CENTRE FOR
CYBERSECURITY
BELGIUM

ACTIVE CYBER PROTECTION (ACP)

Policy document, March 2026

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

Table of contents

Table of figures

Table of tables

1. Vision for the Future

The world is only at the start of the digital transition. To benefit fully from the opportunities that this transition will offer our society and economy, it is vital that our citizens, businesses and governments can maintain trust in the digital domain. To ensure such trust, cybersecurity is crucial.

In recent years, much national and international effort has been directed at improving the cybersecurity of organisations and potential victims. However, while these efforts are essential to bolstering a country's resilience, recent trends indicate that such efforts may be insufficient, as cybersecurity incidents, cybercrime, and online fraud continue to rise. According to the Centre for Cybersecurity Belgium (CCB), the cause for this rise are vulnerabilities: both human and technical vulnerabilities. As a national cybersecurity agency, we see it as our job to assist organisations and citizens in overcoming these vulnerabilities.

Over the course of the last years, the CCB has therefore developed several projects to address these vulnerabilities via a more proactive approach, which we group under **the concept Active Cyber Protection (ACP)**. An important policy step was achieved when the NIS2 Directive officially included ACP as a legal requirement in the definition of national cybersecurity strategies. Consequently, it is now imperative for EU Member States to integrate policies in their national cybersecurity strategies that implement ACP as part of a comprehensive preventive and resilience strategy. This development underscores the importance of proactive measures in safeguarding cyber infrastructure and ensures the security of digital communication across the EU.

The CCB is strongly convinced of the opportunity to promote ACP, to public and private stakeholders, in Europe and beyond. In this guide we wish to outline our understanding of the ACP concept and to share some of our experiences, if they can be to the benefit of others and if they could foster collaboration.

Cybersecurity is not a project, it is a journey.

2. Introduction

The concept of Active Cyber Protection (ACP) is referenced – for the first time legally – in the *EU Directive 2022/2555 concerning measures for a high common level of security of network and information systems across the Union*, the so-called NIS 2 Directive, recital 57 and article 7.

The directive specifies that "*as part of their national cybersecurity strategies, Member States should adopt policies on the promotion of active cyber protection as part of a wider defensive strategy.*"[1] The previous NIS 1 directive already required Member States to adopt national cybersecurity strategies, outlining strategic objectives and priorities. Since the adoption of NIS 2, Active Cyber Protection (ACP) has become a key element in the implementation of National Cybersecurity Strategies. Yet, as transposition efforts continue across the EU, a common definition and operational understanding of ACP have not fully crystallised.

Recital 57 of NIS 2 describes ACP as:

> ***"Rather than responding reactively, active cyber protection is the prevention, detection, monitoring, analysis and mitigation of network security breaches in an active manner, combined with the use of capabilities deployed within and outside the victim network. This could include Member States offering free services or tools to certain entities, including self-service checks, detection tools and takedown services. The ability to rapidly and automatically share and understand threat information and analysis, cyber activity alerts, and response action is critical to enable a unity of effort in successfully preventing, detecting, addressing and blocking attacks against network and information systems. Active cyber protection is based on a defensive strategy that excludes offensive measures."***

The Centre for Cybersecurity Belgium (CCB) developed the notion of ACP well before the NIS2 act was published and has therefore many years of experience in this domain. **In this policy document the CCB wishes to outline its understanding of ACP and share best practices in its implementation**.

[1] As mentioned in recital 57 of Directive (EU) 2022/2555 concerning measures for a high common level of security of network and information systems across the Union.

The CCB considers ACP as a proactive, tailored, automated and participative approach to cybersecurity.

Table 1 Characteristics of the CCB approach to ACP

Proactive	Rather than just reacting to attacks, ACP entails a proactive search for potential threats, vulnerabilities, vulnerable systems and fraud campaigns, before they can be widely exploited and executed. Thereby ACP supports a stronger prevention of cybersecurity breaches in organisations.
Tailored	Because there is no "one size fits all" solution, ACP promotes customised solutions taking into account the different needs and cyber posture of stakeholders, from individuals and small organisations to large firms and public administrations, tailored to their sector and system set-up. Rather than broadcasting warnings, ACP encourages information sharing or service offering per stakeholder only of what is relevant to them, to avoid information overload.
Automated	In a rapidly changing cybersecurity landscape, speed is essential. Automated solutions, preferably at scale, need to be developed to protect systems from increasingly equally automated attacks. Such automation and scalability in the protection can also help overcome the increasing cybersecurity skills shortage.
Participative	ACP encourages an active involvement of all actors, from individuals to large organisations, in identifying and fixing vulnerabilities. Not just their own, but those of the entire society. Instead of a single weak link being enough to enable an attack, ACP aims to turn vigilance into a collective defensive asset: one vigilant citizen or organisation can help protect many others.

Accordingly, the CCB emphasizes the active aspect of the ACP. This means that, as the national CSIRT, it seeks to **actively go out to involve and assist users in strengthening their own digital environment, and in dynamically shoring up their trust in the digital domain**.

This mindset is structured around a clear operational model. The four characteristics - proactive, tailored, automated and participative - define how the CCB approaches cybersecurity. This approach is then applied through - currently five - operational pillars. The concrete projects under each pillar demonstrate how ACP is translated into practice.

3. The Current Project Pillars of Belgium's Active Cyber Protection

The CCB views ACP as a central framework guiding its proactive protective strategy. **The core mission of the CCB is to make Belgium one of the least cyber vulnerable countries in Europe**. To achieve this goal, the CCB **develops, along ACP principles, national projects that address cyber threats, such as malware and phishing, as well as the underlying technical and human vulnerabilities they exploit.**

These **projects are currently grouped along the lines of five operational pillars**: identify and take down malicious infrastructure, user involvement, spear warning, cybersecurity as routine and validated service providers.

