoria recommends promoting and boosting the export trade of our cyber solutions and products through a close collaboration with Flanders Investment and Trade (FIT), the Walloon Export and Foreign Investment Agency (AWEX), the Brussels Agency for Business Support (hub.brussels), and other key stakeholders. In that perspective, Agoria also recommends attracting and facilitating foreign investments in Belgian cyber security skills and services.

Cyber threats often affect multiple countries at once. **International cooperation** is a must to guarantee both a secure cyber environment and swift, adequate responses to large-scale digital invasions. Belgium has vowed to support European cyber security initiatives, but we need to assume a leading role in that cross-border collaboration.

With a stronger digital autonomy and increased investments, Belgium can become a blooming habitat for ambitious cyber organisations and talented security specialists. A **cyber security hotspot** in the heart of Europe, where cutting-edge cyber security innovations can take root and blossom.

After all, our country accommodates many **international headquarters**. Belgium will need to step up its cyber security game to give them the first-class protection they expect and deserve.

> Europe has already lost a leading position regarding smartphones and cloud storage. We don't want to lose control of our cyber security as well. It would only make us even more vulnerable

Bart Preneel
Professor of Cyber Security, Head of Computer Security and Industrial Cryptography (COSIC), KU Leuven
Co-Lead of Research, Cyber Security Initiative Flanders

> When perceived as trustworthy, cyber security can only benefit the socio-economic fabric

Axel Legay
Professor of Cyber Security, UCLouvain
Co-Head, CyberWal by Digital Wallonia

6/ ACKNOWLEDGEMENTS

This report would never have seen the light of day without all the **invaluable guidance** we were so fortunate to receive.

First of all, we would like to extend our deepest gratitude to our **executive, financial and CMiB sponsors** for making this research possible. Thanks to their support, we were able to lay the foundation for future cyber security growth and success.

We are also extremely grateful to all the companies who agreed to participate in the in-depth **interviews**, so we could thoroughly identify the core opportunities and threats in this ever-evolving landscape. Additionally, we couldn't have achieved our goals without the organisations who filled in our **survey**. Their input and insights helped us paint a truthful picture of the cyber security sector in Belgium.

Last, but not least, we want to express our thanks to the **Solvay Brussels School of Economics & Management**, for mapping out and gathering the data at the very heart of this investigation.

Contributors in alphabetical order

Executive sponsors

- Agoria, Belgian Ministry of Defence, Centre for Cyber Security Belgium (CCB)

Financial sponsors

- Approach, Cegeka, Centre for Cyber Security Belgium (CCB), Nokia, Network Research Belgium (NRB) , NVISO, Orange Cyberdefense, RHEA Group, Toreon

CMiB sponsors

- The CMiB Study Task Force: Michel Van Strythem, David Vanderoost, Matteo Merialdo, Bram Couwberghs, Clivio Tappi, Caroline Breure, Thierry Henrard, Bernard Van Hecke, Julie Vandenborne

Interviewees

- Agence du Numérique (ADN), Approach, Ataya & Partners, Atos, KU Leuven, Belgian Ministry of Defence, Beltug, Cabinet of the Prime Minister of Belgium, FOD Beleid en Ondersteuning / SPF Stratégie et Appui (BOSA), Cegeka, Centre for Cyber Security Belgium (CCB), Cyber Security Coalition (CSC), Cyberwall, DistriNet, European Cyber Security Organisation (ECSO), Egmont Institute, Federal Holding and Investment Company (SFPI-FPIM), Hénallux, Howest, Information Systems Audit and Control Association (ISACA), International Association of Privacy Professionals (IAPP), Microsoft, Nokia, Network Research Belgium (NRB), NVISO, Orange Cyberdefense Belgium, Pamica NV, Proximus, RHEA Group, Telenet, Toreon, Vlaams Agentschap Innoveren en Ondernemen (VLAIO)

