CENTRE FOR
CYBER SECURITY
BELGIUM

UNDER THE AUTHORITY OF
THE PRIME MINISTER

CYBERSECURITY STRATEGY BELGIUM 2.0 2021-2025

MAY 2021

.be

Summary

The Belgian population and organizations have various development opportunities thanks to the presence and growth of digital services and technologies. However, government, citizens and organizations are also increasingly facing (advanced) cyber threats, which can increase the risks and compromise the opportunities of digital services and technologies. The goal of this updated National Cybersecurity Strategy is to safeguard the capabilities of services, goods, people and capital across borders.

The aim of this strategy is to present a forward-looking vision of an open, free and secure cyberspace that responds to potential cyber threats Belgium faces or may face. This document identifies the different stakeholders, the main threats, conveys a clear mission and, based on this, puts forward strategic objectives and priorities for the coming years, as well as the resources necessary to be able to achieve them. Since cybersecurity must be treated as a shared responsibility, the different roles of the actors involved are described. The Centre for Cybersecurity Belgium (CCB) is responsible for the coordination of cybersecurity, so it has a key role in the realization of this Cybersecurity Strategy 2.0.

Centre for Cybersecurity Belgium, Brussels, May 2021

Table of contents

1. Introduction

Our society and economy are constantly changing. This process is accelerated by digital transformation. People, organizations, devices, data and processes increasingly connect and interact through online channels such as the internet, mobile devices, Internet of Things (IoT), or the cloud for storing (personal) files and photos. This growth in the use of new technologies has been accompanied by an increase in cyberattacks, as well as an increase in the severity and impact rate of these attacks. Sensitive data, including personal data, customer data and politically sensitive data (e.g. military intelligence), is increasingly at risk of disclosure. Therefore, it is of utmost importance to protect this data by securing the digital environment.

1.1 Policy Context

In 2012, Belgium signed off on its first Cybersecurity Strategy, which focused on recognizing cyber threats, improving security, and establishing measures to respond appropriately to incidents. With the continuous change in the cyber landscape, a new Belgian cybersecurity strategy that responds to current and future risks and threats is needed.

The Cybersecurity Strategy 2.0 shapes Belgian policy and aims to secure the cyber landscape at all levels, for all stakeholders. Monitoring, coordinating and overseeing the implementation of the Belgian Cybersecurity Strategy is the responsibility of the Centre for Cybersecurity Belgium (CCB). The Cybersecurity Strategy 2.0 sets goals for 2025 and will be periodically reviewed and adjusted where necessary.

This Strategy is also framed in an international context. For example, the European Union is working on a number of initiatives to promote and improve cyber resilience within the EU. In July 2016, the *Security of Network and Information Systems* (NIS) Directive was adopted, which was transposed into Belgium law on 7 April 2019: *Act establishing a framework for the security of network and information systems of public interest for public safety*. Article 7 of this directive (reproduced in article 10 of the Belgian NIS Act) requires member states to draw up a national strategy for the security of network and information systems.

In addition, in June 2019, the Cybersecurity Act came into force, which, among other things, expands ENISA's mandate to make it the European

Union's cybersecurity agency. This regulation additionally highlights the need for a European Information and Communication Technology cybersecurity certificate, with a view to increasing trust in and the security of products and services that are crucial for the digital single market.

Finally, national resilience commitments under the NATO *Cyber Defence Pledge* should be kept in mind.

1.2 Cybersecurity

Cybersecurity is the result of a set of security measures that minimize the risk of disruption or unauthorized access to information and communication (ICT) systems.

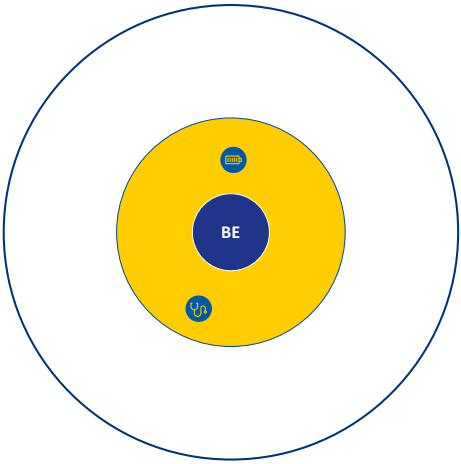
Cybersecurity includes all reasonable and acceptable measures to protect the ICT of citizens, businesses, organizations and government from cyber threats. It involves protecting systems (such as hardware, software and related infrastructure) and networks, as well as the data they contain. Measures to combat the use of ICT for fraud, for incitement or for recruiting terrorists are, strictly speaking, outside the scope of this strategy.

Cybersecurity requires the development and strengthening of technical and organizational measures. First, the right objectives must be identified as well as the appropriate awareness campaigns around cybersecurity for all stakeholders. Consideration should also be given to implementing preventive measures to protect sensitive data from cyber threats and incidents to prevent unauthorized access to this data. It is also necessary to monitor and analyze any threats. Then, if an incident does occur, it is important to be prepared to respond and resolve it in an efficient manner.

Identifying a cybersecurity "governance framework" is important for achieving cybersecurity goals. Consequently, it is crucial to define roles and tasks as well as to clarify the responsibility of all stakeholders involved. Establishing a national governance framework allows for dialogue and coordination of the various activities.

The General Data Protection Regulation, and "Privacy" in general, are not part of cybersecurity as such, but they are obviously a big issue in terms of the CCB's mission to detect incidents and threats. Good cooperation with the Belgian Data Protection Authority is therefore necessary. Similarly, while fighting online disinformation campaigns is not actually a part of cybersecurity, it is connected to it. Cooperation with the competent intelligence and security services is also indispensable in this context.

1.3 Target audiences



Cybersecurity is not just the responsibility of government. It is a collaborative effort to which all stakeholders involved can contribute. Improvements in overall safety will come through everyone's efforts.

i. Population

Citizens are primarily responsible for protecting their own property. This includes smartphones, laptops, tablets, but also the applications on them (such as banking applications) and therefore the data they contain. Protecting their own devices and applications and using them appropriately makes it more difficult for threat actors to launch cyberattacks. With support from the government and the media, such as Safeonweb.be and https://risk-info.be/en, the population can be/become aware of the main cyber threats and feel involved in securing the cyber environment.

ii. Companies

Companies play a big role in protecting their own infrastructure and their employees' data. Small and Medium Enterprises (SMEs, less than 250 employees) have an important place in this, as they comprise more than 99% of Belgian companies. This group of stakeholders includes educational institutions and suppliers of security products. Security products such as firewalls, virus scans, encryption or other software and hardware products make IT systems a lot safer and reduce the likelihood of incidents. Investing in these security products, supporting suppliers of them, and facilitating users of IT systems in the use of these products is important. Developing a basic cybersecurity certification that allows a company to demonstrate that it is paying due attention to the most common cyber threats is a not insignificant aspect of this approach and can also serve as a competitive advantage. In 2019, the European Union also launched a cybersecurity certification framework in this vein.

iii. Government Services

Belgium has a complex government structure which does not make a coordinated cybersecurity policy for government departments easy. The federal government has horizontal, vertical and programmatic services. Regions and Communities have ministries and directorates. The Centre for Cybersecurity Belgium (CCB) develops advice and guidelines that are available to all government departments.

Security and cybersecurity in particular are federal matters and dealt with at the national level.

iv. Organizations of Vital Interest

Our country's Organizations of Vital Interest (OVI) need to be optimally protected against cyberattacks, as incidents affecting these organizations can have a large-scale, national impact.