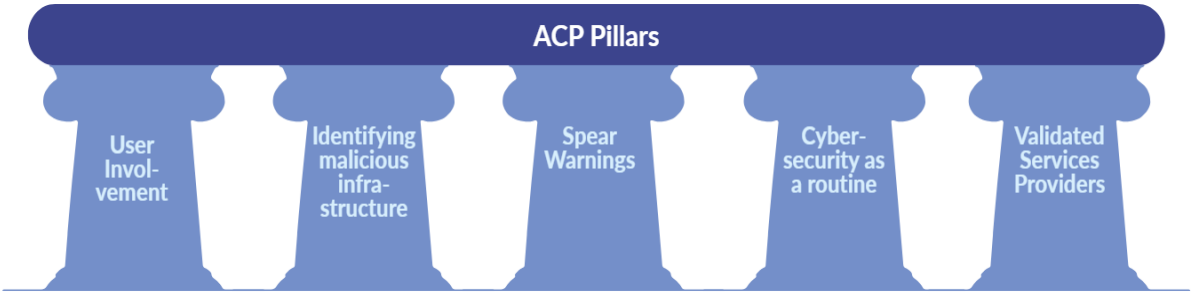

Figure 1 CCB's current ACP operational project pillars

Before discussing these pillars more in detail, it is important to clarify that the **CCB approach to ACP does not aim to be a static endeavour with a finite goal; instead, it is a fluid and progressive effort**. Constantly being revised and honed, it is seen as an ongoing journey rather than a task with a finishing line.

Pillar I – Identify And Take Down Malicious Infrastructure

Infrastructure segmentation projects entail the systematic **identification** of infrastructure that is used by malicious actors, with the objective of **providing timely warnings** about such infrastructures.

One of CCB's pivotal initiatives under this project pillar is the **Belgian Anti-Phishing Shield** (BAPS) - see the respective Annex for more details. Launched in 2021, BAPS operates by issuing warnings for malicious websites at the Belgian DNS level, thereby aligning with the dimension of "active mitigation" outlined in NIS 2.

The project is set up to identify malicious links, and then redirect any Belgian user – customers of the major Belgian Internet Service Providers (ISPs) – away from that page. The CCB maintains a list of suspicious links and if a website requested by an internet user is on that list, the user will be redirected to a warning page. Collaboration with the Belgian ISPs, trusted partners and the public prevented no fewer than 185 million clicks to suspicious websites in 2025 alone, equivalent to around 352 warnings per minute for Belgian internet users.

The project is thereby proactive, automated, tailored, and – as Pillar II demonstrates – it is also participative.

A recent, related initiative under this pillar is called **AdChain**, a national infrastructure, and a clear example of public-private partnership, designed to detect, analyse and disrupt **fraudulent online advertisements**. In response to the growing use of malicious advertisements in investment fraud and other scam campaigns, AdChain enables faster detection, structured risk scoring and coordinated follow-up with public and private partners. By combining technological detection capabilities with validated expert intelligence, it strengthens fraud signal exchange, accelerates disruption efforts and helps reduce financial harm to citizens.

To strengthen the identification of victims linked to malicious infrastructure, the CCB has started to implement a targeted **Metadata communication Project**. The initiative focuses on requesting and analysing limited metadata related to confirmed malicious IP addresses — in particular command-and-control (C2) servers — this in order to warn Belgian victims. This legally supervised approach enhances Belgium's capacity for early detection and targeted victim notification, thereby reducing the impact of serious cyber threats on citizens and national infrastructure. (see Annex for more information).

Pillar II – User Involvement

As expressed in the Belgian cybersecurity Strategy, all users remain ultimately responsible for the protection of their own systems, yet we should all work together to do so. Cyber Agencies should therefore pro-actively inform and support users and **involve them to engage** in their own protection. Moreover, users should be encouraged to **contribute to collective security**.

Projects grouped around the pillar of user involvement therefore focus on building trust with the Belgian population (i.e., media, users, companies, citizens) and spread awareness on

cybersecurity. These projects are branded under the "SafeOnWeb" name, targeting both the public (@Home) and organisations (@Work).

- **SafeOnWeb@Home** uses a mix of communication tools to quickly inform Belgian citizens and advise them on online security and digital threats to reduce the likelihood of falling victim to scammers and cybercriminals.
    - The www.SafeOnWeb.be website provides continuous access to cybersecurity advice. This is also done via social media channels, press and our 600+ partners during our annual awareness campaign, representing all sectors - public, private, academic – and advertisement (owned, earned and paid).
    - Part of the SafeOnWeb's set of services is the SafeOnWeb mobile app to quickly inform internet users of new phishing attempts and to send out new security tips (See Annex for more details).
- **SafeOnWeb@work** ensures that also Belgian **businesses** are ready to compete in an increasingly digitalised world. In fact, by digitising their organisation and production methods, Belgian companies have been able to reduce their investment costs, optimise their processes and get closer to their customers. As a backlash to this exponential transformation, increasingly connected and interdependent systems are broadening the vulnerable surface of organisations and creating new challenges: implementing cybersecurity measures to protect their activities and investments.

  Therefore, and building on the success and recognition of SafeOnWeb.be for the public, the CCB launched a specialized platform SafeOnWeb@Work in November 2023 (https://atwork.SafeOnWeb.be/). Via this platform, Belgian companies and organisations can register their domains and IP ranges to benefit from the SafeOnWeb@Work services. The SafeOnWeb@Work platform builds on the existing Early Warning System and offers a light version so that not just Organisations of Vital Interest, but all companies can receive alerts based on the technical information they have registered.

  On this portal, organisations are able to make maturity assessments, and find various advisory documents, tools, support, templates, and references to help them raise their cybersecurity level. (See Annex for more details.)

One of CCB SafeOnWeb flagship projects in the fight against phishing is the **BePhish project (see Annex)**. For many years now, the CCB has been able to rely on the participation of the public through the notification of suspicious messages. In 2017, the CCB created the email address suspicious@SafeOnWeb.be (in four languages) to which citizens can forward suspicious messages (emails or text messages). In 2025, we received an **average of 27,000 messages per day**. In total, 9.9 million messages were forwarded to suspicious@SafeOnWeb.be.

