CENTRE FOR
CYBERSECURITY
BELGIUM 10Y

10 YEARS OF THE CENTRE FOR CYBERSECURITY BELGIUM

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

.be

Responsible editor
Centre for Cybersecurity Belgium
Mr. De Bruycker, General Director
Rue de la Loi, 18
1000 Brussels

Research, interviews and editorial
the content company

Final editing
Katrien Eggers
Michele Rignanese

Photography
AdobeStock, own archive CCB, Karakters, Cookiecutter & Ron Lach for Pexels

Layout
Karakters.be

Print
Printing office of the House of Representatives

Legal Depot
D/2025/14828/007

Date of publication
October 31, 2025

TABLE OF CONTENTS

Dear Reader,

The Centre for Cybersecurity Belgium (CCB) was set up 10 years ago, thereby creating a single point of contact for cybersecurity in our country. What started with a royal decree on paper and the appointment of 2 motivated pioneers has grown into a highly respected national body backed up by a diverse team of nearly 140 experts. Together with numerous partners, we watch over the digital security of the public, businesses and governments, day and night.

The longer our economy and society rely on digital networks, the more intense this reliance becomes. In the meantime, cyber-attacks are also becoming more sophisticated and targeted. Cybersecurity is therefore an essential building block of our society. The European Union strengthened the regulatory framework in recent years, with among others the NIS1 and NIS2 Directives, the Cybersecurity Act and the Cyber Resilience Act. Each of these initiatives entails additional tasks and responsibilities, but more importantly, opportunities to raise the bar for cybersecurity even higher.

From our central role, we coordinate the follow-up of incidents, support vital sectors and focus on prevention. In other words, since day one, we have invested not only in technology, expertise and procedures, but above all in awareness and citizen involvement. Because more than anything, it is the collective action of all citizens and businesses together that makes us more cyber-resilient. Simple basic measures such as two-step verification and updating software in good time are still the most effective way to prevent damage.

We are therefore proud that Safeonweb has become a trusted reference for the general public, with clear tips and the possibility to easily flag suspicious messages. Every report helps us respond faster, provide more targeted information and be stronger collectively. And with Safeonweb@Work, including its practical guidelines and scans, we help companies gradually become better armed.

Our ecosystem has also since become more professional. Close cooperation, in full confidence, between the public services, the private sector and academia has allowed Belgium, under the coordination of the CCB, to become a European role model for cybersecurity.

This document looks back on a decade of learning, experimentation and embedding best practices. But it also looks ahead, as the rise of AI and geopolitical threats present new challenges. However, our commitment and engagement remain steadfast: to take proactive action to protect our country as much as possible.

Together, we can make Belgium one of the safest digital environments in Europe. That is our ambition. And we can only live up to that responsibility if we can take on the challenge with you.

Miguel De Bruycker
Director General

Phédra Clouner
Deputy Director General

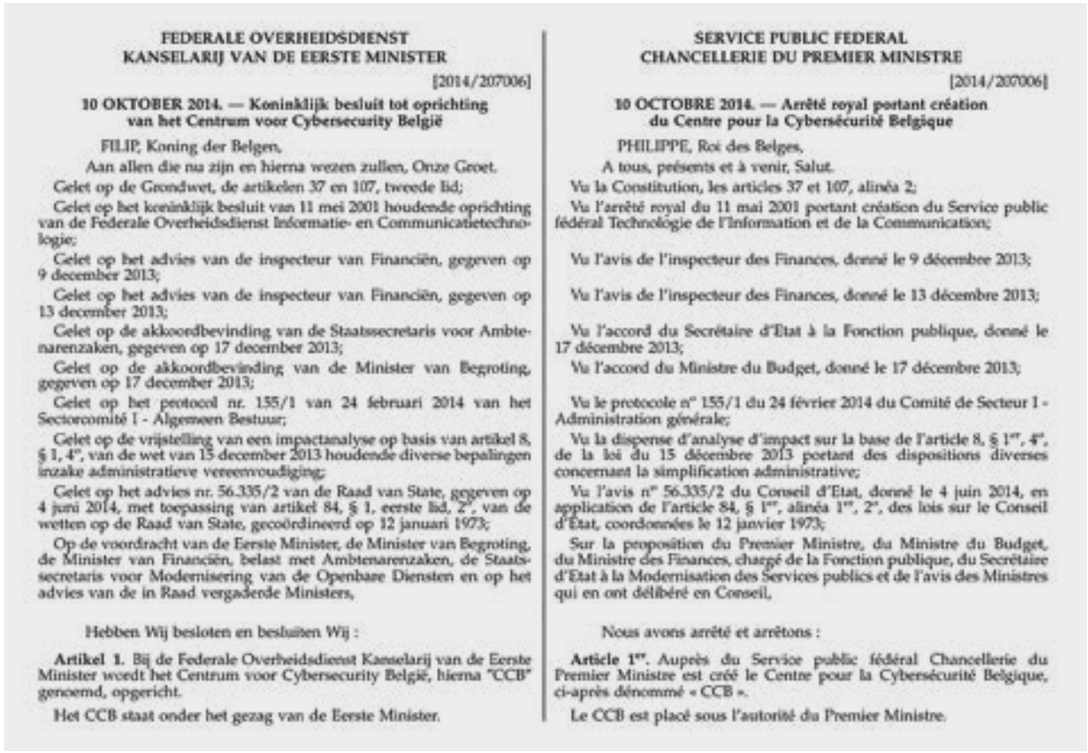
BACKGROUND

The Centre for Cybersecurity Belgium (CCB) was established by Royal Decree on 10 October 2014, and started operations in early 2015. But steps had already been taken to make Internet traffic safe in our country.

1993 saw the launch of Belnet, a federal research programme aimed at developing a network that would allow researchers to connect remotely to supercomputers. Belnet grew into an Internet hub and focused on ensuring the quality of connections and making them secure.

Within Belnet, the Computer Emergency Response Team (Belnet CERT) saw the light of day in 2004. This team responds to inquiries regarding security problems and incidents from members of the research network.

The Belgian Network & Information Security Platform (BELNIS) was also set up within the government. This was a consultative body in which all departments involved in digital security were represented, with the goal of discussing network and information security issues. As the body did not have decision-making power or financial resources, this platform did not immediately lead to concrete results.



FEDERALE OVERHEIDSDIENST
KANSELARIJ VAN DE EERSTE MINISTER

[2014/207006]

10 OKTOBER 2014. — Koninklijk besluit tot oprichting van het Centrum voor Cybersecurity België

FILIP, Koning der Belgen,

Aan allen die nu zijn en hierna wezen zullen, Onze Groet.

Gelet op de Grondwet, de artikelen 37 en 107, tweede lid;

Gelet op het koninklijk besluit van 11 mei 2001 houdende oprichting van de Federale Overheidsdienst Informatie- en Communicatietechnologie;

Gelet op het advies van de inspecteur van Financiën, gegeven op 9 december 2013;

Gelet op het advies van de inspecteur van Financiën, gegeven op 13 december 2013;

Gelet op de akkoordbevinding van de Staatssecretaris voor Ambtenarenzaken, gegeven op 17 december 2013;

Gelet op de akkoordbevinding van de Minister van Begroting, gegeven op 17 december 2013;

Gelet op het protocol nr. 155/1 van 24 februari 2014 van het Sectorcomité I - Algemeen Bestuur;

Gelet op de vrijstelling van een impactanalyse op basis van artikel 8, § 1, 4°, van de wet van 15 december 2013 houdende diverse bepalingen inzake administratieve vereenvoudiging;

Gelet op het advies nr. 56.335/2 van de Raad van State, gegeven op 4 juni 2014, met toepassing van artikel 84, § 1, eerste lid, 2°, van de wetten op de Raad van State, gecoördineerd op 12 januari 1973;

Op de voordracht van de Eerste Minister, de Minister van Begroting, de Minister van Financiën, belast met Ambtenarenzaken, de Staatssecretaris voor Modernisering van de Openbare Diensten en op het advies van de in Raad vergaderde Ministers,

Hebben Wij besloten en besluiten Wij :

Artikel 1. Bij de Federale Overheidsdienst Kanselarij van de Eerste Minister wordt het Centrum voor Cybersecurity België, hierna "CCB" genoemd, opgericht.

Het CCB staat onder het gezag van de Eerste Minister.

SERVICE PUBLIC FEDERAL
CHANCELLERIE DU PREMIER MINISTRE

[2014/207006]

10 OCTOBRE 2014. — Arrêté royal portant création du Centre pour la Cybersécurité Belgique

PHILIPPE, Roi des Belges,

A tous, présents et à venir, Salut.

Vu la Constitution, les articles 37 et 107, alinéa 2;

Vu l'arrêté royal du 11 mai 2001 portant création du Service public fédéral Technologie de l'Information et de la Communication;

Vu l'avis de l'inspecteur des Finances, donné le 9 décembre 2013;

Vu l'avis de l'inspecteur des Finances, donné le 13 décembre 2013;

Vu l'accord du Secrétaire d'Etat à la Fonction publique, donné le 17 décembre 2013;

Vu l'accord du Ministre du Budget, donné le 17 décembre 2013;

Vu le protocole n° 155/1 du 24 février 2014 du Comité de Secteur I - Administration générale;

Vu la dispense d'analyse d'impact sur la base de l'article 8, § 1er, 4°, de la loi du 15 décembre 2013 portant des dispositions diverses concernant la simplification administrative;

Vu l'avis n° 56.335/2 du Conseil d'Etat, donné le 4 juin 2014, en application de l'article 84, § 1er, alinéa 1er, 2°, des lois sur le Conseil d'Etat, coordonnées le 12 janvier 1973;

Sur la proposition du Premier Ministre, du Ministre du Budget, du Ministre des Finances, chargé de la Fonction publique, du Secrétaire d'Etat à la Modernisation des Services publics et de l'avis des Ministres qui en ont délibéré en Conseil,

Nous avons arrêté et arrêtons :

Article 1er. Auprès du Service public fédéral Chancellerie du Premier Ministre est créé le Centre pour la Cybersécurité Belgique, ci-après dénommé « CCB ».

Le CCB est placé sous l'autorité du Premier Ministre.