In this context, Organizations of Vital Interest Refer to the public and private entities that provide an essential service to the Belgian population and that use network and information systems to do so. OVI should therefore be understood as the operators of critical infrastructures, Operators of

essential services, digital service providers and nuclear facilities (as referred to in their respective legal frameworks)[1].

The initial determination of who Organizations of Vital Interest are is done by the sectoral authorities, in consultation with the National Crisis Centre (NCCN) and the CCB. The categorisation is meant to be evolutionary and includes the sectors of energy, mobility, telecoms, finance, drinking water, public health, digital service providers and government.

1.4 Vision

Belgium advocates an open, free and secure cyberspace where citizens and businesses can fully develop, where they can engage internationally, and where fundamental rights are safeguarded and protected. To build and ensure society's essential trust in cyberspace, cybersecurity is of necessary and decisive importance. This is a shared responsibility of all stakeholders and requires a broad-based approach.

1.5 Mission

By 2025, Belgium should be one of Europe's least vulnerable countries in the cyber domain.

The Cybersecurity Strategy 2.0 aims to make Belgium one of the least vulnerable countries in Europe in the cybersecurity domain by 2025. This will be underpinned by outlining action plans to protect all stakeholders, from the general population and private organizations to Organizations of Vital Interest. The strategy is aligned with government and private sector investment strategies for future development and ensures these investments and the creation of new opportunities and jobs. In addition, the strategic objectives enable us to be prepared for new technological developments and the potential risks.

1 Although the country's Scientific and Economic Potential and organizations providing essential services within the public sector fall within the intended scope of "Organizations of Vital Interest," a clear cyber governance framework for these sectors must first be developed.

2. Risk assessment

The Belgian National Risk Assessment 2018-2023 of the National Crisis Centre considers cyber as one of the main risk clusters our country will face in the coming years. Within this cluster, cybercrime and hacktivism against businesses and critical infrastructures are identified as national priority risks.

In 2017, we saw how the WannaCry ransomware spread to more than 150 countries and interrupted business activities, and how the NotPetya malware grew in a flash into the most expensive cyber incident ever.

Furthermore, the evolution of the cyber threat from financially driven to geopolitically motivated is extremely concerning. Western countries are facing a threat in cyberspace that exceeds the danger of physical attacks. These cyber threats can have serious direct consequences on, for example, our electricity distribution, our banking systems or on the availability of all online services. Continued media coverage of cyber incidents, even minor ones, can cause the public to lose confidence in the digital environment and services, which can have pernicious economic consequences.

As part of the hybrid threat, the cyber threat can be used to amplify the effects of other attack methods. With this threat, a combination of, say, a physical attack with a series of cyberattacks can seriously amplify the effect and temporarily create an atmosphere of chaos.

This strategy defines national goals for the period 2021-2025 to meet this constantly changing cyber landscape. In order to set the right priorities in formulating these objectives, it is necessary to have a clear picture of the various cyber risks and threats that Belgium may face during this period. This chapter provides a concise overview of key threat actors and technological risks.

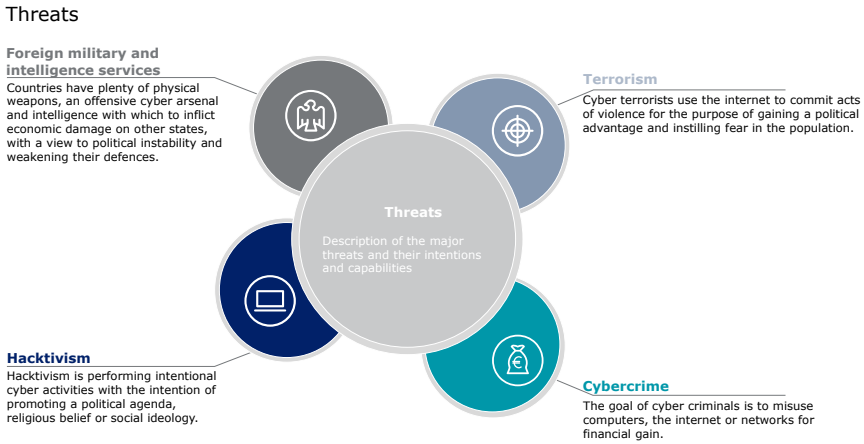
However, it should be mentioned that risk assessment is an ongoing process. Calibrated consultative platforms, such as the Coordinating Committee on Intelligence and Security and its Platform 4 Cyber, will therefore continue to evaluate the measures taken, monitor cyber trends and adjust objectives as necessary. The preparation of a Belgian contribution to the European 5G risk assessment in 2019 is an example.

In addition, as a follow-up to the Belgian National Risk Assessment 2018-2023, the National Crisis Centre foresees a more in-depth analysis with all

involved actors of the main risk clusters (of which cyber is a part). It aims to better identify the underlying causes and effects in order to provide a clear overview to decision-makers when dealing with the risk.
Finally, events that involve an increased cyber risk (international summit, elections, etc.) regularly take place on Belgian soil. These types of events may require an exceptional risk assessment to identify heightened risks and recommend appropriate actions.

2.1 Threat actors

Because the motivations and capabilities of threat actors are constantly changing, it is critical to understand and monitor who the most significant threat actors are. This also allows us to understand how the cyber landscape is evolving. Belgium considers the following actors to be the biggest threat to the Belgian state and population: cybercriminals, foreign military and intelligence services, terrorist groups and hacktivists.



2.1.1 Cybercrime

The (potential) impact of cyber threats emanating from cybercriminals has become increasingly clear in recent years. These include not only threats that could disrupt our infrastructure, but also threats to the integrity, availability

and confidentiality of the information we digitally capture, analyze and exchange. The digitalization of things or goods (Internet of Things) implies that they are 'hackable'. This has a direct impact on the overall security of every citizen, but it also means that these things or goods may contain digital traces that could be of interest in crime investigations.

The main objective of criminal actors, both individual actors and those involved in organized crime, is usually to generate money and profit, for example through phishing, data theft or ransomware. In some cases, they may additionally have destructive purposes in mind, for example data sabotage or cyberattacks. Cybercriminals specialize in specific services, which they then offer on the Dark Web for a fee. This allows a criminal to subscribe to, for example, an Exploit Kit, which allows them to use the latest digital intrusion techniques without any technical knowledge.

Cybercriminals offer their services to anyone willing to pay for them. Therefore, in addition to cyberterrorism, criminal organizations (or individuals) seeking to cause material and/or physical harm should be factored in as a potential threat actor at the national level. Indeed, the potential impact of cyberattacks on critical infrastructures can be such that the stability of state institutions is jeopardized.

2.1.2 Foreign military and intelligence services

Nations and states possess a great deal of knowledge and physical weapons, as well as an offensive cyber arsenal. There is always a chance that they may wish to use these for purposes other than protecting their own citizens. Military and intelligence services can deploy their knowledge and weapons to inflict economic damage on other states, to create political instability in other states, and/or to weaken other states' defences. Foreign military and intelligence services are not only conducting more cyberattacks in order to gain a competitive advantage in terms of intelligence, but increasingly, advanced techniques are being used to disrupt the operations of organizations — and indirectly so the countries in which they are based — for example by exposing confidential information.