This project is first of all a successful **method in awareness, by making users take concrete**

actions when they see a threat. Such activation has been proven to work better and last longer in making users aware than simple information. However, with such big numbers of received messages, BePhish is also a very effective method of **crowd-sourcing on active phishing campaigns**. The forwarded messages are indeed used to support other initiatives, such as **BAPS** but also the **SafeOnWeb App,** as mentioned above.

In 2024, SafeOnWeb adapted several well-known fairy tales, integrating key lessons on safe internet use into each story. This creative approach was well received by the European jury and was awarded at the **ECSM Awards**. The ECSM Awards recognise successful and/or innovative cybersecurity awareness campaigns and promotional materials developed by EU Member States.

Pillar III – Spear Warning Process

An important part of ACP involves **real-time threat detection**. Timely identification enables organisations to respond swiftly, thereby minimizing potential damage.

In order to help organisations in this regard, the CCB seeks to track methods of malicious actors, but intervene before these can act. Whereas Spear Phishing is successfully used by malicious actors to send targeted messages to individuals in order to get into their systems, the CCB uses the same approach but then with the goal of protection, warning and helping organisations pinpoint vulnerable systems.

As part of its overall mission, the CCB systematically collects information on vulnerable systems, encompassing threats, vulnerabilities and intrusions. The centre maintains a list of the most **likely to be exploited vulnerabilities** in Belgium. Next, the CCB scans Belgian Cyberspace to detect if and which systems might be vulnerable to these vulnerabilities. Subsequently, the CCB proactively seeks to identify the owners of these vulnerable systems. Upon identification, the CCB initiates an **individual and tailored spear warning** to the owner of the vulnerable system be it electronically or via regular post, and directly to the CEO (which increases uptake).

This approach reduces an organisation's attack surface making it more difficult for potential attackers to exploit system weaknesses.

The spear warning process unfolds in four distinct phases: prioritization; scanning; identification; warning and informing. In detail:

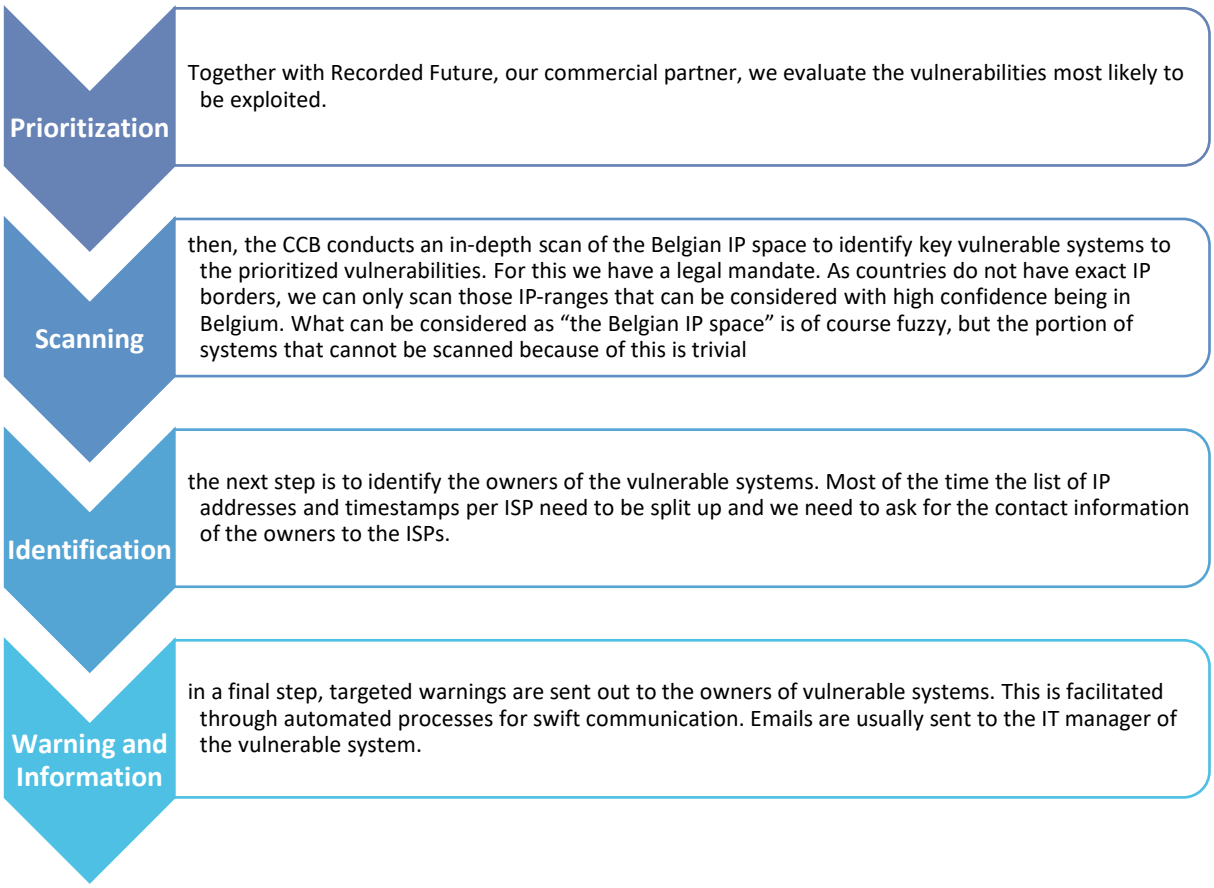

Figure 2 The four distinct phases of the Spear Warning process

The CCB has noticed the impact a direct, targeted and tailored notification has when written by the national authority for cybersecurity versus a generic warning about a vulnerability. Though still not all warned owners apply the necessary and urgent software updates immediately. Quite often, actively exploited vulnerabilities remain unpatched for too long due to a lack of urgency felt at the IT manager's level. This is why the CCB also sends out letters signed by the Director General of the CCB on paper to the CEO, or other legal representative, of the organisation.