Royal decree establishing the Centre for Cybersecurity Belgium

2012: The first cyber strategy

The growing number of cybersecurity incidents prompted the realisation that a comprehensive national strategy was needed. That was elaborated in 2012 by Luc Beirens of the Federal Computer Crime Unit at the Federal Police and Miguel De Bruycker, who worked at the GISS, the General Information and Security Service. This first Cybersecurity Strategy had three objectives:

- Belgium will strive for a safe and secure cyberspace that respects the fundamental rights and values of modern society.
- Belgium will strive to ensure optimal security and protection of critical infrastructures and government systems against cyber threats.
- Belgium intends to develop its own cybersecurity capabilities.

Among the concrete actions to roll out the strategy, this paper explicitly stated the need to address cybersecurity in a centralised and integrated manner, through central management and by developing close public-private partnerships. The draft paper first floated the idea of setting up an independent cybersecurity coordination centre in Belgium.

At first, there was little political enthusiasm for a central coordination centre. However, a number of cyber incidents during 2013 and the arrival of a new federal government in late 2014 meant that cybersecurity was pushed up on the policy agenda.

2013: The Belgacom hack

One of the most notorious incidents from that period was the Belgacom hack. In the summer of 2013, Dutch cyber experts discovered evidence of digital intrusion at telecoms operator Belgacom. Extremely ingenious spyware was found in the IT systems, which had probably enabled criminals to intercept communications and data from Belgacom and its international subsidiary BICS since 2011. After the incident, Belgacom made substantial investments in cybersecurity. Tens of millions of euros went on renewing IT infrastructure and improving security against cyber-attacks.

2013: A European cybersecurity strategy

The implementation of the CCB cannot be seen in isolation from the developments in European cybersecurity policy either. The European Network and Information Security Agency ENISA was created as early as 2004. But it was not until February 2013 that the European Commission presented its first cybersecurity strategy, entitled "An Open, Safe and Secure Cyberspace." This strategy outlined legislative initiatives to promote cybersecurity, highlighted the importance of awareness in the public and private sectors and the need to invest more in R&D for cybersecurity.

At the same time, the Commission encouraged member states to set up the necessary structures to address cyber resilience, cybercrime and cyber defence to be better armed in the event of cyber incidents. The strategy recommended "optimising coordination at the national level between ministries and defining the roles and responsibilities of different national entities in national cybersecurity strategies."

"The implementation of the CCB cannot be seen in isolation from the developments in European cybersecurity policy either. The European Network and Information Security Agency ENISA was created as early as 2004."

2014-2016

CCB ESTABLISHED

The legal basis for establishing the Centre for Cybersecurity was laid down in late 2014. The CCB was given a clear mandate by the government: monitor, coordinate and strengthen cybersecurity in Belgium.

As such, the centre coordinates Belgium's cybersecurity policy. It monitors implementation, proposes initiatives and collaborates on new regulations. Raising awareness is one of its main tasks: informing citizens, businesses and public institutions about online risks and providing concrete tools to counteract them. At the international level, the centre represents Belgium in European consultative bodies. As the remit straddles different competencies and departments, the CCB was assigned to the jurisdiction of the Prime Minister, who has political responsibility.

There was significant interest during the recruitment for the key positions. For the position of director, 16 Dutch speakers and 19 French speakers applied. For deputy director, there were 27 Dutch-speaking and 29 French-speaking candidates. Following the round of selections, Miguel De Bruycker (hitherto employed at Defence) and Phédra Clouner (who worked within the Judiciary) were appointed director and deputy director, respectively, in August 2015, with five-year mandates. Both are still at the helm of the organisation. The rest of the team expanded systematically: from two employees in August 2015 to more than 140 today.

First CCB strategic plan

To guide the expansion of the organisation, the CCB worked on a strategic plan that was presented to the outside world on 26 October 2015. The plan outlined a timeline in three phases: a six-month start-up phase, followed by a three-year build-up phase and a maturity phase over five years. Separate operational objectives were defined for each of these phases, with the establishment of an integrated, coordinating and action-oriented approach as the common thread.

From the outset, the choice was made to align the strategic vision at the national level with highly concrete actions and services provided by the CCB. Prior to the strategic plan, four target groups were defined: citizens, businesses, vital interest organisations (this group was systematically expanded in later phases, under influence from the European NIS Directive) and public services.

This laid the foundation for the service-oriented approach which still typifies the organisation. The action plans explicitly stated the CCB's priority focus on services to the public, such as awareness campaigns. The reasoning was that name recognition among the general public would immediately lead to more awareness among other target groups as well.

At the same time, drawing up a cyber emergency plan was identified as an urgent priority. The plan would specify who can take charge in the event of an incident, in order to contain the impact of cyber-attacks. The idea was to have a unity of command, thereby efficiently tackling cyber-attacks against key Belgian targets.

In January 2015, the Cyber Security Coalition was established.

“From day one, the bar was set high and the period 2014-2016 immediately brought the cybersecurity needs, and the need for a coordinated approach in our country, into focus. Indeed, cyber threats were becoming more frequent, and the need for a coordinated approach more urgent than ever. In that context, cooperation from the start was essential.”

In its initial phase, the CCB grew from two to five staff.
Top, from left to right: Miguel De Bruycker, Phédra Clouner. Bottom, from left to right: Andries Bomans, Valéry Vander Geeten, Jo De Muynck.

From day one, the bar was set high and the period 2014-2016 immediately brought the cybersecurity needs, and the need for a coordinated approach in our country, into focus. Indeed, cyber threats were becoming more frequent, and the need for a coordinated approach more urgent than ever. In that context, cooperation from the start was essential.

The establishment of the Cyber Security Coalition as a private non-profit organisation, on 26 January 2015, was an important step in the right direction. The organisation brought governments, companies and knowledge institutions around the table to exchange experiences, analyse the risks and devise solutions. Thanks in part to this network, the CCB was able to move faster, both strategically and operationally, and lay the foundation for what is today the backbone of Belgian cybersecurity policy.

November 2015: first stress test

The baptism of fire for the fledgling CCB was not long in coming. In November 2015, posts surfaced on YouTube with hackers threatening to take down Belgian government websites. For the centre, this was the first real stress test, once again highlighting the need for a comprehensive cyber emergency plan.

The team immediately set to work to finalise the emergency plan and necessary coordination more quickly. The emergency plan envisages progressive escalation, in line with the severity of the incident, and stipulates which services have to assume which responsibility. Key aspects in this regard are speed, cooperation and clear communication.

The plan that eventually emerged on the table took into account various practical sensitivities, and also helped the CCB finally claim its place in the broader ecosystem. The cyber emergency plan created a clear structure with clear instructions in the event of large-scale cyber incidents that demanded a nationwide, coordinated approach. It was expanded and updated over time.

2016: Early Warning System developed

In 2016, the CCB strengthened its role as the coordinator of Belgium's cybersecurity strategy. As such, the centre helped strengthen cross-border cyber resilience in preparation for the European NIS Directive. At the same time, a first, rudimentary version of the Early Warning System (EWS) was developed in our country, which meant that critical sectors could be quickly alerted to new threats.

The EWS monitors digital networks of Belgian infrastructure and analyses technical indicators that may indicate malicious activity (such as botnets, fraudulent IPs or suspicious domains). The system is based on a combination of automated data collection, threat intelligence and real-time flagging. The flags are translated into alerts for specific organisations.

Sectors such as health care, finance and energy were connected as a priority. The alerts range from a notification regarding a leak in a particular software version to a concrete warning of targeted phishing campaigns.

2017–2020

OPERATIONALISATION

The CCB underwent significant growth after 2017. Cyberthreats and the various forms they took became a familiar occurrence in society. The developing maturity within the CCB not only reflected the growth in headcount, but great strides were also made strategically and substantively.

CERT.be: further development of high-end incident response

On 1 January 2017, the federal Cyber Emergency Response Team (CERT.be) was officially integrated into the CCB. This was more than an administrative reshuffle, the CERT was transferred from Belnet to another service. It was the start of a fundamental embedding of incident response into the broader national cybersecurity strategy.

For the CCB, this was its first big boost. This integration meant that the organisation could evolve. One major trump was the fact that the operations of the CERT could be fully overhauled and integrated into the strategy being rolled out by the centre.

The intention was clear: to scale up, better structure and align the operations of CERT.be with the increased threats in the Belgian and international cyber landscape. CERT.be already operated as a national CSIRT (Computer Security Incident Response Team), but its embedding within the structure of the CCB provided a unique opportunity to further professionalise the service and align it with all the other actions taken to strengthen cybersecurity. CERT.be gained access to more resources, specialised recruitment and policy support.

One of the first priorities after the integration was to build a new team. A more multidisciplinary make-up was intended to ensure that the team could not only respond to incidents, but could also pre-emptively identify threats, make recommendations and facilitate national coordination in the event of incidents.

An important milestone was reached at the end of 2018: the CCB was now operational 24/7 for providers of essential services and critical infrastructures. This permanent availability met the needs from the economy while also providing leverage to greatly improve national preparedness in the event of cybercrises.

Cyber Europe cybercrisis exercises 2018 and 2024.

This operational scale-up was implemented in close cooperation with the National Crisis Centre (NCCN). Thanks to this partner, permanent 24/7 service could be guaranteed.

In the meantime, the service was working on structural knowledge building. Recruiting and retaining cybersecurity specialists posed a continual challenge due to the tight labour market and competition from international players. Yet the team managed to deepen its expertise by making targeted investments in training and taking part in international exercises such as Cyber Europe, a large-scale European cyber crisis exercise organised by ENISA in which governments, companies and other organisations work together to test their resilience to large-scale cyber incidents.

The reputation and professionalism that had been built up were also recognised by other public services. In evaluations and collaborations, it became clear that the integration of CERT.be within the CCB led to more efficient incident management and better cooperation between different federal and sectoral players. The strengthened position of CERT.be was a catalyst for broader initiatives such as the implementation of the NIS directive and the development of the national alert platform.