The capabilities of various national military and intelligence agencies are becoming more sophisticated. Therefore, it is becoming increasingly difficult to detect such cyberattacks and to take preventative action to defend against them. Consequently, the actual activity of these threat actors is much more frequent than statistics indicate.

2.1.3 Hacktivism

Hacktivism is the performance of various intentional cyber activities for the purpose of promoting a political agenda, religious belief, or social ideology. It may be a politically motivated movement that carries out this activity. Currently, the most commonly used attack methods in this regard are doxing[2], DDoS[3], web defacement[4] and unlawfully taking over identities and social media channels.

2.1.4 Terrorism

Cyberterrorism is the carrying out of violent activities using the internet, with the underlying goal of gaining political advantage through intimidation and instilling fear. These acts can result in destruction, loss of life and/or physical harm. The most obvious targets of cyberterrorists are public services, industries and critical infrastructures.

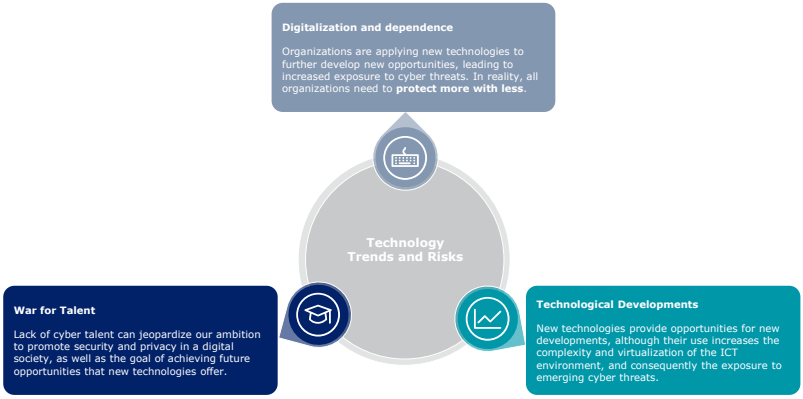
For example, some terrorist groups use the online world as a propaganda and recruitment channel for terrorism. Since 2016 there has been a clear transition from the use of Twitter and Facebook to more encrypted communication channels. Current developments also point to an increasing use of cyber tools to finance terrorism, e.g. through ransomware, cryptomining or even crowdfunding. In this context, there is great concern that terrorist organizations will also carry out more cyberattacks. However, it seems that, until now, these attack techniques are fairly limited. To carry out DDoS attacks, groups still purchase domain hosting services, download software and rent botnets, rather than developing their own cyber weapons.

2.2 Technology trends and risks

The technological landscape does not stand still, and new products are coming onto the market all the time. Organizations are applying these new technologies to stay competitive and develop new opportunities. However, there are also risks associated with these technological developments, also because they help further develop the skills of threat actors. It is therefore crucial to always be aware of developments in technologies and the associated risks.

2 Doxing is the usually unlawful public dissemination of a person's information or documents.
3 DDoS stands for distributed-denial-of-service attacks in which a large volume of data is sent to one specific system to disrupt its normal operation.
4 A web defacement is the unlawful alteration of the content of a website or webpage

Technology trends and risks



2.2.1 Dependency

Organizations are applying new technologies to develop new opportunities and to increase their productivity or efficiency. The increase in the use of these technologies is therefore creating an ever-growing dependence on ICT. This is accompanied by increased exposure to cyber threats. It can also be generally observed that technologies are being deployed at a faster rate than the security for these technologies.

Organizations will be more committed to providing and using new technologies than to allocating budgets for their security. It is often overlooked that new technologies are not always extensively tested immediately. It is therefore a big risk to assume that no attacks exist yet or that it is safe to implement and secure the technology in the usual ways. After all, it often takes a few months or years for most attacks and vectors on a given technology to become public and to be properly protected against. Secure development — with attention for security — should therefore be included in the development process of new software and technologies.

There is also an ever-increasing reliance on third party providers at every step: development, production, maintenance, and processing. This increases the risk and potential critical impact of what are known as “supply chain attacks”.
The interconnection of products can also give rise to “hazardization”.

This is the situation that arises when a product is safe when obtained by a consumer, but when connected to a network, it becomes dangerous due to malicious, incorrect, or careless changes to the operational code.

2.2.2 Technology-specific risks

New applications resulting from emerging technologies often offer major advantages over traditional methods; for example, in terms of efficiency and economies of scale. However, there are sometimes specific security risks associated with them.

A good example is cloud computing. The big advantage is that the infrastructure no longer needs to be maintained and everything scales with the pace at which the organization grows. A central cloud infrastructure can therefore be professionally well secured. However, the risk is that an unauthorized access suddenly means compromising a very large amount of information.

Two economic threats can also be formulated in this regard. First, the world of cloud-based applications is characterized by the presence of a limited number of global players, where economies of scale can be played out, creating a concentration risk. On the other hand, innovation in this market is often offered by new, much smaller players. These young organizations are often not on the same level in terms of performance and maturity of processes. This can lead to misplaced confidence in these applications.

Ever-increasing technological development of new (types of) ICT-based products and services in many economic sub-areas also requires supervisory authorities to rapidly evolve market surveillance and inspection capabilities. On the flip side, of course, these technologies sometimes offer advantages for building market surveillance more efficiently.

Authorities already pay considerable attention to person-centred aspects around “security” and “privacy”. In contrast, the product-related aspects of these topics, such as regulation and control, are barely covered by the supervisory authorities, if at all. Thus, there is a need to adjust the existing legal framework. This should be done mainly from a European/international framework. The European Cybersecurity Act is an important step in this regard, and requires a clear Belgian implementation.

Another common risk is individually protecting internet-connected devices. The biggest recent challenge in this area is the Internet of Things (IoT).

It is very important to assess the risks and establish the necessary security before deploying new technologies. The speed in development and adoption of new technologies such as artificial intelligence, quantum computing, blockchain, and smart meters & grids makes appropriate evaluation of (and protection against) all risks challenging.

2.2.3 War for Talent

With the digital transformation and the adoption of new technologies, there is also a rise in misuse of these systems. It is therefore important as an organization to invest in recruiting IT profiles, as well as IT security profiles. However, there is a lack of cybersecurity talent in the job market. There are few courses where cybersecurity is a (major) component. Often it is taught as an ancillary subject, so little knowledge of it is gained or transferred in practice.

Therefore, there is a clear shortage of cybersecurity professionals. As a result, many organizations will not be able to fill these positions or will fill them with other profiles. The challenge of finding competent and reliable employees obviously goes hand in hand with the internal threat ("the insider threat").

3. Strategic objectives and approach

The aim of a cybersecurity strategy is to respond to technological developments and to meet the high need to protect the population, the private and public sectors and the vital sectors. The Cybersecurity Strategy 2.0 contains six strategic objectives for the next four years. This strategy prescribes a number of actions to achieve these strategic objectives. This will be achieved thanks to the help of various stakeholders.

3.1 Strengthen the digital environment and increase trust in the digital environment

3.1.1 Investing in a secure network infrastructure

Work will be done together with the internet service providers (ISPs) to create a more secure basic network infrastructure. New protection techniques will follow technological evolutions, such as the Internet of Things (IoT) and new generations of fixed and mobile networks.

Network infrastructure security can be improved by adopting more secure internet standards (DNS security, secure routing, encryption, etc.). These standards provide a safe way to exchange data, i.e. a "safe data transport layer". Online data exchange is then secure across the board. This reduces the risk of an attack on a weak link in the chain.