In **2025, 32,000 spear warnings were sent to Belgian organisations and individuals**. Moreover, as the cyber threat landscape is always evolving, besides the warnings for vulnerabilities, CCB started to send out warnings also on leaked credentials and for malware infections that might lead to significant damage. This kind of infection often leads to ransomware attacks. Therefore, it could be assumed that thanks to this campaign, CCB was able to prevent some ransomware incidents, although we will never know how many exactly.

Considering these figures, and actions, it does not come as a surprise that the Spear Warning Project was awarded the first place of the Publica Awards in 2023, in the category "security & safety".

Another flagship initiative under this pillar is the **Early Warning System (EWS, see Annex).** This initiative is tailored to provide warnings to Organizations of Vital interest (including NIS2 essential entities) and Organisation of Special Interest at the national level in Belgium.

In addition to vulnerability- and credential-based warnings, the CCB operates the National **Anti-DDoS Project**, also referred to as the **"Red Button" initiative**. This project focuses on the monitoring, early detection, and prevention of Distributed Denial-of-Service (DDoS) attacks targeting Belgian organisations (see Annex for more information). The project is built on a structured threat intelligence and analysis model in which incoming signals are assessed and assigned varying confidence levels. By combining intelligence feeds, technical monitoring, and contextual threat analysis, the CCB is able to distinguish between low-confidence indicators and credible, imminent threats. When a sufficiently high confidence level is reached, targeted warnings are issued to potentially affected organisations, enabling them to activate mitigation measures before or during an attack.

Pillar IV – Cybersecurity As A Routine

Just as fire safety or intrusion security is a default part of an organisation's security routine, the CCB believes **cybersecurity standards and norms should be part of every organisation's security routine as well**.

Just as for fire safety or electricity compliance, such routine can best be set up via a label or certification framework.

For those organisations who are already under strict regulatory cybersecurity requirements, implementing cyber protection measures can aid in meeting their compliance standards. For those organisations where cybersecurity requirements are not mandatory, building a routine with standard norms, controls, labels, and certifications will help them augment their level of cybersecurity. The CCB therefore developed the **CyberFundamentals framework (CyFun®)**, in order to introduce standard security norms, external controls, and certifications for all stakeholders at all levels. **With CyFun® cybersecurity can be made into a routine**.

In Belgium, CyFun® has been accepted as a **national label and certification scheme**. It is also **included in the NIS2 law** as a possible by default instrument for **presumption of compliance**. Additionally, organisations can secure their **supply chain** by requiring suppliers to have a CyFun® label or certificate. In future, it could assist in supporting appropriate **Cyber Insurance**.

To facilitate international use, no specific references were included regarding national legislation. The framework has already been formally adopted, and is co-owned by at least three other EU Member States: Romania, Malta and Ireland, demonstrating its international capacity.

CyFun®is built around six core functions: govern, identify, protect, detect, respond, and recover.

- **Govern:** Ensures that cybersecurity is treated as strategic priority, not just a technical issue. It sets clear expectations, policies, responsibilities and authorities, and makes sure these are communicated and reviewed across the organisation.
- **Identify:** Helps build a clear understanding of what matters most to the organisation, such as systems, people, assets, data, and the processes and tools that support operations. This function helps recognize potential cyber threats and lays the foundation for informed decisions about managing cybersecurity risks.
- **Protect:** Involves putting safeguards in place to reduce the chance of a cyber incident or limit its impact. Thi includes technical measures, processes, and awarenes efforts.
- **Detect:** Supports the ability to notice cybersecurity events quickly. Early detection helps reduce harm and allows for faster response.
- **Respond:** Covers the actions taken when a cybersecurity incident occurs. It help contain the issue, coordinate communication, and reduce disruption.
- **Recover:** Focuses on restoring affected services and operations after an incident. It also includes learning from the event to improve future resilience.

An additional toolbox was created to guide organisations in choosing their appropriate protection level and assist in the implementation of the framework.

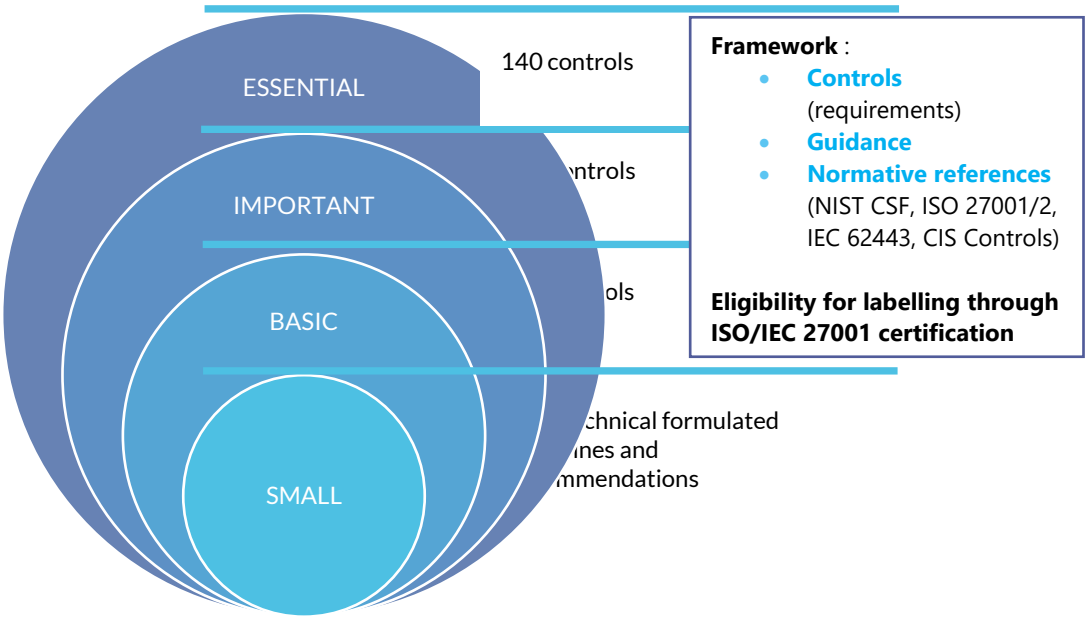

Figure 2 Overview of the CyberFundamentals Framework

Based on CCB historical data, retro-fitting was done on successful cyber-attacks using anonymised data. The conclusion is that: measures in assurance level basic were able to cover 82% of the attacks; measures in assurance level important were able to cover 94% of the attacks; measures in assurance level essential were able to cover 100% of the attacks. Based on these attacks, key measures were identified at each level to prioritize the countermeasures to