After the terrorist attacks in 2016, part of the Provision Terro was used for cybersecurity

2016: Provision Terro as leverage

Following the terrorist attacks on Brussels Airport (Zaventem) and the Brussels metro in March 2016, the federal government decided to release additional structural and non-structural funding for projects aimed at tackling radicalisation, terrorism and violent extremism. Although this so-called 'Provision Terro' was not explicitly related to cybersecurity, this particular budget framework still played an important role for the CCB.

As terrorist networks also make significant use the digital domain, there was very quickly a clear link to cybersecurity. In that context, the CCB submitted proposals to use part of the Provision Terro to strengthen Belgium's digital resilience.

These funds therefore made it possible to enhance cooperation among public services. Indeed, combating cyber-related forms of terrorism requires cooperation between the CCB, State Security, the Federal Police, Defence, the Judiciary and foreign partners. These budgets provided the necessary room to jointly train personnel, build shared infrastructure and launch pilot projects that would otherwise have struggled to get funded.

Threat intelligence

The level of knowledge within the CCB was further expanded, which in 2020 led to the CERT.be service being split into a Cyber Threat Research and Intelligence team (CyTRIS) and a CERT team, which would now focus on cyber emergency response. Both facets of cybersecurity are still essential, and are part of the CCB's core business: intercepting and analysing threat information on the one hand and handling incidents on the other.

The Cyber Threat Research & Intelligence Sharing team has provided various services since 2018. It monitors diverse sources on a daily basis, collects and organises information that may be useful to alert potential victims, and performs in-depth cyber threat & intelligence analysis, on which it issues reports.

CyTRIS also sends spear warnings (individual alerts) to organisations where a given vulnerability has been identified on IT infrastructure, where malware has been discovered, or for which stolen login credentials have been found. It is also responsible for initial contact with organisations that report an incident to the CCB, in order to investigate the incident.

BePhish and the Belgian Anti-Phishing Shield (BAPS)

Phishing has been a major focus from the outset and remains one of the most common forms of cybercrime, with a significant impact. Clumsy, simply-written emails have evolved over the years into extremely realistic messages through all possible communication channels: email, text, WhatsApp and social media.

It quickly became clear that the traditional reactive model (intervening after a victim has reported an incident) was inadequate. As such, the CCB developed the BePhish project. Since 2019, citizens can report suspicious communications 24/7 at suspicious@safeonweb.be. There is an automated analysis and blocking system behind this mailbox. It processes an average of 25,000 emails a day.

Thanks to this initiative, the centre had a large amount of information on fraudulent websites. To actively combat these criminals, a second initiative was launched: the Belgian Anti-Phishing Shield

BAPS warning page

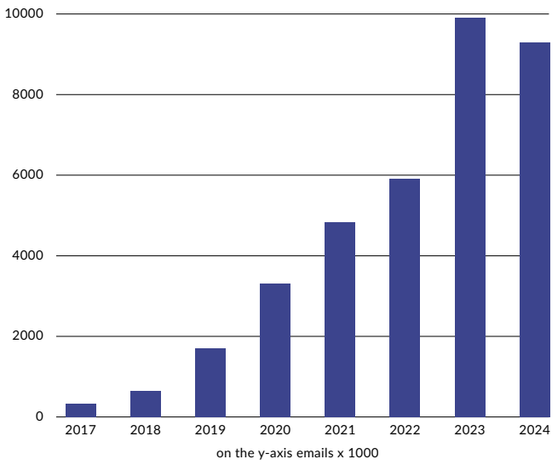
(BAPS), an additional wall of defence against these fraudulent pages on the internet. Indeed, visitors who click on these links are redirected to a warning page from the CCB.

Large-scale collaboration with Internet service providers was necessary in order to make this idea a technical reality. Proximus was the first provider to come on board, followed fairly quickly by Telenet. More than 100 providers now participate in BAPS. The redirecting page was triggered fully 240 million times in 2024.

The Anti-Phishing Shield reduced the response time against fraudulent websites from days to minutes. It is effective not so much on account of its technological inventiveness as the fact that citizens have been involved since its inception and continue to report messages with suspicious URLs on a large scale. Thanks to a robust spam filter that emerged from this philosophy, the CCB, along with providers, also prevents fraudulent emails from getting into the mailboxes of citizens and businesses.

The tandem BePhish and BAPS is a unique contribution to collective security: thanks to all the reports, the CCB can quickly detect trends and send out alerts via Safeonweb. The controversial idea of active government intervention in Internet traffic grew into one of the CCB's hobby horses. Restricting freedom of movement in cyberspace prompted several complaints, but they were successfully overturned each time.

Evolution of mails to suspicious@safeonweb / URLs BAPS



The 'NotPetya' incident and the Spear Warnings

On 27 June 2017, the CCB received reports from several European countries about a wave of cyber incidents. The attacks looked like ransomware, but were actually 'Not Petya' wiper malware. In other words, the goal was not to collect a ransom in exchange for releasing data, but rather to remotely render systems permanently unusable. This was a global cyberattack, and primarily targeting companies with operations in Ukraine.

The attackers had developed a system that could spread at lightning speed through various networks. One of the companies that suffered the biggest impact was Danish logistics firm Maersk. It had to take down its entire IT infrastructure to halt the attack. Staff were obliged to switch back to using pen and paper.

In our country, the CCB had to move particularly quickly to follow up on the incident. 'NotPetya' was part of the reason for developing the so-called Spear Warnings: when vulnerabilities are identified on an IT network, the CCB is authorised to identify the IP address of the organisation in question. It can then alert companies and other organisations about these vulnerabilities. This proactive attitude therefore helps prevent cyber incidents.

NotPetya-marked the start of the CCB Spear Warnings.

Gradual expansion of the Early Warning System

In order to respond to digital threats in a faster and more targeted manner, the CCB focused on further developing its Early Warning System (EWS) starting in 2018. This alert system has been Belgium's technological radar in cybersecurity ever since.

The system was gradually expanded during this period, both in scope and depth. The CCB also developed a methodology for ranking reports by risk and urgency, which enhanced effectiveness and confidence in the system. The Early Warning System has since become an essential tool in Belgium's cybersecurity arsenal.

Quarterly Cyber Threat Report

In addition to real-time threat information, the CCB saw the need for a structural reporting model that provided insight into trends, vulnerabilities and emerging risks. This led to the Quarterly Cyber Threat Report (QCTR) - a quarterly report via which the CCB has been transparently sharing the cyber threat context in Belgium with critical stakeholders in critical sectors, policymakers and other agencies involved, since 2019. By informing them about the broader threat landscape, the CCB helps them reinforce their own risk management.

Each QCTR includes insights on dominant attack vectors, emerging vulnerabilities and sectoral trends (such as increased activity in the healthcare sector or among municipal governments), and analysis of larger incidents. The goal is information sharing. For this, the CCB gathers data from incident reports, international threat feeds and input from partners within the ecosystem - including commercial partners and CSIRTs.

NIS1 Directive

Between 2017 and 2020, the CCB played a key role in the transposition of the first European Directive on Network and Information Security (NIS1). This directive, formally adopted in July 2016, marked an important step in enhancing cybersecurity within the European Union. The goal was to strengthen the digital resilience of critical infrastructures and essential services, promote cross-border cooperation and ensure the stability of the digital single market.

Right from the preparatory phase, the CCB kept a close eye on this regulatory process. As soon as it became clear that the NIS directive was coming, the CCB took steps to bring the Belgian regulatory framework into line with the forthcoming European requirements. To handle this complex task, the CCB bolstered its legal and technical capacity.

Besides actively representing Belgium in the European NIS Cooperation Group and the CSIRT network, the CCB was responsible for preparing national legislation. This process ultimately led to the NIS Law of 7 April 2019, which laid down the legal framework for the security of network and information systems of general interest for public security, and the Royal Decree coordinating implementation.

The operational implementation of NIS1 was also the responsibility of the CCB. The CCB set up the Cyber Security Sectoral Authorities Platform (CySSAP), a structure in which relevant public services and sectoral authorities (such as FSMA for the financial sector or BIPT for post and telecommunications) are briefed, advised and coordinated on a regular basis.

Nevertheless, Belgium was the last EU member state to implement the NIS1 directive. The fragmentation of decision-making power among different stakeholders proved particularly problematic. Indeed, each sector had to individually assess what the impact of NIS1 would be. As the challenges proved new and difficult to comprehend, some sectors applied the brakes.

Last but not least, the CCB developed a reporting point for cybersecurity incidents, in accordance with the NIS directive. For the CCB, the implementation of NIS1 represented not only a confirmation of its institutional role, but also a new catalyst for further expansion.

COVID-19 and cyber risks to the healthcare system

As a result of NIS1, each sector had to list the providers of essential services. Within the healthcare sector, it was agreed in 2019 that the sector had no such providers. As such, the healthcare sector did not have to meet the obligations of the NIS directive. As a result, the sector was not included on the CCB's priority list either.

However, the outbreak of the COVID-19 pandemic in the spring of 2020 completely changed the situation. Hospitals were suddenly among the preferred targets of cybercriminals, who wanted to put further pressure on the healthcare system and had their sights on the data.

The cybersecurity ecosystem offered collective support at that time. The CCB supported a 'coalition of the willing' of cybersecurity and IT service providers, consulting firms and independent experts willing to provide free support to hospitals. Through the website wehelpourhospitals.be, healthcare facilities could connect with these partners for advice, risk analyses, incident response, etc.

This period made it painfully clear that the relationship between the cyberworld and sectoral governments needed to be reviewed. An overhaul, with the CCB being assigned a central oversight role, led to a much more effective model. This would subsequently be demonstrated with the implementation of NIS2: despite the fact that the number of critical sectors involved rose from 7 to 18, Belgium would be the first EU member state to transpose the directive into national law.

With the centre more than fulfilling its role, with an efficient use of resources and a respected offering of practical services and support, this period saw a growing realisation among policymakers that the CCB was essential to the security ecosystem in Belgium. Moreover, during this period, the centre also developed the habit of linking its strategy and action plans to clear project budgets. This high level of transparency regarding its operations and funding are still the case today.

"In order to respond to digital threats in a faster and more targeted manner, the CCB focused on further developing its Early Warning System (EWS) starting in 2018. This alert system has been Belgium's technological radar in cybersecurity ever since."