Such standards can also ensure more trusted identities and publications on the internet. This can be done, for example, by encouraging the use of technology such as Itsme and Extended Validation Certificates on websites.

A test environment ("testbed") for infrastructure can also be developed. A testbed is a platform that allows new infrastructure to be tested in a reliable, controlled and secure environment before it is widely used.

3.1.2 Establishing a Cyber Green House

Establishing a Cyber Green House will provide a significant boost to innovation in the cybersecurity sector. The creation of such an innovation centre aims to test innovative cyber solutions and business models in a risk-free environment and to disseminate Cybersecurity Guidelines and Best Practices.

3.1.3 Foster expertise and knowledge

To meet the need for greater security and more security professionals, more has to be invested in expertise and knowledge. Educational institutions make a significant contribution to the cybersecurity landscape. They not only play an important role in increasing knowledge by conducting research, but also by contributing to the development and provision of relevant training.

There will be further investment in Research & Development (R&D) in the area of Cybersecurity. The private sector and educational institutions such as universities and colleges will work closely together.

European initiatives in this framework will be evaluated from this objective. Security managers of public institutions should be trained to an adequate level of security, through training programmes for public officials.

To address the lack of information security professionals, both within the government and private sector, more young people should be encouraged to pursue STEM (Science, Technology, Engineering and Mathematics) courses. This requires establishing contacts with communities and defining a coherent policy on the subject in collaboration with relevant partners. For example, awareness and information materials can be provided to schools or mentoring programmes can be organized.

3.1.4 Cybersecurity Certification and Labelling of Products, Services and Processes

Belgium will create a framework to allow companies to evaluate and certify the security of ICT products, services and processes.

This framework will be aligned with the EU Cybersecurity Act 2019 and developments underway at the European level. The EU Cybersecurity Act aims at a European recognition of delivered certificates, as well as maximum alignment with existing European and international reference frameworks.

To this end, as required by the EU Cybersecurity Act, Belgium will establish a *National Cybersecurity Certification Authority (NCCA)*. The NCCA, in consultation with, among others, market surveillance authorities, other sectoral authorities and the National Crisis Centre, will coordinate the necessary expertise in cybersecurity certification, authorize certificates with high security requirements and establish close cooperation with

BELAC (the Belgian accreditation organization) by making maximum use of existing processes, procedures and regulations.
Work will also be done on a cybersecurity recognition mechanism for companies, with a special focus on SMEs who wish to demonstrate that basic cybersecurity requirements, best practices and policies are in place. It is important for strategic sectors to think about an integrated approach that combines IT aspects, physical protection and staff screening.

These initiatives strongly support the vision of this Cybersecurity Strategy and will boost customer confidence in the security of the digital environment.

3.1.5 Strengthening the cyber skills of intelligence and security agencies

To provide an appropriate response to the rapidly growing threats, the capabilities and skills of our intelligence and security services must at least keep pace with them. The human capital of technical experts in cybersecurity constitutes the nation's best weapon against these new threats.

In order to provide our services with the necessary experts, alternative recruitment and employment methods will be evaluated and used whenever possible. After all, the need for young and highly trained computer experts does not only exist within our security services. The "War for Talent" is being fought among specialized companies, large multinationals and all the security services in Europe and beyond. To expand their knowledge, such technical experts often seek new challenges and are usually not looking for a job for life. A sufficiently flexible recruitment system and more competitive remuneration should enable our security services to better compete on the labour market.

Government departments must also offer their technical cybersecurity experts sufficient high-quality technical training. This not only counts as an important motivating factor, but it also guarantees sufficient technical knowledge and expertise.

3.2 Arming users and administrators of computers and networks

Almost all of the internet's infrastructure and systems are in the hands of private owners. It is therefore of great importance that every owner of a

computer system or network is adequately armed to protect it from cyber threats and attacks.

3.2.1 Raise awareness and engage

In addition to informing citizens about potential threats, the government is striving to make citizens more aware about how to better protect themselves from potential cyber risks.

To protect systems and computer networks, not only are technical protection measures necessary, but each user must use them responsibly. Those who are sufficiently aware and vigilant quickly become the best detection system for cyberattacks. From the website www.safeonweb.be, the public can get all the information about specific threats, how to recognize them and how to protect themselves or respond.

The internet belongs to and is for everyone. Its safety is also a shared effort. Therefore, the population is urged to participate in security. For example, anyone can forward suspicious emails to **suspicious@safeonweb.be**. Such initiatives will be expanded.

The CCB organizes an annual awareness campaign through the media and frames it through European initiatives. The European cybersecurity agency the ENISA organizes European Cybersecurity Month every October.

Through good collaborations, contact between citizens and quality service providers in cybersecurity in our country should be facilitated. Such streamlined contact should enable citizens to address security incidents and neutralize problems.

Raising awareness also has a direct impact on the business community and creates a general culture of concern and safety. Awareness campaigns, such as through webinars, guides or the cybersecurity KIT, should be further deployed.

3.2.2 Informing about threats and vulnerabilities

Timely warnings about emerging and significant threats or vulnerabilities is crucial.

The CCB permanently analyzes all available information on cyber threats or vulnerabilities and sends out alerts where necessary. For the public, the CCB has the necessary digital media and maintains a direct and transparent

relationship with the general media. BE-Alert from the National Crisis Centre (NCCN) can support and send alerts within a specific region.

Companies and organizations are urged to publish a "Coordinated Vulnerability Disclosure Policy." Through sectoral authorities, professional organizations and the Cyber Security Coalition Belgium, they will be informed of significant threats or vulnerabilities. Organizations of Vital Interest will also receive targeted and non-public alerts through the CCB's Early Warning System (EWS).

The CCB, with the national Computer Emergency Response Team (CERT.be) and as a national CSIRT (Computer Security Incident Response Team), is tasked with detecting, analyzing and informing users of online security problems and vulnerabilities. However, this cannot be done without the support of internet service providers who must quickly forward the warnings to their vulnerable or threatened customers.

3.2.3 Disseminate cybersecurity guidelines and best practices

Cyber threats and the attack techniques used are evolving very quickly. Knowledge sharing and the sharing of best practices is therefore very valuable. Not only does this enrich knowledge and generate new ideas to address the threats, but it also facilitates decision-making. Cybersecurity knowledge is shared through existing or to-be-established platforms.

The CCB maintains an Online Cybersecurity Reference Guide to assist organizations in developing a cybersecurity strategy. The guide offers "basic" and "more advanced" recommendations in terms of planning, risk management, security measures and evaluations in the use of computers and computer networks. The identification and management of risk is critical in this regard. The guidelines offered are based on international standards and are continuously updated by the CCB. As such, companies are strongly encouraged to adopt these guidelines in their cybersecurity policies.

3.3 Protecting Organizations of Vital Interest from all cyber threats

Across the world, Organizations of Vital Interest are facing a rapidly increasing and more sophisticated cyber threat. Given that cyberattacks against these organizations can have a significant impact on our society

and on national security, it is crucial to support them appropriately to protect themselves.

3.3.1 Optimize information exchange and send alerts

The CCB, as the national cybersecurity authority, receives all pertinent threat information from its partners. It continuously analyzes this received information and sends out alerts through its Early Warning System (EWS) or other channels. This ensure that

the Organizations of Vital Interest are continuously informed about relevant cybersecurity threats, vulnerabilities or incidents.