Surveyed companies

- AgiNtech, AKKA Belgium, Apogado, Approach Belgium, Arrow, Ataya & Partners, Atos Belgium, AXS Guard, Axxes, B12 Consulting, Bureau Veritas Certification Belgium, C2D System House, Ceeyu, Cheops Technology, Cisco Systems Belgium, Cognizant Technology Solutions Belgium, Colt Technology Services, Computacenter, Copaco Belgium, Cyber Security Management, Data Protection Institute, Davinsi Labs, Dilaco, Direct, DXC Technology Belgium, e-BO Enterprises, Ernst & Young, Exclusive Networks, G DATA CyberDefense AG Belgium, Haviland, HeadMind Partners Belgium, i-Force, INNOCOM, Intigriti, J IT Smart Your Network & Security, Jimber, MCG, Metastore, Microsoft, Minotaur, MT-C, Neddine Solutions, Netcure, Netropolix Software, Nitroxis, Nokia Bell, Network Research Belgium (NRB), NSI IT Software & Services, NVISO Belgium, OLINKO, OneSpan, OneWelcome, Orange Cyberdefense Belgium, Privacy Praxis, Procsima-Group, Prodata Systems, Proximus, Resilient Business, RHEA Group, Rittal, Saphico, Savaco, Sertalink, Simac, Sitac Europe, Skyforce, SPIE Belgium, Spotit, ST Engineering iDirect (Europe), Sweepatic, SWITCHPOINT, Telenet, Thales Belgium, Tigron, Tobania, Toreon, TrueGEN, Trustteam, Vanmarcke

Contributors at Agoria

- Study Department, Marketing & Communications, Senior Management & Board of Directors, Anje Van Vlierberghe, Patrick Coomans

External support

- Copywriting support: com&co
- Survey support: Afsprakenmaker
- CyBOK support: Helen Jones, Project Manager, Cyber Security Body of Knowledge, University of Bristol