2020-2024

GROWTH

Despite all the efforts, the number of incidents reported to the CCB continued to rise sharply. Among other things, ransomware was having an ever-bigger impact, both in the public and private sectors. Worldwide, cybercrime is still considered the main risk of serious financial loss. The CCB's remit therefore remains acutely relevant.

In August 2020, the mandates of director Miguel De Bruycker and deputy director Phédra Clouner came to an end. The federal government decided to extend their mandates for five years. In this regard, besides continuing its existing remit, the CCB was tasked with updating its vision and strategy in line with the growing threat in the cyber landscape.

The National Cybersecurity Strategy 2.0

To realise this remit, the National Cybersecurity Strategy 2.0 was implemented within the CCB. This included six strategic objectives:

- Strengthen the digital environment and build confidence in the digital environment
- Arm users and administrators of computers and networks
- Protect organisations of vital importance from all cyber threats
- Respond to the cyber threat
- Improve public, private and academic collaborations
- Make a clear international commitment

Director General Miguel De Bruycker explained the new strategy as follows:

"In any society, you need enforceable rules, and it's no different in cyberspace. We therefore need to strike a new balance between a totally open, free and anonymous Internet, and a dependable Internet in which enforceable rules and national laws still apply. However, none of this should get in the way of communicating freely and anonymously.

A balance between a totally open and free cyberspace and an Internet in which certain legal rules can still be enforced is clearly possible, in my opinion. Three concepts can significantly improve cybersecurity in the medium and long term: Trusted Sender, Trusted Publisher & Spear Warning.

For example, at the European level, it is possible to make sure that if you come to a website that does not have a nationally registered organisation or entity linked to it, you will be flagged.

The Belgian implementation of the EU Cybersecurity Act must be implemented as a priority, so that our country has the mandatory National Cybersecurity Certification Authority by June 2021. The necessary resources for this have been budgeted. Subject to a political decision, the plan worked out with the FPS Economy can be implemented."

The new strategy was approved by the government in 2021. Having paved the way in its first five years by creating partnerships and improving cybersecurity coordination in our country, and having laid the foundations for a more integrated approach to security, the CCB's goal was to further expand the range of services offered and become even more responsive to specific needs and threats.

As an explicit ambition, the Director and Deputy Director pushed to make Belgium one of the least cyber-vulnerable countries in the EU. All the actions implemented during this period fell within this objective. In addition, the organisation was tasked with a number of special responsibilities, meaning that it could further enhance its coordinating role.

Growth in the budget and team

As of the start of 2020, the CCB had around 50 employees and an annual operating budget of about €15 million. As a result of the Cyber Strategy 2.0 and the European obligation to set up a National Cybersecurity Certification Authority (NCCA), growth to 80 employees and a budget of about €36 million per year were envisioned.

National Cybersecurity Certification Authority

The European Union undertook large-scale regulatory work to enhance cybersecurity. The Cybersecurity Act was passed in 2019, laying the foundation for common certification of ICT products, services and processes. In this regard, the EU aimed to increase the cyber resilience of all member states and boost the quality of and confidence in cyber-secure products through common standards.

In each member state, a National Cybersecurity Certification Authority (NCCA) was now required to oversee and guide companies through the certification process. The Authority also has the mandate to issue guidelines for certification at the national level. In Belgium, this task was entrusted to the CCB, which strengthened its role and expanded its competencies.

The NCCA oversees certification and monitors compliance with certificates issued by Conformity Assessment Bodies (CABs). It can also be consulted in complaints regarding product certification, or misuse thereof. The NCCA also has the authority to enforce compliance.

National Cybersecurity Coordination Centre for Belgium

Another outgrowth of European initiatives was the setting up of the National Cybersecurity Coordination Centre for Belgium (NCC-BE) in 2021. The EU aims to spend the funds it sets aside for research and innovation in the field of cybersecurity in a more coordinated way. The idea is to integrate national priorities and needs into an overarching European approach. At the same time, the EU wants to better inform researchers and innovative companies about the financial support available, so that this leads to more cross-border projects. The NCC-BE encourages dialogue between companies, academics, researchers and government. It aligns the policy in research, development and innovation, and helps realise the Belgian Cybersecurity Strategy. The NCC-BE links existing and future initiatives in cybersecurity, creates synergies and supports educational programmes. In addition, the NCC-BE ensures that all regions, communities and the federal government combine their efforts for a unified approach to cyber threats. Moreover, the NCC-BE supports organisations in securing EU funding, and coordinates strategic investments.

At the European level, the NCC-BE represents Belgium and ensures that the cybersecurity interests of the Belgian government, industry and academics are always heard.

Under the aegis of the European Cybersecurity Competence Centre (ECCC), the NCC-BE works with a network of 29 national coordination centres. This initiative strengthens cybersecurity innovation, supports industrial policy and contributes to Europe's technological sovereignty.

National Cybersecurity Coordination Centre for Belgium (NCC-BE) (2021)

Preparations for NIS2

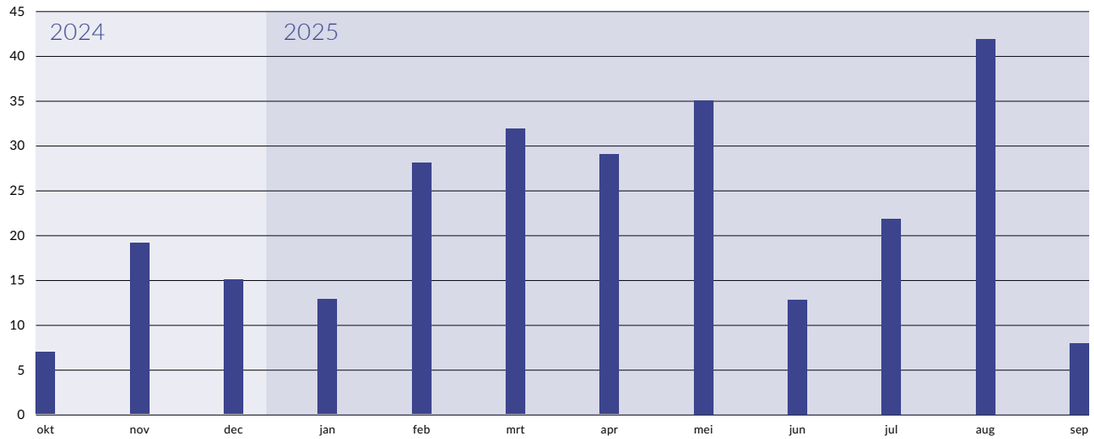
In December 2020, the European Commission announced that it would prepare a NIS2 directive, as the successor and further refinement of NIS1. The intention was of course to further enhance cybersecurity, but also to further streamline the approach within the EU. Indeed, NIS1 had left member states with relative freedom to interpret the European requirements. However, this led to varying interpretations and differences in implementation among member states. This shortcoming would be remedied with NIS2.

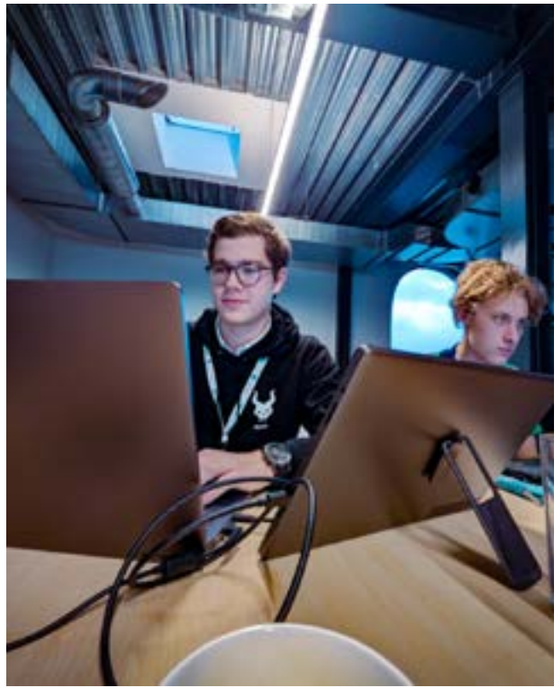
One of the most significant changes from its predecessor was the fact that the number of affected sectors that would be subject to the obligations of NIS2 was extended. In Belgium, over 100 entities from 7 sectors including energy, transportation, healthcare, digital infrastructure and public services fell within the scope of NIS1. After implementation, NIS2 would apply to more than 4,000 entities from 18 sectors.

The CCB participated at the European level in consultations on the interpretation of the NIS2 directive. The parliamentary work in Belgium (the transposition of the European directive into Belgian law) was prepared together with the administrations, the CySSAP forum (in which the sectoral authorities are represented) and the political level.

The NIS2 Law entered into force in Belgium in October 2024. Thanks to early discussions and preparations, the CCB smoothly scaled up its approach to NIS2: it would evolve into the central body for monitoring and verifying compliance with NIS2, working closely with the sectoral authorities.

Reports from October 2024 to September 2025





Hack the Government, the first-ever ethical hacking event (2024)

Coordinated Vulnerability Disclosure (CVD)

A legal procedure for reporting vulnerabilities has been in place in Belgium since 2023. The CCB is obliged to receive notifications from researchers regarding potential vulnerabilities that fall under Belgian law. Coordinated Vulnerability Disclosure (CVD) is a process whereby researchers, companies and governments handle the discovery and reporting of security problems in ICT systems, products or services in a structured and secure manner. The goal is to remedy vulnerabilities in a timely and responsible manner, so they are not exploited early.

In November 2024, the CCB hosted Hack the Government, the first-ever ethical hacking event. The aim was to demonstrate that ethical hackers can help make Belgium more cyber-secure. This unprecedented initiative brought together the community of ethical hackers to identify vulnerabilities in government websites and systems.

The CCB created a registration tool for NIS2 entities through the existing Safeonweb@work platform and developed a pragmatic system for reporting incidents. Indeed, the new directive required organisations to notify any significant incident to the CCB immediately after being discovered.

To support organisations in meeting the NIS2 requirements, the CyberFundamentals framework (CyFun®) was developed, a practical guide for taking cybersecurity measures, structured in different levels, tailored to the maturity of the organisation. In this way, the framework is also relevant to companies and organisations outside the NIS2 sectors. The public debate on NIS2 led in any case to much more awareness of cybersecurity among the Belgian business community.