In Belgium, sectoral authorities have a crucial responsibility in identifying, regulating and monitoring the Organizations of Vital Interest. A consultation platform between these sectoral authorities (Cyber Security Sectoral Authorities Platform – CySSAP) should help optimize the management of information exchanges with Organizations of Vital Interest, also in view of cross-border dependencies.

3.3.2 Improve protection for international institutions

Belgium is home to many international institutions, including NATO (North Atlantic Treaty Organization) and institutions of the European Union. The Belgian Organizations of Vital Interest that support these institutions will be identified so that appropriate protection can be provided.

In addition, good dialogue and cooperation with the international institutions in our country is important and necessary to increase the effectiveness of protection and response to cyberattacks.

3.3.3 Be able to handle incidents with national impact

The National Cyber Emergency Plan continues to be operationalized. Through optimal cooperation between the CCB's national Computer Emergency Response Team (CERT.be), the Integrated Police Services and the National Crisis Centre (NCCN), incidents are dealt with quickly and effectively and legal investigations are immediately integrated.

Incidents with a national impact are escalated to the appropriate level and acted upon by ad hoc Rapid Reaction Teams where other services and partners are also efficiently engaged.

3.3.4 Exercises

The Belgian Cyber Emergency Plan was approved by the Council of Ministers in 2017 and describes the procedures to be followed by the various services in the event of a cyber incident. This plan should be evaluated each year and adjusted as needed. The CCB plays a coordinating role in this. Holding regular exercises is important for building resilience to incidents and to test the effectiveness of the Emergency Plan. The lessons learned from these exercises can then inform the annual reviews of this plan.

Therefore, the participation of Belgian security forces, other government departments and Organizations of Vital Interest in both international and national exercises is highly desirable. The coordination of Belgian participation in such exercises is ensured by consultation between the CCB, FPS Foreign Affairs, NCCN and the Ministry of Defence.

3.4 Responding to cyber threats

Addressing increasing cybercrime and government threats requires investment in the rapid identification of, and response to, danger to our population, to our economy, or to Organizations of Vital Interest.

3.4.1 Mapping the international threats

The Continuous monitoring and assessment of international cyber threats is critical to reducing the risk of cyberattacks and incidents. It is the first step of any defence.

The cyber intentions and capabilities of "actors" against our essential and vital interests must be identified and the potential sources of threats must be monitored. In order to protect our computer networks, the evolution of their technical tactics, techniques and procedures must be known as much as possible and our means of protection relative to them must be evaluated..

3.4.2 Disrupting criminal cyber infrastructure

Cybercriminals specialize and reuse the attack techniques and software circulating on the Dark Web. To carry out their high-tech or large-scale cyberattacks and also to remain anonymous, they use proprietary as well as compromised computer systems on the internet.

Disrupting this criminal cyber infrastructure partially undermines the criminals' business model. This can include:

- Detecting and neutralizing the infrastructure through legal means
- Detecting compromised systems and notifying the owner
- Protecting public and corporate communications from known malicious infrastructure
- Sharing information nationally and internationally

It requires all intelligence and security agencies to work closely together.

3.4.3 Develop an appropriate repressive capacity

To reduce Belgium's vulnerability in the cyber domain, preventive measures are crucial. Well-informed and resilient citizens, businesses and governments will ward off and discourage future cybercriminals. The influx of criminal cases decreases with each investment in prevention. As a result, the police and the judiciary will no longer have to deal only with symptoms, but must be able to tackle the root causes.

At the same time, it is clear that cybercrime will continue. An effective and competent repressive shutting-down mechanism is therefore still needed to optimally address the residual category of computer crimes committed. Perpetrators of computer crime must be identified and caught, and evidence of the part they play must be gathered. As stated above, the criminal infrastructure must be mapped out and dismantled, illegal assets must be seized and confiscated, and the suspects must be prosecuted and properly punished. Since cybercriminals mainly operate in an international context, this also requires coordination with other countries affected.

This strategic plan's ambition is to support the development of an appropriate repressive capacity. Such repressive capacity must be able to adequately and competently detect, investigate, prosecute, and sanction cybercrime.

The objective here is first of all to build up the appropriate capacity and expertise at all levels of the integrated police (both the local police and the decentralised and central services of the federal police) so that the mapping-out and investigation capacities expected of each level can be effectively and quickly realised in a digital environment.

The intention is subsequently to ensure that the prosecutor's offices and the courts of all judicial districts and residences have sufficient prosecutors,

investigating judges and sitting magistrates with an interest in cybersecurity and cybercrime and who are following an aligned training path for this purpose. These magistrates are supported by specialized internal networks within which they can exchange and discuss experiences, problems and best practices. The investigation and prosecution activities of the judiciary must be guided by an extensive policy on cyber crime.

3.4.4 Develop an appropriate defence capability

The internet is increasingly becoming a target and a tool in international conflicts.

All NATO heads of state and government have declared that cyberspace should be considered a new operational domain (in addition to the classic land, air and maritime domains) in which military and intelligence operations can be conducted.

Adversaries use every opportunity in and across cyberspace to strengthen their information position, to disrupt our civilian and military systems, and to undermine confidence in the information that supports our operations. The further expansion of cyber capabilities within the General Information and Security Service (ADIV/SGRS) and the Ministry of Defence is therefore one of the priorities in the policy paper of the Minister of Defence and in the Strategic Plan of Defence. It should also eventually lead to the creation of a fifth component that will focus specifically on the cyber threat. The objective is twofold: a better understanding of and protection against the cyber threat, and a better understanding of the opportunities. The cyber strategy of the Ministry of Defence sets out these objectives in concrete terms. Moreover, this component will have an important dual character in support of society in case of (hybrid) crises.

3.4.5 Attribution

Identifying and attributing a cyberattack to a particular person, group or state plays an increasingly important role in world politics. The discussion around the need and possible international coordination of the attribution of a cyberattack is high on the international agenda of NATO, EU and UN, among others. Attribution, however, remains a political and sovereign decision with a major impact on foreign policy. A possible attribution will therefore be thoroughly analyzed and decided through a coordinated national procedure. For this, capacity building is crucial.

3.5 Improve public, private and academic collaborations

In the prevention, reduction, treatment and monitoring of cyber threats and incidents, cooperation between the stakeholders involved, both at the national and international level, is a key to success.

3.5.1 Promote coordination and collaboration

Each stakeholder that plays a role in Belgium's cybersecurity has its own specific responsibilities. However, it is crucial to coordinate all initiatives centrally. The CCB, as the national authority, is responsible for coordination between the stakeholders involved: including public services but also the private and scientific sector.

Cybersecurity knowledge and the evolution of the cyber threat will be shared through existing or new platforms between the relevant security agencies, public authorities, and the private and academic sectors. Regular meetings allow experts to share information and experiences directly and to network with each other. The open and structural dialogue should allow the CCB to better understand the most urgent needs.

3.5.2 Supporting the Cyber Security Coalition

The Cyber Security Coalition is a unique partnership in which players from academia, public agencies and the private sector join forces in the fight against cybercrime. By 2020, 100 organizations from the three sectors were already active members, contributing to the coalition's mission and goals.

The coalition provides a response to the urgent need for cross-sector collaboration, by:

- sharing knowledge and experience
- initiating, organizing and coordinating concrete cross-sector initiatives
- raising awareness among citizens and organizations
- promoting the development of expertise
- and making recommendations for more effective policies and regulations

The government, and the CCB in particular, will actively support the Cyber Security Coalition and participate in its activities.