Solvay Brussels School of Economics & Management

Leadership

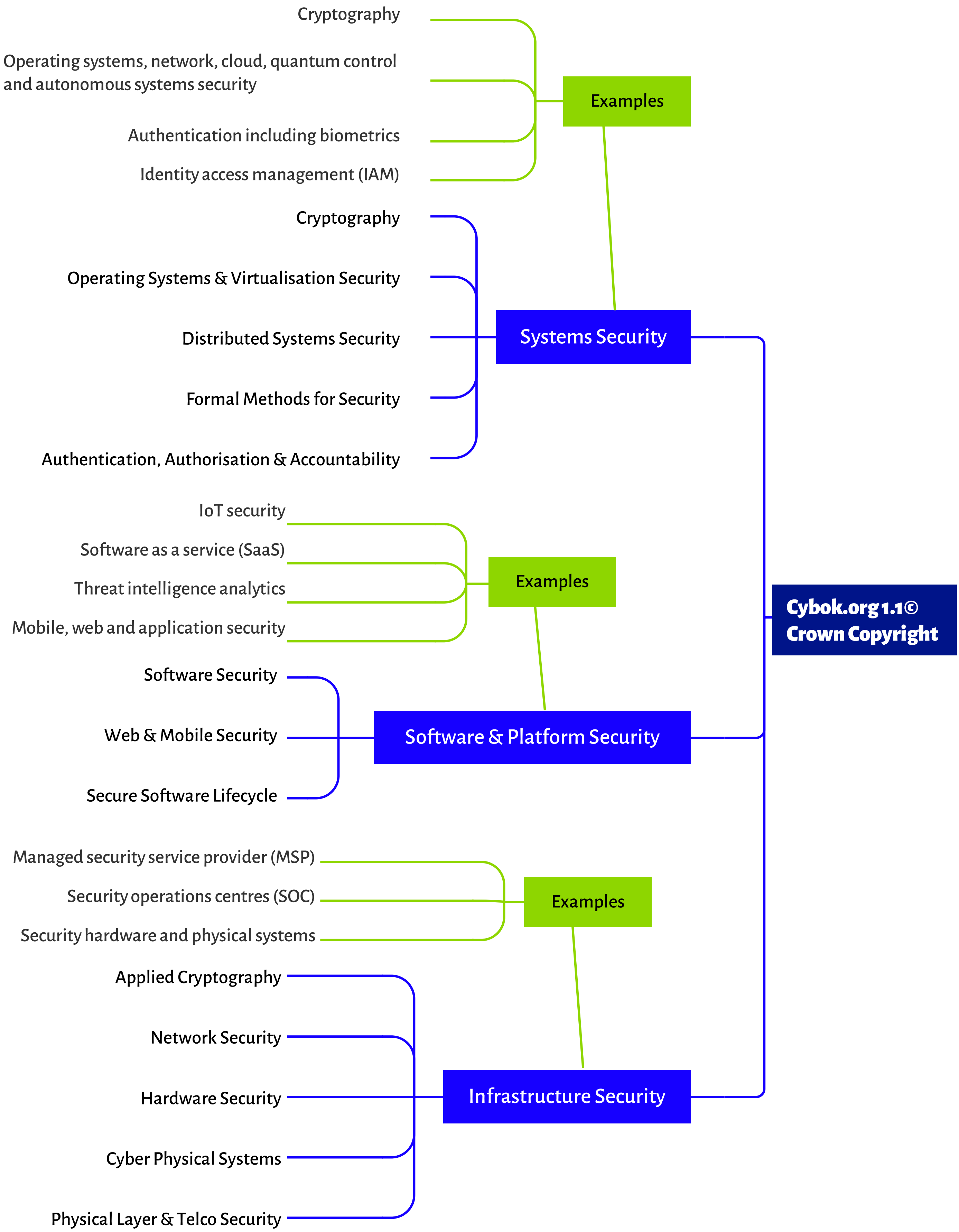
- Nicolas Ameye, Georges Ataya

Students

- Maxence Beyssier, Valentina Escobar Ospina, Laieq Hidari, Sergio Storino Chirolla

7/ ANNEX

This extensive infographic provides more information about the different CyBOK categories, as introduced in section 4. Source: https://online.agoria.be/cyber/cyber_CybokEx.pdf



Cybok.org 1.1© Crown Copyright

Systems Security

- Cryptography
- Operating Systems & Virtualisation Security
- Distributed Systems Security
- Formal Methods for Security
- Authentication, Authorisation & Accountability

Examples

- Cryptography
- Operating systems, network, cloud, quantum control and autonomous systems security
- Authentication including biometrics
- Identity access management (IAM)