Stop Phishing

The efforts to prevent crime via phishing, within the global approach of the Belgian Anti-Phishing Shield (BAPS), continued unabated. In 2020, a new project called "Stop Phishing" saw the light of day. The goal was to prevent e-mails or text messages containing malicious links from reaching citizens and businesses. They were intercepted even before they reached the e-mail box or text message folder.

This project became a successful public-private partnership with the operators involved, and received explicit support from the government. It represented another step in the proactive and preventive approach of the BAPS. The government funded part of the software used by participating service providers via the CCB.

PhishNemo

PhishNemo is an extension of the BAPS project. This initiative was originally developed by the Federal Judicial Police (FGP) of Limburg, and has since evolved into a collaboration between the latter and the CCB. While the Belgian Anti-Phishing Shield relies primarily on notifications from citizens, PhishNemo has been proactively looking for suspicious domain names that might be used in phishing campaigns since 2023.

This is by comprehensively screening new domain names. It looks for traces of known phishing tools - so-called 'fingerprints'. Thanks to this approach, fraudulent domains can be detected even before the first phishing email is sent. The domains detected in good time are immediately added to the BAPS system, so that they can be redirected straight away, through partnerships with Internet service providers.

By taking over this system from the Limburg FGP, the project could continue to grow. The CCB works with private partners to this end, who maintain the IT systems. As a result, PhishNemo can actively contribute to the Belgian Anti-Phishing Shield.

Hacktivism peaks after Russia invades Ukraine

In February 2022, Russia invaded Ukraine, the start of a long-running war. Although cybercriminals are primarily interested in financial gain, a close link between geopolitics and cyber-attacks has since developed. These shifts in the geopolitical landscape meant that the CCB had a place as a permanent member of the National Security Council.

This permanent accession to the permanent consultation of intelligence and security services was a very important milestone for the organisation. Indeed, the CCB was now an integral part of the country's security architecture. It also gave the organisation access to additional operating funds from the Ukraine provision.

It also proved to be the logical choice in practice: the more time went on, the more hacktivist groups appeared on the scene. Their preferred modus operandi includes Distributed Denial of Service (DDoS) attacks, in which websites get overloaded, and hack-and-leak operations. Since the outbreak of the war in Ukraine, a rise in ransomware attacks against municipalities and government agencies has also been observed in several European countries, including Belgium.

Given the geopolitical context, the run-up to the European, national and regional elections in June 2024 saw heightened vigilance for cybersecurity events, or heightened threats. Federal, state and local governments alike could count on advice and technical support from the CCB. During the election weekends in June and October 2024, continuous monitoring was ensured and the CCB also kept an emergency team on standby.

Moreover, the CCB had also conducted a security audit in previous election cycles. This formed the basis for a series of recommendations, which led to a significant increase in the security of election IT systems. Partly as a result, elections in Belgium have never been disrupted by cyber- attacks.

> "As an explicit ambition, the Director and Deputy Director pushed to make Belgium one of the least cyber-vulnerable countries in the EU. All the actions implemented during this period fell within this objective. In addition, the organisation was tasked with a number of special responsibilities, meaning that it could further enhance its coordinating role."

ACTIVE CYBER PROTECTION, A PROACTIVE VISION

Digitisation opens up unprecedented opportunities for citizens, businesses and governments. But the more we digitise, the greater the risks. Cybercrime is evolving rapidly, attacks are becoming more sophisticated and the impact on our society is only growing. To meet this threat, securing the digital environment is an essential condition.

Since its inception, the CCB has seen it as its mission to make vulnerabilities (both human and technical) visible and actively neutralise them. Instead of reacting only after an incident, the CCB focuses on prevention, rapid detection and targeted responses.

In 2024, this proactive approach was given an umbrella name: Active Cyber Protection (ACP). This concept includes a series of ongoing and additional projects that strengthen cybersecurity even before an incident can occur.

At the insistence of the CCB, ACP was included in the European NIS2 directive, which entered into force in Belgium in 2024. This directive requires companies across a range of key sectors to adopt additional security principles and implement risk management systems.

The NIS2 Directive therefore demands a more active approach from all Member States, and also imposes Active Cyber Protection as a legal requirement. As Belgium intends to play a leading role in this area, ACP is a central pillar of our national cyber strategy. The CCB makes this abstract concept concrete with an approach that is proactive, tailored, automated and participatory:

- **Proactive:** not waiting for an incident to occur, but detecting and addressing threats before they cause damage.
- **Tailored:** no one-size-fits-all. Communication and responses are tailored to the needs of specific organisations and sectors.
- **Automated:** speed is critical. Automation allows for faster responses and compensates for the acute shortage of cybersecurity experts.
- **Participatory:** cybersecurity is a shared responsibility. Employees, partners and citizens must be actively involved.

This vision takes shape through five strategic pillars. These pillars form a flexible framework that is continually evolving in line with the ever-changing tactics of cybercriminals.

PILLAR I: RAISING AWARENESS BY INVOLVING PEOPLE

A strong cybersecurity policy starts with the general public and increasing their awareness. This has been the guiding principle of the CCB since inception. By flagging suspicious messages, citizens can actively contribute to raising the country's cybersecurity level. The initiatives in the context of Safeonweb serve to arm citizens and businesses against digital threats. This undeniably forms the basis of the proactive vision, and by extension the philosophy of the CCB.

For citizens: Safeonweb@home

Safeonweb@home informs citizens about current dangers via a website, campaigns and social media. The Safeonweb app plays a key role in this regard: it alerts users to phishing attacks in good time and offers accessible security tips.

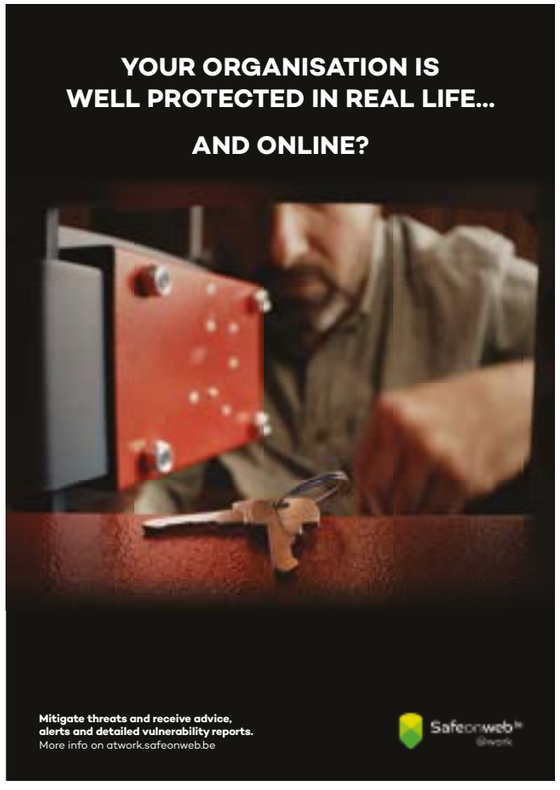
Another success story that focuses on citizens is suspicious@safeonweb.be, an e-mail address in four languages where citizens can report suspicious e-mails. In 2023 alone, nearly 10 million reports were made. An impressive figure that shows how valuable their contribution is in the fight against cybercrime.

82% of the population is familiar with Safeonweb

For businesses: Safeonweb@work

Since 2023, Safeonweb@work has also been operational: a platform tailored to Belgian companies with clear, actionable recommendations for integrating cybersecurity into daily policy - without heavy investments or complex procedures.

Through an online portal, companies can register their domains and receive automatic alerts regarding vulnerabilities in their IT infrastructure. The platform also includes self-assessment tools, basic guidelines and best practices, so that organisations can bolster their security levels at their own pace. In this way, the CCB helps increase the cyber maturity of the professional landscape.



Campaign Safeonweb@work 2024

PILLAR II: DETECT AND DISABLE CRIMINAL INFRASTRUCTURE

The second pillar focuses on the core of cybersecurity: the infrastructure criminals use to carry out attacks. For example, phishing websites or fraudulent servers. With the Belgian Anti-Phishing Shield (BAPS) project, the CCB is tackling these practices at the source.

Together with Belgian Internet service providers, malicious websites are automatically detected and disabled by immediately redirecting the user to a safe landing page. In this way, approximately 100,000 Belgians a day are protected from potentially harmful websites.

Speed and automation are the strength of the system. Malicious URLs are continuously updated and integrated directly into the DNS systems of providers. Threats are therefore intercepted in real time, often before they can do any damage. In this way, BAPS is a textbook example of proactive cyber protection: silently in the background, but with measurable impact.

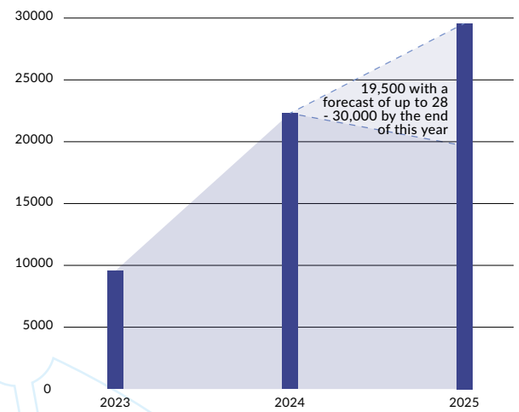
This approach has not gone unnoticed elsewhere in government, finance and police services. Various organisations indicated that they have valuable data within their own domain, such as information about fraudulent web shops or investment fraud. However, they do not have the ability to redirect domains at the national level in an automated manner.