3.6 A clear international commitment

The cyber threat is global and cannot be addressed solely at the national level. International cooperation is an important pillar of a decisive national cybersecurity policy. Cybersecurity requires a holistic perspective that employs the various vectors of international cooperation (diplomatic, military, economic, etc.). It is therefore important that the various authorities involved, in close consultation and in their separate powers, work closely together.

Belgium supports the legislative and diplomatic role of the EU, NATO and other relevant international organizations in their contribution to an open, free and secure cyber environment and will actively participate whenever possible. Particular attention goes to the agency for cybersecurity in Europe, ENISA. Since its inception in 2004, ENISA has been developing an overall culture and awareness for network and information security in the EU. The CCB will continue to represent Belgium in the various bodies and platforms of ENISA.

Bilateral cooperation between all relevant authorities in Belgium and their foreign counterparts also optimizes international cooperation and can strengthen trust.

4. Responsibilities

Collaboration and the assumption of shared responsibility are crucial for developing effective cybersecurity. Defending the digital environment in Belgium against (emerging) threats is not just the government's responsibility. The other stakeholders can also make relevant contributions to the various goals and related action plans, including citizens, businesses and Organizations of Vital Interest.

Just as in the real world it is the responsibility of every ICT system owner to properly secure their system and to manage and use it responsibly. Every citizen should be informed and aware of the main risks when using ICT and the internet and should heed the security advice given. Specifically, this means that every user must both take care of the technical security of their systems and use these systems in a responsible manner. Companies and public institutions must protect their environment and understand their responsibilities if they are victims of a cyberattack.

4.1 The Centre for Cybersecurity Belgium (CCB)

The CCB monitors, coordinates and oversees the implementation of Belgian cybersecurity policy. From an integrated and centralized approach, it manages the various projects in the field of cybersecurity and ensures coordination between the services and authorities involved, and the public authorities and the private or academic sector.

In cooperation with the National Crisis Centre, the CCB ensures crisis management in cyber incidents. For administrations and public institutions, the CCB disseminates standards, guidelines and safety norms.

The CCB raises awareness of the main cyber threats and how to protect against them. Specific programmes with public and private entities should increase expertise in the cybersecurity domain.

The CCB is also tasked with coordinating Belgian representation in international cybersecurity forums, monitoring international commitments and proposing the national position in this area. It does this with a view to coherent foreign action in close consultation with the FPS Foreign Affairs and the Ministry of Defence.

The CCB proposes the Belgian position to the European institutions, among others regarding certification and labelling of products and services.

4.1.1 CERT.BE

As the national CSIRT (Computer Security Incident Response Team), the CCB also has an important detecting and alerting role. The Computer Emergency Response Team (CERT.be), as an operational service of the CCB, is responsible for detecting, observing and analyzing online security issues such as cyber threats, vulnerabilities in ICT systems or cyber incidents. CERT.be will continually inform the population, companies, public services and Organizations of Vital Interest about these issues. In this sense, CERT.be is the central hub for exchanging cybersecurity information.

4.2 The Federal Police

The integrated police services, in cooperation with their partners, are responsible for combating computer crime.

As the first-line police, the local police are the first point of contact for citizens, businesses and government agencies. In this role, they engage the specialized services (RCCU/FCCU) when required.
Within the Federal Judicial Police, the Regional Computer Crime Units (RCCUs) and the Federal Computer Crime Unit (FCCU) are responsible for the legal handling of ICT crime.

An RCCU is responsible for providing specialized assistance in investigations in a computerized environment — with mainly a supporting role in forensic analysis of ICT material (PCs, smartphones) — for cases concerning all kinds of crime, for both the local police and the Federal Judicial Police of the district of which it is part. It also deals autonomously with the legal approach to computer crime files linked to its district operation. Here, the collection of digital evidence is important, with the aim of tracking down the perpetrators and bringing them to justice.

As an operational service, the FCCU is part of the Central Directorate for Combating Serious and Organised Crime. In addition to a forensic support analysis role, primarily as support for the central services, it is responsible, on an autonomous basis, for the legal handling of computer crime cases related to attacks on the ICT infrastructure of critical infrastructures or vital sectors. When it comes to other complex attacks that cannot be

linked to a district or are cross-district, the FCCU plays a coordinating role. The FCCU also serves as a national point of contact in the international approach to cybercrime.

4.3 The Public Prosecutor's Office

Investigations in general, but also for cybercrime in particular, are conducted in each judicial district under the direction of the competent Public Prosecutor. The latter gives the integrated police services and, if necessary, other investigative services the necessary orders to collect evidence and bring the truth to light. Ultimately, it is the public prosecutor who will or will not bring the cyber crimes to court. On these matters, the Public Prosecutor usually has one or more reference cybercrime magistrates who are primarily responsible for investigating cybercrimes.

The Federal Prosecutor is part of the Public Prosecutor's Office and is specifically charged with the exercise of criminal procedure for well-defined crimes (including terrorism, violations of humanitarian law, etc.). The Federal Prosecutor's Office may also be asked to take charge of coordinating criminal investigations that cover several jurisdictions or have an international dimension, in consultation with the Crown Prosecutor. The Federal Prosecutor has a Cyber Unit that includes federal magistrates who are particularly focused on the investigation of cyber crimes. These include complex cybercrimes with a large international dimension, committed by organized criminal networks using advanced techniques, and threats to Critical National ICT Infrastructures. Finally, the Federal Prosecutor is also tasked with promoting international operational cooperation and represents the Public Prosecutor's Office at EUROJUST and the European Judicial Cybercrime Network. If a cybercrime cannot be immediately located in a well-defined district, the Federal Prosecutor may order the first and most urgent investigations.

The Cyber Emergency Plan engages the Public Prosecutor's Office in the management of cyber incidents and crises.

Criminal policy and the proper overall and coordinated operation of the Public Prosecutor's Office is the responsibility of the College of Public Prosecutors. The latter may issue instructions that are mandatory for all members of the Public Prosecutor's Office. They are assisted by national expertise networks (REN), composed of a multitude of relevant partners.

With regard to cybercrime, this is the CYBERCRIME REN, the main coordination of which is done by the Prosecutor-General's Office in Antwerp. On policy questions, the CYBERCRIME REN is the appropriate point of contact.

4.4 Defence

The Ministry of Defence is developing a cyber strategy, policy plan, and the necessary capabilities to support military and intelligence operations from, as well as conducted in, the cyber domain. These investments will enable Belgium to have long-term technical/technological capabilities that will allow it to protect necessary infrastructure from cyberattacks, and if necessary, to carry out a counter-attack.

The Ministry of Defence will have a high-tech cyber capability to maintain its freedom of action in and through cyberspace in military operations.

Additionally, the Ministry of Defence supports national cybersecurity policy by:

- Loyally fulfilling the commitments set forth in the National Cyber Emergency Plan;
- Engaging its capabilities as needed as a technical expert in support of specific legal cases or as technical support for specific CERT.be cases;
- Offering senior expertise level malware analysis to national stakeholders;
- Integrating relevant cyber threat intelligence into the national cyber threat intelligence platform;
- Tracking actors with intentions and capabilities of cyberattacks on national vital interests and structures;
- Coordinating, where appropriate in consultation with Foreign Affairs and the CCB, Belgian participation in international cybersecurity exercises;
- Making the mil.cert infrastructure available as a backup site for CERT.be's Incident Management, in crisis situations where the national infrastructure is unavailable;

- During national crises, deploying its intrusive and offensive capabilities to respond with a cyberattack of its own to neutralize an attack and identify its perpetrators.