protect against the known cyberattacks relevant for that assurance level. (For more information see Annex.)

Pillar V – Validated Service Providers

The internet offers users **anonymity**. This is one of its great success factors. However, the concept of anonymity is a double-edged sword. While it can foster a sense of liberation, it also has the potential to boost malicious activities. Without **accountability**, individuals might exploit anonymity to engage in harmful activities.

This led to a growing need for some **validation** to counteract these negative aspects. As fraud prevention technology gets more sophisticated, account takeover tactics are keeping pace. According to researchers, account takeover attacks are still rising, representing a problem when it comes to monetary losses and the unquantifiable **loss of credibility and customer trust**.

Moreover, recent technologies, such as **generative AI**, exponentially fuel previous techniques such as ever more believable social engineering, phishing and other types of attacks, giving cybercriminals an unparalleled access to personally identifiable information, allowing them to start an account takeover. **It becomes increasingly difficult to distinguish real from fake interaction.** This is why **authenticity** becomes more and more complex to prove.

It is this specific conundrum – how to make sure that what appears online is safe and validated – that led the CCB to start wondering how to ensure that online presence can be secured. Because of the rise in the number of fraudulent websites used for phishing purposes, the CCB created the **Validated service providers pillar of ACP.**

One of the fundamental aspects of a safe online environment is seeking the **balance between anonymity and validation**. It is important that **the freedom anonymity provides, does not oppose the increasing need for validation online for security purposes**. It is equally important to introduce layers of liability and accountability to provide validated services. Validation mechanisms should be implemented where personal/sensitive/critical information is used, for both privacy and security reasons. **Digital identities linked to real credentials** can deter malicious actors and establish an environment of trust and credibility.

With the Validated sites project, CCB developed a **browser plugin** to assess and indicate to users the level of reliability of websites they visit. With a 3-level colour code the plugin tells users whether the site they are visiting is safe to leave personal data (Green), only safe to consult information (Orange) or is known malicious (Red). The plugin isavailable on laptops and desktop and aims an 90% green light experience in Belgium when surfing online (see Annex for more details).

The CCB further wishes to leverage the potential of digital identity, and engage with the opportunities that are present in the Revised EU eIDAS Regulation, which encourages the use of Digital Identity all across the Union.

4. Conclusions and way forward

Cybersecurity is not a project, it is a journey. It is an ongoing process that demands continuous adaptation, and collaboration. In today's interconnected world, cyber threats are constantly evolving, requiring a dynamic and proactive approach.

Organisations and individuals must not view cybersecurity as a one-time endeavor with a defined endpoint but rather as an ongoing expedition towards resilience and preparedness. This policy document provides insight into the strategic framework adopted by the CCB, emphasizing the importance of **proactive, tailored, automated and participative projects, demonstrated along the five current pillars.**

Consequently, the **CCB recognizes the significant role of national cybersecurity agencies taking proactive measures and supporting users in identifying and rectifying vulnerabilities before succumbing to cyber threats**. Acknowledging the regulatory obligations delineated in the NIS 2 Directive, and the comprehensive definition of ACP, **the CCB emphasises that this endeavour cannot be pursued in isolation**. Agencies need to work together across borders, not just with the private sector, but with each other, underlining the essential **international dimension of ACP initiatives.**

In particular, cyber-enabled fraud has emerged as one of the most visible and damaging consequences of digital insecurity. By integrating fraud prevention and disruption into the ACP framework, Belgium reinforces its commitment to protecting not only networks and systems, but also citizens' financial security and trust in the digital environment.

In light of all these perspectives, the **CCB extends invitations to international partners, encompassing both public and private sectors, to engage in the endeavours and collectively brainstorm innovative strategies**. The CCB encourages all interested parties to reach out, expressing interest in collaborating or sharing information on the principles articulated in this document.

Interested parties are already encouraged to **explore the Annexes** to this document, where detailed information regarding CCB ACP specific projects is provided. This Annex serves as a succinct repository for best practices and offers avenues for potential cooperation. Interested stakeholders can gain insight into CCB ongoing initiatives, facilitating exchange of expertise and resources. The annex thus becomes a vital resource for those seeking to deepen their engagement with the ACP framework as translated by the CCB and contribute to its objectives of enhancing cyber resilience on a national and international scale.

By fostering an environment of collaboration and shared expertise, **Belgium aims to bolster its cyber resilience and contribute to the global efforts in combating cyber threats**.