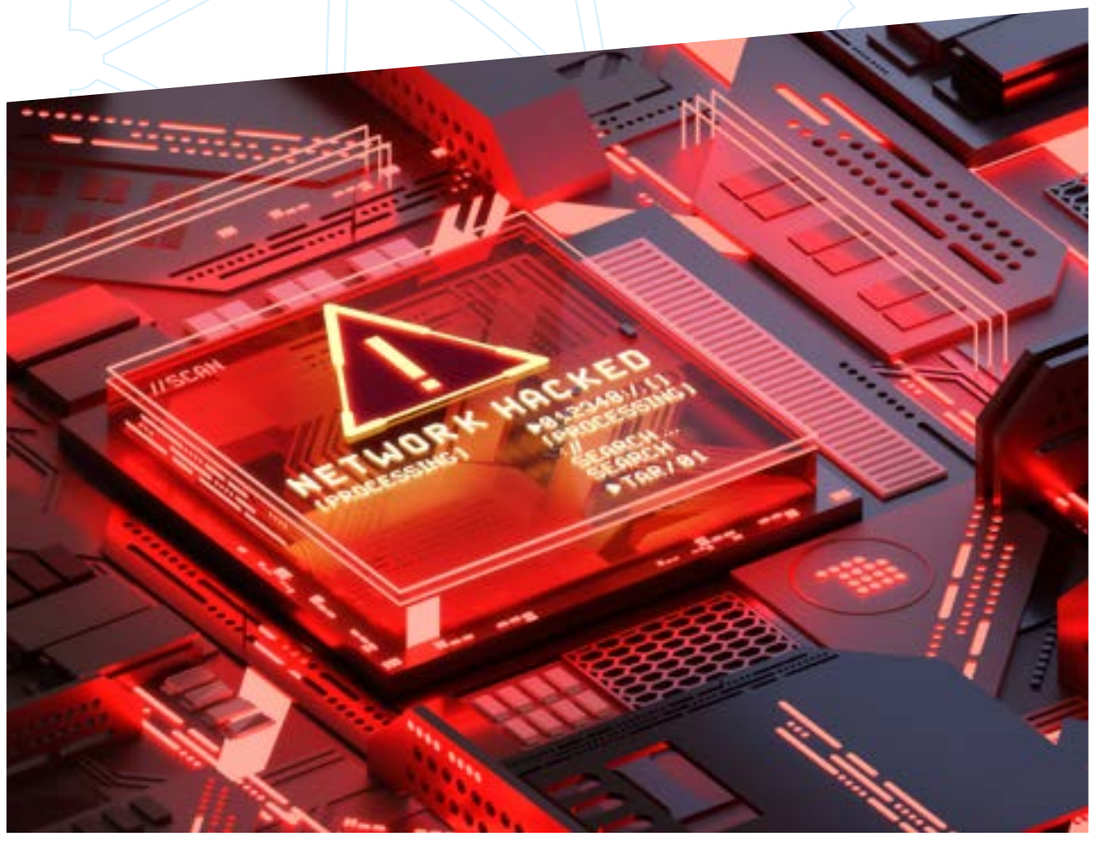
As such, the CCB has developed the concept of trusted partners: privileged access to the BAPS system for carefully selected partners. The partners supply the data, the CCB then handles the practical redirecting of suspicious domains through cooperation with the ISPs. Today, the FPS Economy, the FSMA, Itsme and a number of Belgian banks, among others, are active as trusted partners within this system.

PILLAR III: FLAGGING THREATS IN A FOCUSED WAY

Cybercriminals often use spear phishing: targeted attacks on specific individuals to obtain sensitive information. The CCB takes a similar approach, but for the benefit of users. With 'spear warnings', the CCB informs organisations directly about vulnerabilities in their digital environment.

Figures on the evolution of spear warnings





This approach allows organisations to take rapid, targeted action even before a vulnerability can be exploited. The best-known initiative is the Early Warning System (EWS), a platform aimed specifically at organisations with critical or vital infrastructure that are subject to the obligations of the NIS2 Directive.

Through this portal, CCB analysts are in direct contact with these vital organisations. For them, the EWS is an extra pair of eyes: it monitors digital signals, detects risks and proactively sends alerts. In addition, the organisations also receive personalised notifications about data breaches, leaked login information and insecure systems within their infrastructure, among other things.

This proactive approach not only helps avoid incidents, but also increases awareness and response times within organisations.

PILLAR IV: EMBED CYBERSECURITY IN THE ORGANISATION

To become truly resilient, organisations must incorporate cybersecurity into their daily operations. The CCB therefore developed the CyberFundamentals Framework: a practical and scalable model that helps organisations strengthen their digital protection step-by-step. The framework consists of three assurance levels (Basic, Important and Essential), preceded by an entry level: Small. Each level includes a set of concrete measures. 'Small' thereby serves as a guide for very small organisations that do not have any experience yet with cybersecurity, and are taking their very first steps.

The measures from the CyberFundamentals Framework are tailored to the most common cyberattacks and were validated against CERT attack profiles. The effectiveness of the model has since been proven:

- The **Basic** level covers around 82% of common attack types.
- With the **Important** level, this percentage rises to 94%.
- Organisations that achieve the **Essential** level even protect against 100% of these attacks

The framework is based on international standards such as NIST Cybersecurity Framework, ISO and IEC, and is accessible to organisations of all sizes. Certification by an external body is possible, but this is not a requirement.

CyberFundamentals makes cybersecurity concrete, measurable and achievable, even for SMEs or organisations without an IT department. Moreover, the model grows in line with the risks: it is in constant evolution in order to stay relevant in a rapidly changing digital world.

PILLAR V: CREATING A TRUSTED ENVIRONMENT

The Internet provides a certain freedom, and with that freedom comes anonymity. But of course, this anonymity is a double-edged sword. On the one hand, it protects our privacy and freedom of speech. On the other hand, it opens the door to abuse. This is precisely why the need for more transparency and digital validation is growing: to restore trust and counter the dark side of anonymity.

The search for this new balance between anonymity and identity is not a straightforward exercise. In essence, it is a change in behaviour: citizens need to get used to the idea of identification becoming a natural part of their digital presence. This is the only way to better allocate online activities and therefore make them more secure.

"Together with Belgian Internet service providers, malicious websites are automatically detected and disabled by immediately redirecting the user to a safe landing page. In this way, approximately 100,000 Belgians a day are protected from potentially harmful websites. "

To give Internet users more confidence in the parties with whom they interact online, the CCB developed the Safeonweb browser extension. This extension displays a clear colour code for each website visit:

- **Green** means that the website owner is validated and therefore trustworthy.
- **Orange (or amber)** indicates an unknown or unvalidated owner. In this case, caution is advised.
- **Red** indicates a known unsafe or malicious website that you should completely avoid and not share data with.

The extension is designed with security as well as ease of use in mind. It works automatically in the background and shows at a glance whether personal data can be shared securely. This gives the browser/user more assurance that the recipient with whom he or she wishes to share data is safe.

Is suspicious content still discovered on a validated website? Then the status changes immediately, based on the first notification: from green to orange or even red. That way, the system stays up-to-date and reliable at all times.

CCB FOR EVERYONE

AWARENESS RAISING: CHALLENGE NUMBER 1 AT THE OUTSET

In its first years of existence, the CCB faced a structural challenge: Belgium was increasingly confronted with cyber threats, but there was still no awareness among the general public. Citizens, businesses and even some public services underestimated the risk.

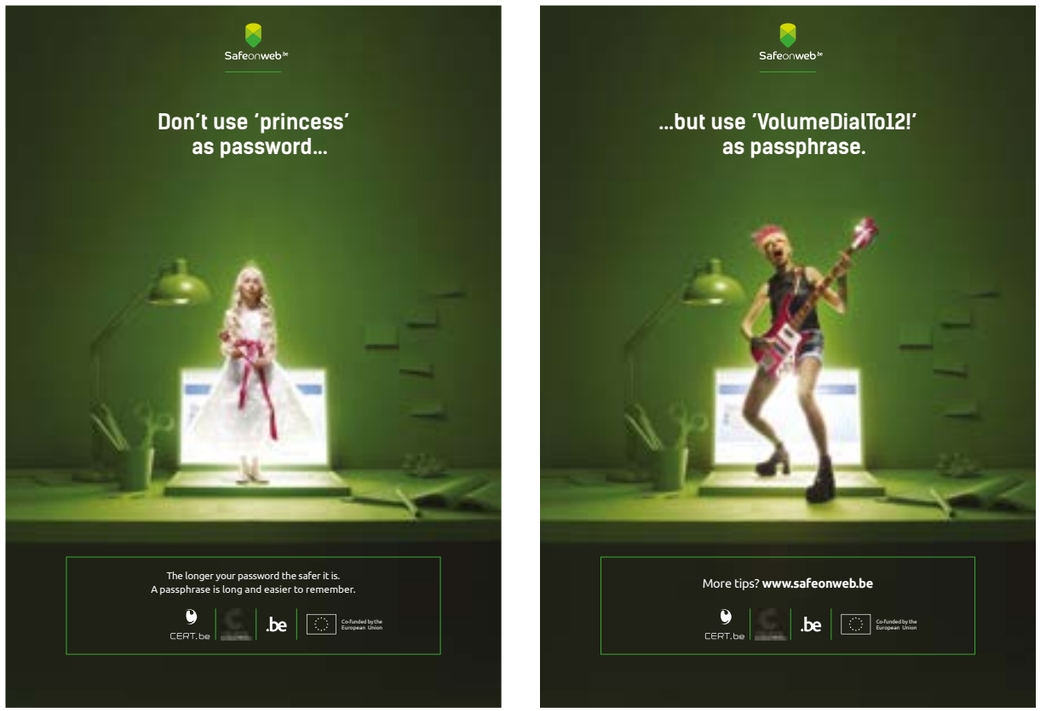
Realising that the strength of any security is ultimately determined by the human link, it was decided not only to invest in detection and incident response, but at the same time to work on raising awareness on a large scale through awareness campaigns.

The first campaigns focused on specific risks: phishing emails, weak passwords, clicking on suspicious links and the importance of updating software regularly. To strengthen the impact of these actions, the CCB focused on working with partners such as banks and telecom companies and the Cyber Security Coalition. Employers and local governments were specifically approached to further disseminate the information.