4.5 The National Crisis Centre (NCCN)

The NCCN, together with the CCB, ensures the organization and coordination of the Cyber Emergency Plan at the national level. The NCCN and the CCB are jointly responsible for crisis management.

The management of the direct and indirect societal consequences of a crisis remains the prerogative of the NCCN, the sectoral authorities, and the members of the government concerned. The NCCN organizes and directs communications in the event of a national cyber crisis (see National Cyber Emergency Plan).

The NCCN's 24/7 on-call service ensures the availability of CERT.be, which provides first-line support for national incidents and crises.

The NCCN provides legal and organizational support to sectoral authorities for the identification of critical infrastructures and Operators of Essential Services of Essential Services of essential services. It also contributes to the assessment of cyber risks that may disrupt the operation of Organizations of Vital Interest or certain events (see Chapter 3).

The NCCN manages the list of Organizations of Vital Interest and is responsible for coordinating the follow-up on and adaptation of the relevant regulations.

Finally, the NCCN continuously analyzes key national risks (including cyber risks) and conducts ad hoc risk analyses on special issues that present an increased risk, in cooperation with all relevant partners.

4.6 State Security (VSSE)

The mission of the State Security Service (VSSE) is to collect, analyze, and process intelligence on activities that threaten or could threaten the internal security of the state, the external security of the state, or the state's scientific and economic potential.

As part of its mission, the VSSE maintains appropriate contacts with and gathers intelligence from foreign ancillary services, and shares the information received as much as possible with CERT.be and with other relevant partners.

4.7 The Federal Public Service Foreign Affairs

The roles of the Federal Public Service Foreign Affairs in terms of cybersecurity are:

- Acting as an International Single Point of Contact at the diplomatic level, both bilaterally and within relevant multilateral organizations (including EU, NATO, OSCE), especially at times of crisis.

- Determining Belgium's representation in international negotiations and dialogues, in consultation with the relevant Belgian authorities.

- Informing relevant Belgian authorities of pertinent international evolutions.

- Defining a position in international dossiers, in agreement with all the Belgian authorities concerned.

- Coordinated or uncoordinated international attribution of malicious cyber activities.

- Offering its experience to the competent authorities (CCB), as well as the environment of an international network for observing and analyzing online security problems, such as cyber threats, vulnerabilities in ICT systems, or cyber incidents.

4.8 The National Security Administration (NSA)

The National Security Administration is preeminent in the realm of information security, albeit the most sensitive data or "classified" information.

The Cybersecurity Strategy in this document addresses four distinct audiences. Three of these audiences are also among those targeted by the National Security Administration:

- Companies
- Government Services
- Organizations of Vital Interest

For companies and government agencies, the NSA is developing a number of products that allow for better protection of classified information in a cyber environment. The use of data encryption developed by the NSA can take the security of classified information in the cyber domain to the next level, in both the private and public spheres. For example, the national classified network, the development and organization of use of which still has to be worked out, will facilitate the secure exchange of information between public administrations, thus reducing cyber risks.

For certain vital organizations, the NSA can also perform security verifications (security advice or screening of sensitive occupations). To do so, it first requires these organizations to go through a risk analysis, threat analysis and impact analysis and to map out the security measures of their information systems. This process not only raises awareness of the measures taken by these organizations in the cyber domain, but also reinforces these measures.

4.9 The Coordination Unit for Threat Analysis (CUTA)

The responsibilities of the Coordination Unit for Threat Analysis (CUTA) include assessing the threat of terrorism and extremism. In the event of cyber threats or incidents that are (potentially) related to terrorist or extremist groups or ideologically or religiously inspired hacktivists, CUTA may conduct a threat analysis for the National Crisis Centre in cooperation with its partner agencies.

4.10 Sectoral authorities

The NIS Act of 7 April 2019 (establishing a framework for the security of network and information systems of general interest for public safety) and the implementing Royal Decree of 12 July 2019 specify how sectoral

authorities in Belgium are each responsible for the identification, standardization and inspections of Operators of Essential Services in their sector. The CCB and National Crisis Centre have an important advisory role in this. The NIS Act identifies six different sectors for Operators of Essential Services — Energy, Transportation, Finance, Digital Infrastructure, Healthcare, and Drinking Water — alongside digital services such as cloud computing services, online search engines, and online marketplaces.

4.11 The Belgian Institute for Postal Services and Telecommunications (BIPT)

The Belgian Institute for Postal Services and Telecommunications (BIPT) monitors the security of the electronic communications networks and services of telecom operators. For example, BIPT monitors operators' compliance with both legislation (e.g. risk analyses and related security measures) and its decisions, handles security incident reports (including incidents that constitute a personal data breach, in conjunction with the Data Protection Authority, APD-GBA), and has various powers to do its job (including issuing binding instructions to an operator). It also has a Crisis Response Team in case of the aforementioned incidents.

BIPT is also the sectoral authority and inspection service for the digital infrastructure sector (Internet Exchange Points, providers of DNS services and registries of top-level domain names) under the NIS Act and for the electronic communications and digital infrastructure sectors under the "Critical Infrastructures" Act.

Furthermore, BIPT is in charge of monitoring the application of the legal provisions transposing the Radio Equipment Directive, or RED (2014/53/EU), concerning products containing a radio functionality.

4.12 Federal Public Service Economy

The Federal Public Service Economy, SMEs, Self-Employed and Energy has the task of creating the conditions for a competitive, sustainable and balanced functioning of the goods and services market in Belgium. Given the increasing digitalization of our society and businesses, the FPS Economy is involved in several areas of cybersecurity.
It is the relevant administration for the identification, standardization and

supervision of the energy and digital service provider sectors under the NIS Act.
Victims of different types of cyber scams can report cyber fraud to Meldpunt/Point de contact, a service of the FPS Economy, which shares relevant data around these reports with the CCB and refers victims of cybercrime to the police.

Given the importance of SMEs to the Belgian economy, the FPS Economy will work more closely with the CCB to increase the cybersecurity of this group of companies.

4.13 Governance framework and consultation platforms

In addition to their own various responsibilities, collaboration among the stakeholders involved is a key factor in preventing, reducing, handling and monitoring cyber threats and incidents. Cybersecurity knowledge and the evolution of the cyber threat is shared between the relevant security agencies, public authorities, and the private and academic sectors via existing or new platforms. Regular meetings allow experts to share information and experiences in direct contact and to network with each other.

In Platform 4 Cyber of the Coordination Committee on Intelligence and Security (CCIV/CCRS), the intelligence and security services discuss general cybersecurity policies.

Consultation between the supervisory authorities of Organizations of Vital Interest takes place via the Cyber Security Sectoral Authority Platform (CySSAP).

The Cybercrime Expertise Network (REN) brings together experts from the public services in the area of cybercrime, for periodic consultation. This is coordinated by the General Prosecutor's Office in Antwerp.

The CSI/DPO platform (les Conseillers en Sécurité de l'Information/Data Protection Officers) brings together the security advisors and data protection officers of each government department. A specific meeting on cyber issues is organised every quarter as part of CCB/CERT's Quarterly Cyber Threat Report.