Annex

THE BELGIAN ANTI PHISHING SHIELD (BAPS)	
Webpage	https://baps.safeonweb.be/en/baps
Aim	To reduce the click-rate of malicious websites in the Belgian cyberspace.
Project	The Belgian Anti Phishing Shield (BAPS) was launched in 2021 to warn internet users about malicious websites at the Belgian DNS level. If the requested website by an internet user is on a list with suspicious links - maintained by the CCB - the user will be redirected to a warning page.
How it works	BAPS is built on the BePhish project (see below). Suspicious weblinks are sent to the CCB via the email address suspicious@SafeOnWeb.be. It is also possible to send a screenshot of a fraudulent SMS and QR code messages. Our technology is able to detect URLs in images and QR codes. Domains are checked for content and end up on the so-called "BAPS list" with malicious websites if no content can be found. Suspicious URLs are passed on to Google Safe Browsing and Microsoft SmartScreen. The browsers then use this information to warn internet users about malicious websites. Since the CCB has no control over the speed at which Google and Microsoft react to this list of malicious links, the CCB and the Belgian Internet service providers Belnet, Proximus, Telenet and Orange developed a procedure to warn internet users in real time: every time a user clicks on a link, a DNS request is sent to the Internet Service Provider (ISP). Thanks to BAPS, the DNS server of the ISP compares the requested website with the list of malicious websites. **If the requested website is on this list, the ISP's DNS server will redirect the user to a warning page**. The list of malicious websites is again fuelled by the forwarded messages received via the BePhish project.
Figures	Collaboration with the Belgian public prevented no less than 185 million clicks to suspicious websites in 2025, or about 352 warnings to Internet users per minute.

EARLY WARNING SYSTEM (EWS)	
Webpage	https://ccb.belgium.be/cytris/early-warning-system
Aim	The Early Warning System (EWS) aims to strengthen the cyber resilience of Belgian organisations of vital or special interest, by providing continuous monitoring, tailored threat intelligence, and proactive alerts on emerging cyber threats.
Project description	The EWS is the flagship CTI platform of the CCB, designed for the most vital organisations in our country. It offers a centralised environment where onboarded organisations receive threat intelligence, alerts, and strategic insights about their security posture. Unlike standalone warning systems, EWS is a comprehensive service platform combining monitoring, reporting, community engagement, and personalised alerts

	(including spear warnings).
How it works	Vital Organisations are invited by the CCB to register in the EWS portal, create an account and provide relevant organisational and technical information (e.g. domains, IPs, contacts, sector). CCB analysts continuously compare this data with intelligence from trusted partners and internal sources. When threats are detected, organisations receive tailored, actionable alerts. The platform includes: • a portal with reports and alerts • Continuous CTI monitoring and analysis • Attack surface ratings to identify vulnerabilities • Connect & Share events for knowledge exchange • Integration of spear warnings (automated and manual) The system acts as an additional layer of protection, complementing organisations' own security capabilities.
Legal framework	The EWS operates under the CCB's mandate to enhance national cybersecurity and support organisations, particularly essential entities those covered by NIS2. It relies on voluntary registration and information sharing, combined with lawful processing of threat intelligence to provide targeted and proportional alerts.
Figures	In 2025, the CCB published 568 reports and 14 Flash Alerts on the EWS portal.

SPEAR WARNING	
Webpage	https://ccb.belgium.be/cytris/faq-on-spear-warnings
Aim	The Spear Warning project aims to proactively detect vulnerabilities and cyber threats affecting Belgian organisations and to directly notify them, enabling rapid remediation and preventing potential cyberattacks and damage.
Project	Spear Warning is a proactive notification service operated by the CCB that identifies vulnerable systems, leaked credentials, and malware infections. Once a risk is detected, targeted organisations are informed directly, allowing them to take immediate action. The project focuses on early detection and fast communication, significantly reducing exposure time and limiting the risk of exploitation.
Legal Framework	One of the most difficult parts of setting up a spear warning service on national level was obtaining all necessary legal provisions. It took the CCB quite some effort to find the right balance and convince political authorities. The CCB now has the legal mission to detect cyberthreats and vulnerabilities that could lead to significant cyberattacks and damage. While respecting proportionality, collecting only information necessary to identify the vulnerability, with the sole purpose of immediately informing the owner of the vulnerable system, the CCB can conduct non-discriminatory and non-intrusive

	scans. Another legislative initiative was needed to allow the CCB to obtain identity and contact information. Thanks to this new legal framework and a constructive collaboration with the Service Providers we can identify and notify most of the companies at risk within a few days after detecting the vulnerability.
Figures	The CCB sent out 32,000 spear warnings in 2025. Depending on the vulnerability we can measure a fast reduction ranging from 50% to 90% within days, rather than weeks or months. The effect is significant, even for older vulnerabilities for which several general warnings have already been published. Besides the warnings for vulnerabilities the CCB also started sending out warnings for leaked credentials and for malware infections that might lead to significant damage.

SAFEONWEB@HOME: SAFEONWEB APP	
Webpage	https://safeonweb.be/en/safeonweb-app
Aim	The main human traits which cybercriminals exploit, are ignorance and gullibility. With this project, the CCB wants to increase awareness on phishing and online swindles amongst the general population by showing that not every message can be trusted and that you can never be entirely sure who sent a message. Sending out a regular and effective warning about immediate threats can make a significant difference without wanting to create fear and excessive distrust.
Project	The SafeOnWeb app is a mobile application for Android and iOS mobile devices. The app sends alerts to users about actual cyber threats in Belgium, in a way comparable to news flash apps. The SafeOnWeb app is provided free of charge for iOS (App Store) and Android (Google Play Store). The app strengthens ACP by enabling rapid, direct communication with citizens when major phishing campaigns or urgent cyber threats emerge.

BEPHISH	
Webpage	https://safeonweb.be/en/what-suspicioussafeonwebbe
Aim	Citizens are encouraged not just to be aware of suspicious mails via our app, but also to undertake action. They can forward suspicious emails or text messages to the CCB email address suspicious@SafeOnWeb.be. This activation of the population keeps their attention to phishing messages longer and more engaged. The aim of BePhish is to further raise awareness about the latest phishing campaigns and reduce and counter as much as possible the success rate of phishing.
Project	The CCB appeals to internet users to forward suspicious messages (emails or screenshots of text-message) to the email address suspicious@SafeOnWeb.be (available in Dutch, French, German and English). From the received suspicious

	messages and URLs the CCB extracts attachments and links. Attachments are analysed in a sandboxed environment. If the analysis shows that an URL is malicious, it is forwarded to Google Safe Browsing and Microsoft Smartscreen. These two lists of malicious websites are used by most browsers to provide a browser-level warning. This way, internet users are warned if they have clicked on a malicious link. Suspicious links also "feed" the BAPS project (mentioned earlier).
Figures	In 2025, 9,929,354 messages were forwarded to suspicious@SafeOnWeb.be, resulting in the detection of more than 185 million suspicious URLs.