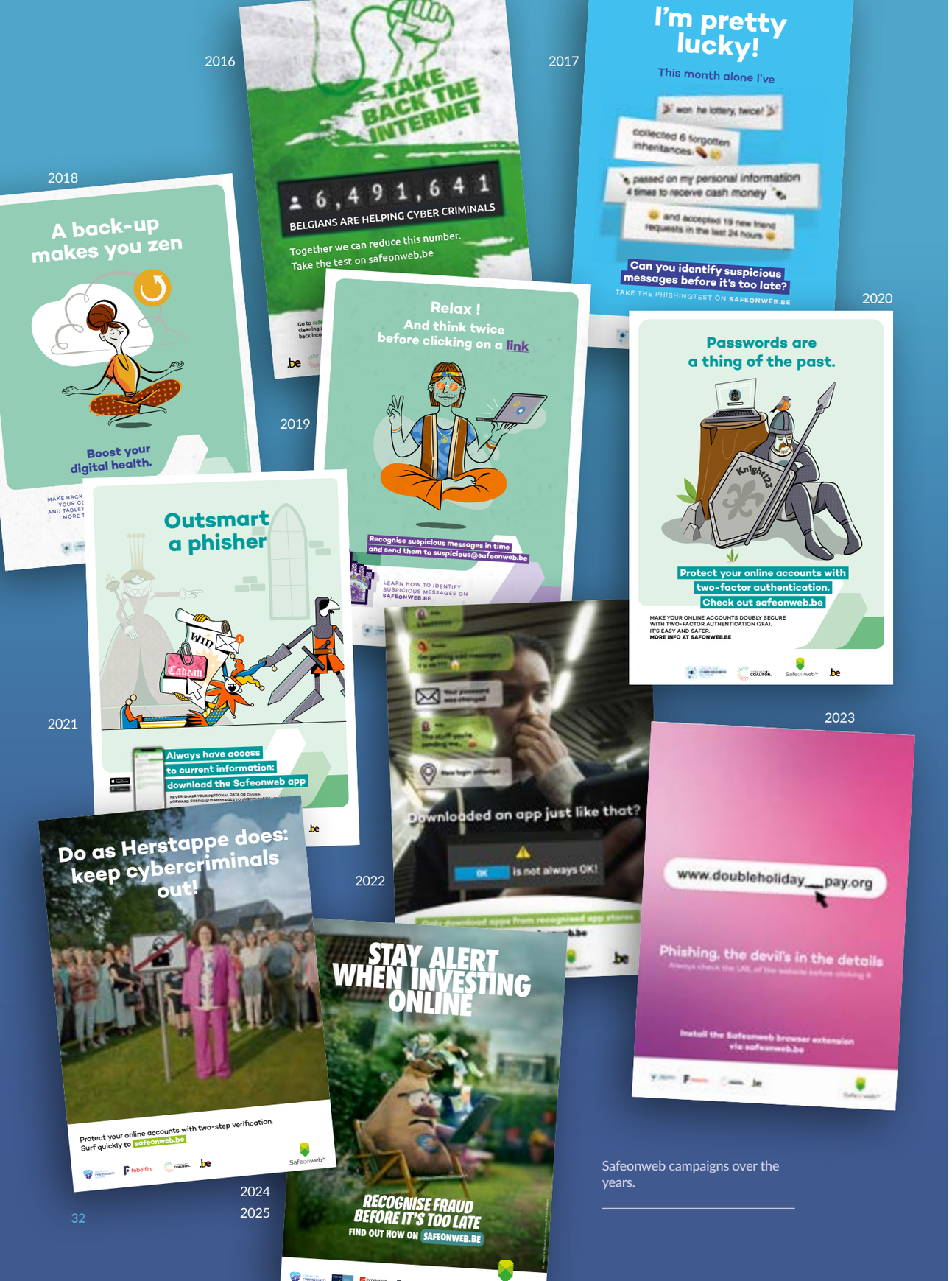
Internally, these campaigns laid the foundation for a new, multidisciplinary way of working at the CCB. Communications specialists and technical teams worked with behavioural psychologists and marketeers to develop the first campaigns. For a government organisation, it was a groundbreaking, creative way to raise awareness.

Part of European awareness raising

The CCB plans its annual campaign in the month of October. That is no coincidence. Indeed, October was declared European Cybersecurity Month, an annual initiative of the European Commission and the agency ENISA. This campaign also focuses on raising cybersecurity awareness and broadly



First Safeonweb campaign



Safeonweb campaigns over the years.

informing citizens and organisations on how to better protect themselves online.

To generate additional impact, the CCB also organises information campaigns in the interim, at times when scammers are also extra active: around holidays, sales periods or according to current events.

The centre also gets involved in Safer Internet Day, a global awareness campaign organised every year in February and specifically targeting schools and youth organisations.

Finally, the organisation happily shares and boosts campaigns by partner organisations on the topic of cyber prevention.

Partners reach out

The theme of the annual Belgian campaign is selected based on current events and key trends. It is conducted in the three national languages and involves actors from all sectors.

This involvement is one of the strengths of the awareness campaigns: on the one hand, the CCB has a series of privileged partners such as the FPS Economy, the FSMA, the Federal Police, bank federation Febelfin, and the Cyber Security Coalition. They act as a sounding board, involved in management and providing feedback at all stages of the campaign's development: from selecting the theme, to translating it and how it is portrayed in the campaign, to the power to persuade and encourage the public to change their habits. Each partner brings its know-how and knowledge from the field to the table.

On the other hand, the centre can also count on more than 600 organisations who undertake to distribute the materials. By having all these partners help disseminate the campaign, it has an impact far beyond the paid media plan organised every year, and is longer-lasting.

Another strength is the philosophy of the campaigns. The tone is light, simple and clear. The aim is to convince as many people as possible (including those who struggle with IT or are scared of the online world) that they can make a difference. This positive reinforcement is combined with a solution-oriented message, so awareness is accompanied by a concrete solution that makes life easier, such as the mailbox suspicious@safeonweb.be. And finally, recognisable situations are drawn on - such as frustration with long, complicated passwords - that are translated into a humorous concept.

Tangible results

One of the most important results of the past 10 years is that the umbrella platform Safeonweb.be has been developed into a recognisable brand for digital security in Belgium, with clear, easily accessible information and testimonials. Research has shown that 82% of the public is now aware of safeonweb.be as the reference for cybersecurity. The name recognition of this brand has therefore outgrown CCB.

44% of Belgians say they have already reported a suspicious e-mail or SMS to suspicious@safeonweb.be. The system receives more than 9 million notifications every year. As such, the CCB's goal is achieved: involve the public as much as possible, as the first and most important target audience to enhance cyber resilience.

ACCOLADES

THE EUROPEAN PRESIDENCY 2024

In the first half of 2024, Belgium assumed the rotating presidency of the Council of the European Union. During this period, the CCB took on international responsibilities and played a leading role to promote Belgian priorities. There was a strong focus on cybersecurity during the presidency. It was a unique opportunity to put Belgium on the map as an international pioneer in this field.

One of the top priorities was the negotiations between the Council of the European Union (the meeting of the competent ministers), the European Parliament and the European Commission on two legislative initiatives: the Cyber Solidarity Act and an amendment to the Cybersecurity Act (from 2019). The Belgian delegation, composed of the Permanent Representation to the EU and experts from the CCB, successfully reached a political agreement on both Acts in record time, before the deadline for the European elections in June 2024.

In 2019, the **EU Cybersecurity Act** laid the foundation for a European certification system for cyber-secure products, processes and services. This meant that one certification was valid for the entire union. An amendment to this act was voted on during the Belgian presidency. This included adding providers of managed security services (such as security audits, penetration testing or incident response) to the certification system. Thanks to this certification, customers of these service providers get more guarantees in terms of quality and reliability. It also allows them to verify their supply chain.

The **Cyber Solidarity Act** came into force in early 2025. It included the implementation of a European warning system for large-scale cyber threats. This system brings together the competencies of national and cross-border cybersecurity centres with the goal of detecting, analysing and responding to attacks. This exchange of information across borders is fundamental to successfully combating large-scale cybercrime operations, with a coordinated approach.

The EU also decided in this Act to develop a joint mechanism for emergency situations. This involves actions in three areas:

- heightened preparedness to be able to respond in key sectors such as finance, energy and health care. Organisations from these sectors should be tested for weaknesses that may be vulnerable to cyber-attacks.
- setting up an EU Cybersecurity Reserve, consisting of a range of selected private sector providers. EU Member States or institutions (and even non-EU countries) can then claim from this reserve to help deal with large-scale incidents. In the summer of 2025, the agency ENISA was mandated to make this operational at the European level.
- establishing mutual assistance: a member state stricken by a cybersecurity incident can count on support from the other member states.

To bolster cooperation between the various actors in the 27 member states, the CCB organised the Brussels Cybersecurity Summit in January 2024. The summit brought the Belgian ecosystem together with representatives of cybersecurity ecosystems from the rest of the EU - across different fields of action: technical, strategic and finance experts. Another new aspect was that the directors of national and regional cybersecurity authorities met at an informal summit.

Brussels Cybersecurity Summit (2024)

Another realisation was **EU-CyCLONe**, the organisation that acts as a liaison between the national authorities of member states for managing a cyber crisis. This body was set up in the wake of

the NIS2 directive. During the Belgian presidency, the first procedures and rules were agreed upon within EU-CyCLONe, on the exchange of information and the coordination of interventions. These procedures, and CCB leadership, were tested immediately during the European elections in 2024 and also during the 'Cyber Europe' exercise, one of the largest international exercises in cyber incident management.

In addition to EU-CyCLONe, the CCB also chaired two other European networks. Firstly, the NIS Cooperation Group, where member states come together to shape the implementation of the NIS2 directive, thereby ensuring essential services in the EU. The CCB set the tone at the Group, by being the first European member state to transpose the directive, among other things. The CCB also chaired the European Computer Security Incident Response Team (CSIRT) Network for 18 months, where the technical 'fire crews' of cyber incidents consult with each other.

Under the aegis of the CCB, a comprehensive review and inventory of the cybersecurity landscape in the EU was also carried out. The resulting Council conclusions on the future of cybersecurity, summarised in a text entitled 'Implement and Protect Together', were formally adopted by all European telecommunications ministers, after negotiation. In the document, the 27 member states called for less legislative fragmentation, clearer roles and responsibilities, closer cooperation with enforcement agencies and a greater focus on Active Cyber Protection, among other things. As a result, the focus of European policy was de facto shifted to implementation rather than new legislation. In this way, some of the spearheads of the CCB were also endorsed at the European level.