SIT (Synergy IT) is the platform for sharing knowledge and consulting between IT managers from all federal public services (Federal Public Services, public social security institutions and public utility Institutions). The SIT meets on a monthly basis, with the goal of initiating and following up on joint IT initiatives, both government contracts and projects, as well as providing technical input on G-Cloud initiatives.

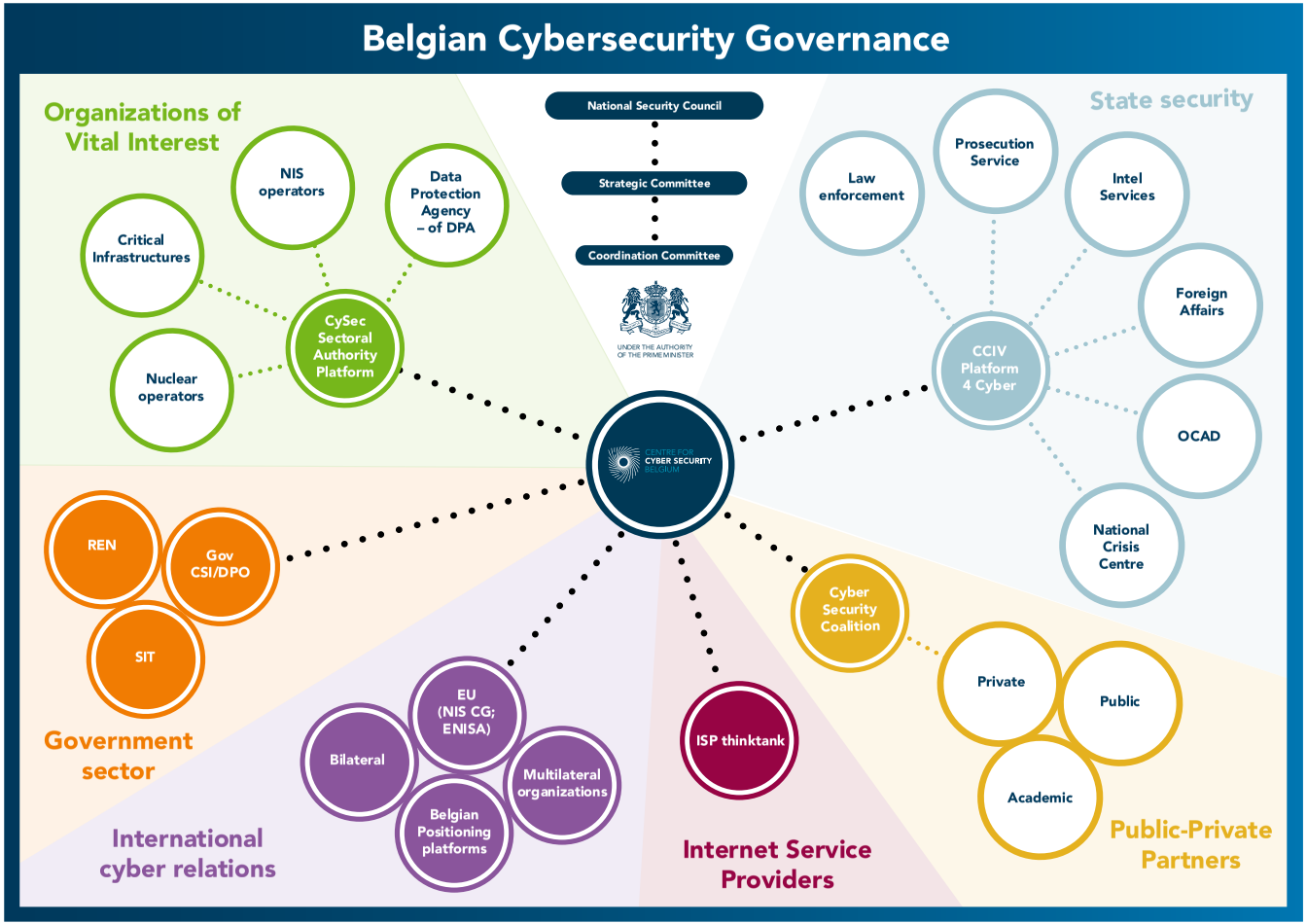
The development of formal Belgian positions in international discussions takes place through the proper channels of FPS Foreign Affairs.

The Interministerial Economic Commission (IEC) is an independent, flexible, technical-administrative coordination mechanism at the FPS Economy, SMEs, Self-Employed and Energy that can assist in defining and aligning the administrative positions of the federal and federated authorities in national, European and international dossiers.

IIn the ISP think tank, the CCB regularly consults with the largest internet service providers in Belgium regarding concrete measures and projects that can increase cybersecurity for Belgian citizens and companies.

The quarterly cyber threat reports, organized by the CCB and CERT.be, bring together several of these consultation platforms and inform all participants and Organizations of Vital Interest about the active threats.

The Cyber Security Coalition Belgium regularly brings together experts in the domain from the private, academic and public communities. This is done during experience-sharing events and in focus groups to discuss best practices, experiences or initiatives about various topics (cloud security, NIS, crypto, etc.)


Belgian Cybersecurity Governance
Organizations of Vital Interest
NIS operators
Data Protection Agency – of DPA
Critical Infrastructures
CySec Sectoral Authority Platform
Nuclear operators
National Security Council
Strategic Committee
Coordination Committee
UNDER THE AUTHORITY OF THE PRIME MINISTER
State security
Law enforcement
Prosecution Service
Intel Services
Foreign Affairs
CCIV Platform 4 Cyber
OCAD
National Crisis Centre
CENTRE FOR CYBER SECURITY BELGIUM
REN
Gov CSI/DPO
SIT
Government sector
Cyber Security Coalition
Private
Public
Academic
Public-Private Partners
EU (NIS CG; ENISA)
Bilateral
Multilateral organizations
Belgian Positioning platforms
International cyber relations
ISP thinktank
Internet Service Providers

5. Resources

To execute the stated vision and the six strategic objectives of this ambitious strategy, significant but essential additional investments are required. A clear commitment from the Belgian government to these resources is thus the cornerstone of this renewed national cybersecurity strategy. Indeed, increased cyber capacity is crucial to effectively and feasibly arm our economy, government services and Organizations of Vital Interest against ever-increasing cyber threats.

Investments in cybersecurity also have a direct and clear economic impact. If the government succeeds in inspiring and ensuring trust in "digital life", businesses and citizens will be more comfortable investing in more digital applications. This will boost productivity and economic growth in our country, and cyberattacks will be even more avoidable.

With this concrete investment commitment, Belgium is following the significant initiatives in neighbouring countries. In addition, the investments are referred to generate important confidence about the realistic implementation of our objectives, especially among our European and international partners. After all, many of them have an important office or representation in our country.

The mission to make Belgium one of Europe's least vulnerable countries in the cyber domain by 2025 is a collective effort. In addition to the CCB, other government departments, the intelligence and security services, as well as the business community, the Organizations of Vital Interest themselves, academia, and citizens each have individual responsibilities to achieve the ambitious goals set.

The federal government has an important responsibility in this, to set the direction but also to set the example. It will therefore build a credible cyber capability that can keep pace with other Belgian actors and seek to connect to the capabilities of our neighbouring countries.

Prepress and printing
Central printing office of the Chamber of Representatives

Brussels, May 2021

Responsible editor
Center for Cybersecurity Belgium
M. De Bruycker, Director
Rue de la Loi, 18
1000 Brussels
D/2021/14828/004