Software & Platform Security

- Software Security
- Web & Mobile Security
- Secure Software Lifecycle

Examples

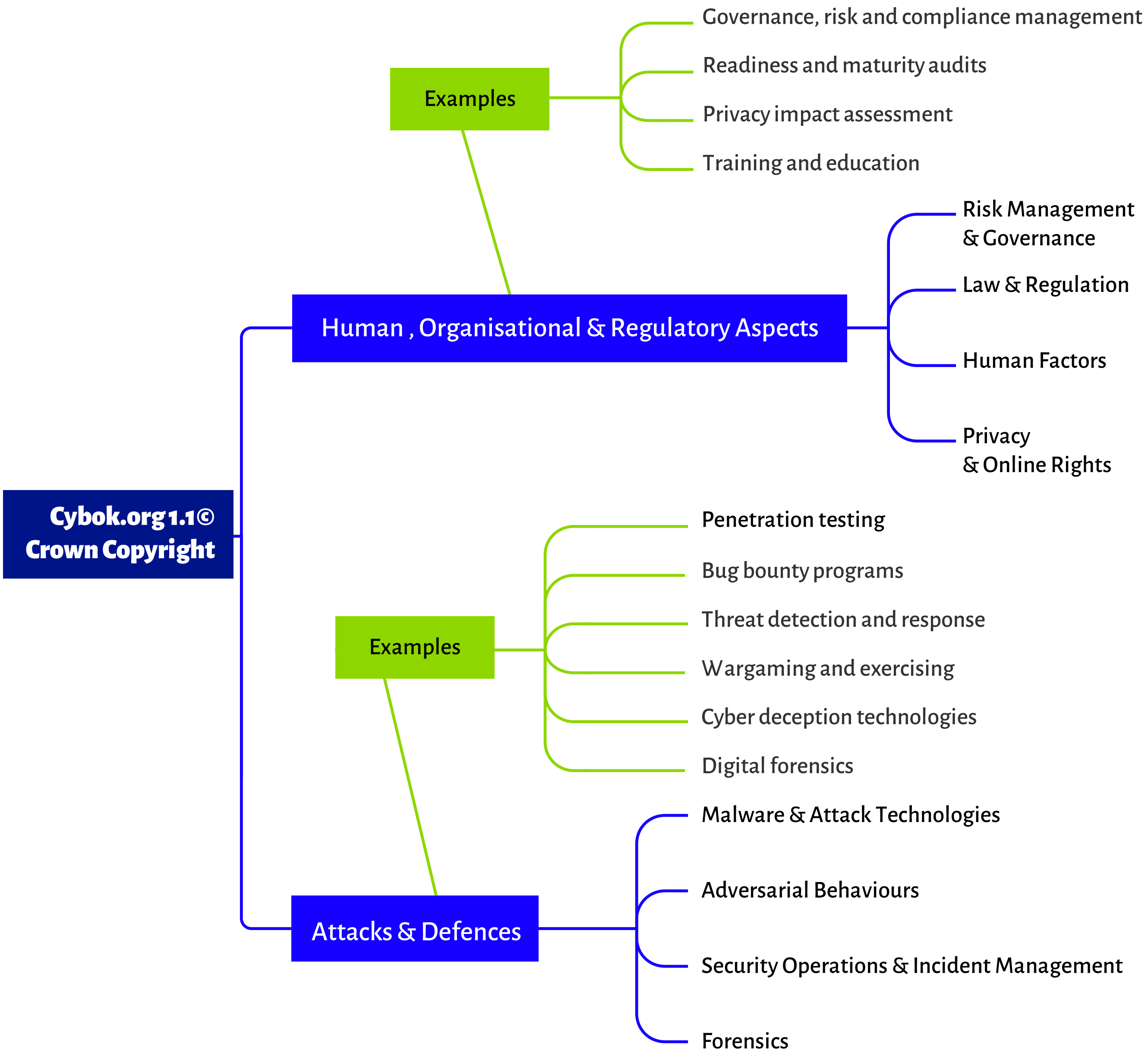
- IoT security
- Software as a service (SaaS)
- Threat intelligence analytics
- Mobile, web and application security

Infrastructure Security

- Applied Cryptography
- Network Security
- Hardware Security
- Cyber Physical Systems
- Physical Layer & Telco Security

Examples

- Managed security service provider (MSP)
- Security operations centres (SOC)
- Security hardware and physical systems



Cybok.org 1.1© Crown Copyright

Human , Organisational & Regulatory Aspects

Examples

Governance, risk and compliance management

Readiness and maturity audits

Privacy impact assessment

Training and education

Risk Management & Governance

Law & Regulation

Human Factors

Privacy & Online Rights

Attacks & Defences

Examples

Penetration testing

Bug bounty programs

Threat detection and response

Wargaming and exercising

Cyber deception technologies

Digital forensics

Malware & Attack Technologies

Adversarial Behaviours

Security Operations & Incident Management

Forensics

.AGORIA

DF 02/06
285
072
002
DX 01/87
710
YU 07/26

8/ REFERENCES

Please find a list of all consulted information sources below. Bear in mind that some of them are only available in Dutch, French or English.