International recognition

Belgium received unanimous praise at the end of its European presidency in late June 2024. The accomplishments in the cyber domain had also contributed to this success. The cross-cutting approach and transparent way in which the representatives of the CCB had prepared dossiers together with the Permanent Representation to the EU was greatly appreciated. Their enthusiasm and efforts to unite experts and policy makers around concrete achievements paid off.

As a result, the centre grew into a respected and authoritative voice at the European level. This generated a lot of interest in the Belgian cybersecurity strategy and the various projects within the Active Cyber Protection concept. The approach devised by the CCB is therefore finding inroads elsewhere:

- The Active Cyber Protection concept is recognised by the EU as best practice, in alignment with the NIS2 Directive (increased cyber resilience in critical and essential sectors).
- The CyberFundamentals framework has since been adopted by several countries, as well as private companies.
- Spear Warnings: various cybersecurity agencies are looking at setting up a similar warning system in their own countries.
- Belgian Anti-Phishing Shield: the United Kingdom has implemented a similar system for its government departments, the French data protection authority and the cybersecurity centre ANSSI are looking into developing a French version, and at the European level there is interest in a wider rollout.

Another illustration of the CCB's reputation is the global community it now reaches through its online Connect and Share events. Since 2020, more than 8,000 IT and cyber professionals from 70 countries have participated in these sessions. They cover both technical and strategic topics. International keynote speakers willingly make contributions.

Awards

Belgium has undeniably become a pioneer in cyber protection over the last 10 years. The ambition to make our country one of the least cyber-vulnerable countries in the EU has been achieved. Comparative studies and international rankings bear this out.

Through the CCB's work and coordination with national partners, Belgium is ranked among the top 10 in reputable cybersecurity indexes including the **National Cyber Security Index** (NCSI) and the EU Cybersecurity Index. In the **BitSight EU Ranking**, Belgium is in the top three.

The International Telecommunication Union (ITU) is the United Nations agency for information and communications technology. Its **Global Cybersecurity Index 2024** identified Belgium as a Tier 1 role model for Europe. This study examines 5 areas (Legal, Technical, Organisational, Capacity Development and Cooperation). Belgium achieves an overall score of 96.81 out of 100, outperforming the European and global average on all pillars.

This is international recognition of the efforts made by the CCB and the Belgian cybersecurity ecosystem as a whole.

Belgium's annual awareness campaigns have also been in the international spotlight: in 2022 and 2024, the video of the annual awareness campaign was awarded a European Cybersecurity Award for the best awareness video.

In 2023, the Spear Warning project won a Publica Award

"Belgium has undeniably become a pioneer in cyber protection over the last 10 years. The ambition to make our country one of the least cyber-vulnerable countries in the EU has been achieved. Comparative studies and international rankings bear this out."

CCB IN THE WORLD

Ten years after the CCB was established, ensuring the cybersecurity of our country, its citizens, businesses and public institutions remains a challenge. Technological advances, the professionalisation of cybercriminals and geopolitical developments have led to a sharp increase in the number of cyber attacks and the emergence of new forms of fraud. As the national coordination centre, the CCB is monitoring the situation closely.

CURRENT THREATS VERSUS 'OLD' THREATS

The threat landscape has continued to evolve in recent years. More than anything, the methods used by criminals and state actors have changed. We can broadly distinguish three major groups, each of which has its own methods.

Which threats are there?

ORGANISED CYBERCRIMINALS

Whereas cybercrime used to be mainly the work of individual hackers, today we see internationally organised groups working according to a sophisticated business model. Ransomware attacks, where data is encrypted and only released after a ransom is paid, have grown into a billion-euro industry. The attacks are also much more focused today.

A widespread attack, such as Wannacry, in which hundreds of thousands of computers around the world were held hostage for a short time, is less frequent today. Ransomware attacks are now better prepared and are specifically targeted at a particular victim or groups of victims.

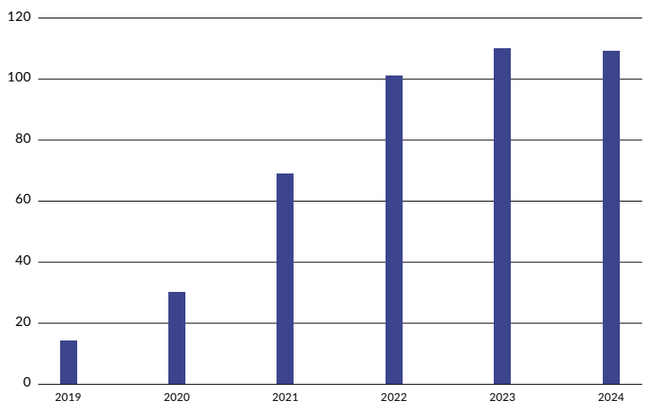
At the same time, technological evolution has also made it easier to carry out a ransomware attack. Ransomware-as-a-Service (RaaS) is when cybercriminals offer a complete ransomware package to other criminals. In this way, malign actors no longer need to have an IT background to successfully target an organisation, with the result that attacks are much more widespread and frequent.

HACKTIVISTS

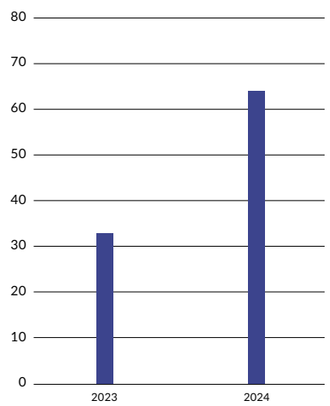
Hacktivists carry out attacks from ideological or political motives. Their main goal is not financial gain, but to disrupt a society's democratic processes or disseminate a message.

In most cases, they use DDoS attacks, in which websites or online services are rendered temporarily inaccessible by being overloaded. In the short term, the impact is usually limited, but the symbolic value can be significant. A lot depends on the geopolitical situation and any tensions, which lead to spikes in these attacks. The modus operandi has remained largely the same over the years.

Evolution of ransomware



Evolution of DDOS



STATE ACTORS

State actors act on behalf of a state. They have different goals from those of hacktivists and criminal groups. They have more resources, highly sophisticated technology and operate extremely discreetly. Their goal is usually strategic: to capture sensitive information or technology and penetrate critical infrastructures.

While the number of visible incidents still seems rather limited, that does not mean these attacks do not take place. On the contrary, precisely because these attacks often remain under the radar, their real impact is difficult to assess. Moreover, state actors sometimes use criminal groups as cover, so it is not always clear exactly who is behind the attack.

Frequency: from sporadic to daily

The number of cyber incidents has undeniably increased in recent years. Where ransomware and phishing regularly appeared 20 years ago, they are now a daily reality. That is because the threshold for carrying out an attack is lower. There has been an explosion of actors as a result.

Moreover, we see that attacks are coming in quicker succession. As a result, the threat menace is structurally higher than a few years ago. Cyberattacks are therefore no longer the exception, but a fact of life that every organisation has to take into account.

Where criminals strike today

Many of the cyber-attacks in 2025 have been opportunistic: criminals look for a weak link and strike when they see their chance. Yet clear patterns are emerging. Government agencies, grid operators, and financial institutions are still targeted in particular, not only because they possess valuable data, but also because they are symbolic targets.

Knowledge institutions and technology companies are also more frequently targeted for theft of intellectual property, sensitive research results or technological know-how. Industry and the logistics sector are also at higher risk. Attacks in these sectors can disrupt production processes, hamper supply chains and cause significant economic damage.

Cyber as a geopolitical weapon

Geopolitical tensions have emerged in the digital domain, and the growing rivalry between international power blocs has noticeably increased the number of cyber-attacks with (geo)political motives. In the process, states themselves are increasingly using cyber sabotage and cyber espionage as an extension of their foreign policy.

Cyber has therefore become a weapon in its own right: it can disrupt a country, strain critical infrastructure and expose confidential information.

One striking aspect is that the lines between criminal groups and state actors are becoming increasingly blurred. Criminals sometimes operate at the behest of a regime, and states sometimes use existing networks to cover their tracks. The result is a threat landscape in which geopolitics and cybercrime are increasingly intertwined.

The impact of new technology: AI and quantum

New technologies pose a threat, but at the same time offer opportunities. AI is an excellent example. For example, criminals are increasingly using AI to make phishing emails more convincing, generate fake images or videos (deepfakes) and automate attacks. The scale and speed at which this is happening is making detection more difficult. At the same time, AI can just as easily be an ally: technology that helps identify attacks faster, understand patterns and make defence systems smarter and more efficient.

While AI primarily represents a breakthrough in software, quantum technology will revolutionise hardware. When quantum computers are perfected, their unprecedented computing power will be able to crack traditional encryption and coding in a short time. Researchers are therefore already working intensely on quantum-proof solutions such as post-quantum cryptography. For now, it is still difficult to predict when this technology will mature and how far-reaching the consequences will be.

Staying vigilant for new breakthroughs while continuing to invest in research and expertise is therefore essential. Whoever manages to harness the power of AI and quantum in time will have an edge in a digital world that continues to accelerate.

Belgium at the forefront of Europe's digital security

As a relatively small country, Belgium can justifiably call itself a pioneer in cybersecurity today and is among the leaders in Europe. And that is no coincidence: our strength is a pragmatic and results-oriented approach, where other countries sometimes still get bogged down in endless procedures and bureaucracy.

> "The difference between past and present is not in the type of attacks, but rather in the professionalisation, scale and intertwining with geopolitical, criminal and ideological motives. Whereas with WannaCry and NotPetya the world saw how disruptive a cyberattack can be, today we see that attacks are more subtle and targeted."

A telling example is the way we transposed the NIS2 directive into a national framework. The Early Warning System (EWS) developed by the CCB to rapidly detect and share threats is also regarded as a success story. And the CyberFundamentals framework that provides tools for better cyber protection is attracting international interest.

Cybercrime is still a clearly international phenomenon. An attack on our infrastructure could have far-reaching consequences elsewhere. Europe is therefore still the primary framework for coordinating the fight against cybercrime and digital threats. Through joint projects, information sharing and networking, the national and regional ecosystems reinforce each other. Our country has consciously chosen to take a leading role in this European story.

CENTRE FOR
CYBERSECURITY
BELGIUM 10Y

https://ccb.belgium.be