SAFEONWEB@WORK	
Webpage	https://atwork.safeonweb.be/ https://atwork.safeonweb.be/
Aim	The SafeOnWeb@Work project aims to raise the level of cybersecurity of all Belgian companies and organisations by providing them with content, tools and services such as vulnerability detection, alerts, templates, advice, and support.
Project	Contrary to the Early Warning System, which is limited to the Belgian Organisations of Vital Interest and on invitation only, The SafeOnWeb@Work platform is open to all Belgian entities. The platform is divided in 2 parts: a website and a portal with secured login. • **The website** is publicly available and gathers tools and services for Belgian companies and organisations to make maturity assessments, and find various advisory documents, tools, support, customizable policy templates to kickstart information security management, self-assessments to identify cybersecurity gaps and references to help them raise their level of cybersecurity both on the short and long-term. • **The portal** has an authentication mechanism based on eID (called "ItsMe" in Belgium) and relies on the Federal Authentication Service (FAS). Once authenticated in the portal, Belgian companies and organisations can fill in their contact information and their network information (domain names, IP addresses, IP ranges). The portal uses a 'light-version' of the existing Early Warning System to send out relevant alerts to registered companies based on the registered technical information. Once registered, users can activate dedicated services such as the Cyber Threat Alerts (receive email alerts if a vulnerability or an infection is detected on their network assets), the Quick Scan Report (a yearly snapshot of the organisation's domain and network identifying threats and describing mitigating actions).

CYBERFUNDAMENTALS FRAMEWORK (CYFUN®)	
Webpage	https://cyfun.eu

Aim	The CyberFundamentals Framework offers a clear, step-by-step approach that helps organisations to protect their data, significantly reduce their risk of the most common cyber-attacks, and their cyber resilience. Implementing CyFUN® can build trust between organisations and also provides support for regulatory compliance.
Project	CyFUN® was developed based on international standards and frameworks in the field of ICT and Industrial cybersecurity. The framework is built on three maturity levels plus a set of key, non-technically formulated guidelines for the smallest entities. It can be used by any organisation, regardless of size, sector, or cybersecurity maturity. The four levels build up in terms of the number of controls in a coherent way. CyFUN® allows the cybersecurity maturity level to be increased over time so that invested resources can result in a coherent increase of cybersecurity CyFUN® was initially developed by the CCB, but is now a standard recognized by the Belgian Accreditation Organisation (Belac). Moreover, it is used in, and co-owned by, more than three other EU Member States (including Romania, Ireland, and Malta), making it ever more a European framework..
How it works	CyFun® is based on the National Institute of Standards and Technology's Cybersecurity Framework (NIST/CSF) and complemented by relevant insights from other standards including ISO 27001/ISO 27002 (for establishing an information security management system), IEC 62443 (cybersecurity for operational technology in automation and control systems.), the CIS Critical Security Controls (ETSI TR 103 305-1).The scheme is validated by the Belgian National CSIRT, including its Computer Emergency Response Team (CERT.be) who provided the anonymized real-world cyber-attack information. This data was used to obtain the attack coverage rates. • **Starting level Small** allows an organisation to make an initial assessment. It is intended for micro-organisations or organisations with limited technical knowledge. • **AL Basic** (34 security controls) contains the standard information security requirements for all enterprises. These provide an effective security value with technology and processes that are already available. Where justified, the measures are tailored and refined. Building on the Basic level, security requirements are added to protect organisations from increased cyber risks to achieve a higher level of assurance. 82% of CERT attack profiles are covered by requirements on level BASIC • **AL Important** (117 security controls) is designed to minimise the risks of targeted cyber-attacks by actors with common skills and resources in addition to known cybersecurity risks. 94% of CERT attack Profiles covered by requirements on level IMPORTANT • **AL Essential** (140 security controls) goes a step further to also respond to the risk of advanced cyberattacks by actors with extensive skills and resources. 100% of CERT attack profiles are covered by requirements on level ESSENTIAL CyFun® is built around six core functions: govern, identify, protect, detect, respond, and recover. These functions allow, regardless of the organisation and industry, to

	promote communication around cybersecurity among both technical practitioners and stakeholders so that cyber-related risks can be incorporated into the overall risk management strategy of the organisation. Certification or labelling is possible through impartial and competent accredited conformity assessment bodies (CABs) that perform verification (BASIC/IMPORTANT) or certification (ESSENTIAL) audits. CyFun® can also be used as a tool for demonstrating compliance to the NIS 2 cybersecurity requirements.

SAFEONWEB BROWSER EXTENSION	
Webpage	https://atwork.safeonweb.be/protect-my-organisation/safeonweb-browser-extension https://atwork.safeonweb.be/protect-my-organisation/safeonweb-browser-extension
Aim	The SafeOnWeb Browser Extension helps users assess how trustworthy a website is and whether it is safe to share personal data.
Project	For every website you visit, the SafeOnWeb Browser Extension shows you if the owner has been validated (Green) or not (Amber). Known malicious or insecure websites are marked (Red), and you should leave immediately Websites without a validated owner (Amber) should be suited for reading only. You should only share personal and sensitive information if the owner of the web site is validated (Green). If a hacker puts malicious content on a website with a validated owner, the validation status will change to Amber or Red directly after the first notification.
How it works	The **Extension** allocates a **score** to the websites you visit: • Green (OK) - score of 4 out of 4: the website owner has an Extended Validation Certificate issued by a Certificate Authority or the site owner is registered on atwork.SafeOnWeb.be (for Belgian organisations only). Therefore: It should be OK to continue surfing on this website. It should be OK to share data on this website. • Amber (!) - scores from 1 to 3 out of 4: the website owner has an Organisation Validation Certificate, or a Domain Validation Certificate issued by a Certificate Authority, and the website is not registered on atwork.SafeOnWeb.be Therefore: It should be OK to continue surfing on this website. If any doubts, refrain from sharing data on this website. • Red (X) - score of 0 out of 4: the website lacks basic security features or is known as malicious. The website owner has no Certificate and therefore has not been validated. Therefore: We advise against browsing this website and sharing any data. **This score is based on three variables**; The **Certificate Type Score**, which reflects the validation level of the Certificate you have obtained for your Website. This score is computed as follows;