https://ccb.belgium.be/en/ncc

https://ccb.belgium.be/en/news/cyber-strategy-20-make-belgium-one-least-vulnerable-countries-europe

https://ccb.belgium.be/sites/default/files/CCB_Strategie 2.0_UK_WEB.pdf

https://cybersecurity-bites.be/

https://cybersecurity-research.be/

https://cybersecurity.proximus.be/survey2021/research-report-cybersecurity

https://cyberwal.be/

https://cybok.org/

https://digital-strategy.ec.europa.eu/en/news/new-eu-cybersecurity-rules-ensure-more-secure-hardware-and-software-products

https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies

https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391

https://online.agoria.be/cyber/cyber_overview.pdf

https://technologyforabetterworld.be/en

https://techwolf.ai/

https://www.agoria.be/fr/etude-Cyber-securite-dans-industrie-manufacturiere

https://www.agoria.be/nl/studie-Cybersecurity-in-de-maakindustrie

https://www.agoriaconnect.be/

https://www.austcyber.com/resources/sector-competitiveness-plan

https://www.beltug.be/impact-item/les-priorites-des-cio-belges-et-de-leurs-equipes-la-gestion-des-donnees-et-les-defis-lies-a-larchitecture-informatique-et-a-la-cybersecurite-sont-des-priorites-absolues-pour-les-decideurs-tic/

https://www.condorcet.be/securite-des-reseaux-et-systemes-informatiques/securite-des-reseaux-et-systemes-informatiques.html

https://www.csipme.fgov.be/

https://www.cyberseek.org/heatmap.html

https://www.dekamer.be/FLWB/PDF/55/2627/55K2627001.pdf

https://www.digitaletoekomst.be/nl/cyber-security/aan-de-slag/dit-betekent-het-vlaams-beleidsplan-cybersecurity-voor-jouw-bedrijf

https://www.digitalwallonia.be/fr/publications/cyberexcellence-projet-recherche-cybersecurite/

https://www.digitalwallonia.be/fr/publications/keepitsecure/

https://www.enisa.europa.eu/

https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework

https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165

https://www.gartner.com/en/doc/757928-predicts-2022-cybersecurity-leaders-are-losing-control-in-a-distributed-ecosystem https://www.hrzkmo.fgov.be/

https://www.investopedia.com/terms/v/valueadded.asp

https://www.mastercard.com/news/europe/en/newsroom/press-releases/en/2022/january/mastercard-reveals-record-levels-of-cybercrime-in-belgium-during-the-pandemic/

https://www.mil.be/nl/cyber/

https://www.npsi-pnis.be/nl/cybersecurity

https://www.vlaio.be/nl/begeleiding-advies/digitalisering/cybersecurity/vlaams-beleidsplan-cybersecurity

https://www.weforum.org/reports/global-risks-report-2022/

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.

.AGORIA

CENTRE FOR
CYBER SECURITY
BELGIUM

APPROACH

cegeka
IN CLOSE COOPERATION

NOKIA

THE NRB GROUP

nviso

Orange
Cyberdefense

RHEA
GROUP

TOREON

About Agoria

Technology federation Agoria unites more than 2,100 Belgian businesses, 70% of which are SMEs. Together, they represent approximately 324,000 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, is the voice of the Belgian cyber security industry.

Find out more at agoria.be

About the Centre for Cyber Security Belgium (CCB)

The CCB, established by a Royal Decree in 2014, is the national authority for cyber security in Belgium. The organisation supervises, coordinates and monitors the application of the Belgian cyber security strategy 2.0. It wants to optimise information exchange and to enable companies, the government, providers of essential services and the population to protect themselves appropriately. The CCB operates under the authority of the Belgian Prime Minister.

Find out more at ccb.belgium.be

About the Ministry of Defence

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

The Cyber Capacity will collaborate closely with national and international partners, such as NATO, the Centre for Cyber Security Belgium (CCB), the State Security Service (VSSE) and the Federal Police.

Find out more at www.mil.be

Eric Van Cangh
Senior Business Group Leader Digital
+32 492 23 24 34
Eric.VanCangh@agoria.be

Yves Schellekens
Senior Cyber Security Consultant
yves.schellekens@outlook.com

Julie de Bergeyck
Program Manager AI & Deeptech
+32 474 99 71 16
julie.debergeyck@agoria.be

Patrick Slaets
Senior Expert Studies Centre
+32 497 27 76 48
patrick.slaets@agoria.be

Embracing technology
Embracing ambition

.AGORIA