	• 3/3 if you have obtained any type of Certificate and registered your website on the SafeOnWeb@Work portal or you have obtained an Extended Validation Certificate; • 2/3 if you have obtained an Organisation Validation Certificate; • 1/3 if you have obtained a Domain Validation Certificate; or, • 0/3 if you have not obtained any type of Certificate for your website. The **Certificate Authority score**, is a score of 1 or 0 depending on whether the Certificate Authority that delivered your website's Certificate is a known actor on the market and referenced in the CCB's databases. The **Domain Score** reflects whether your domain is registered as malicious, in which case your total score will always bee brought down to 0.

ADCHAIN – FRAUDULENT ADVERTISEMENT DETECTION INFRASTRUCTURE	
Webpage	/
Aim	To rapidly identify, analyse and disrupt fraudulent online advertisements, in particular those linked to investment fraud and other large-scale scam campaigns. The goal is to reduce financial harm to citizens and to strengthen public-private fraud-signal exchange.
Project	Development of a national infrastructure that supports the structured and scalable detection of fraudulent online advertising campaigns across digital platforms. AdChain combines advanced technological detection mechanisms, developed by a Belgian company, with validated governmental insights to enable faster analysis, coordinated follow-up, and more effective disruption of malicious advertisement campaigns. The infrastructure is deployed across relevant digital platforms and operates within a strong public-private partnership framework, ensuring close collaboration between governmental entities, industry stakeholders, and platform providers to enhance resilience against online advertising fraud.

NETFLOW DATA PROJECT	
Webpage	/
Aim	To identify and warn Belgian users whose systems may be communicating with known malicious infrastructure (in particular command-and-control (C2) servers), through the legally supervised analysis of targeted network metadata.
Project	Under Article 21 of the NIS 2 Law (2024), the CCB cooperates with Belgian Internet Service Providers (ISPs) to obtain limited metadata (netflow data) concerning traffic to and from specifically identified malicious IP addresses. The sole purpose of the project is early detection and victim notification.

How it works	The CCB maintains a list of confirmed malicious, foreign C2 servers, based on treated incidents, intelligence feeds, open-source intelligence, dark web monitoring, stakeholder reports (e.g. BePhish, NIS2 notifications), and international partners. Following legal authorization and under the supervision of the Data Protection Authority, CCB can ask ISPs to share strictly limited metadata for all traffic in Belgium to and from these C2 IPs (e.g. source/destination IP addresses, timestamps, ports, traffic volume — but never content). The CCB analyses this metadata to detect suspicious communications, identify the potential victims in Belgium, and then immediately warn them (See also Spear Warning).

RED BUTTON (NATIONAL ANTI-DDOS PROJECT)	
Webpage	/
Aim	The Red Button project aims to monitor, detect, and prevent Distributed Denial-of-Service (DDoS) attacks targeting Belgian organisations and critical services through intelligence-driven early warning to (potential) victims and coordinated mitigation.
Project	The project focuses on proactive threat detection, timely warnings, and coordinated response between targeted organisations, ISPs, hosting providers, and authorities. .
How it works	The Red Button procedure follows a continuous four-phase cycle: 1. **Monitoring** – Continuous intelligence-driven monitoring to detect early signs of DDoS threats. 2. **Response** – Rapid coordination and support to mitigate ongoing attacks and assist targeted organisations. 3. **Analysis** – Processing attack data and logs to update indicators of compromise (IOCs) and improve detection. 4. **Improvement** – Capturing lessons learned to refine methodologies, detection rules, and resilience strategies. The system is highly automated and includes: • real-time data collection and analysis • large-scale **blocklists of verified malicious IPs** • sharing of actionable threat intelligence (CTI), mitigation advice, and ready-to-use firewall rules to (potential) victims When high-confidence threats are identified, targeted organisations are proactively contacted and warned with actionable information, allowing them to take preventive or mitigating measures before or during an attack.
Figures	In 2025, Belgium was among the most targeted EU countries for DDoS attacks, with pro-Russian hacktivist group NoName057(16) launching five coordinated campaigns, often linked to geopolitical events and sometimes announced in advance. Despite the high frequency of attacks, the operational impact remained limited thanks to

	effective coordination under the Red Button procedure. The project processes and maintains blocklists containing hundreds of thousands of malicious IP addresses, contributing to a significant reduction in impact and enabling organisations to maintain service availability.

PHISH-NEMO	
Webpage	https://ccb.belgium.be/news/strengthened-collaboration-federal-judicial-police-combat-phishing
Aim	To proactively detect suspicious domain names at an early stage, before phishing campaigns can be deployed at scale, and to strengthen the rapid blocking of fraudulent domains through their integration into the Belgian Anti-Phishing Shield (BAPS).
Project	PhishNemo is a proactive phishing domain detection system originally developed by the Federal Judicial Police of Limburg. Through its integration into BAPS, the project enables suspicious and validated fraudulent domains to be fed directly into the national DNS blocking infrastructure. This allows phishing domains to be blocked before they can cause widespread harm and significantly reduces the time between detection and intervention. The project relies on a proportionate validation process and is reinforced through cooperation between the Federal Judicial Police, the CCB and Secutec, combining public and private expertise in DNS monitoring and phishing disruption. In 2025, this contributed to nearly 16,000 redirects to the BAPS warning page.