CENTRE FOR
CYBER SECURITY
BELGIUM

Nouvelle cyberstratégie belge : faisons de la Belgique un des pays les moins cybervulnérables d'Europe !

Security Forum

21/10/2021

Phédra Clouner

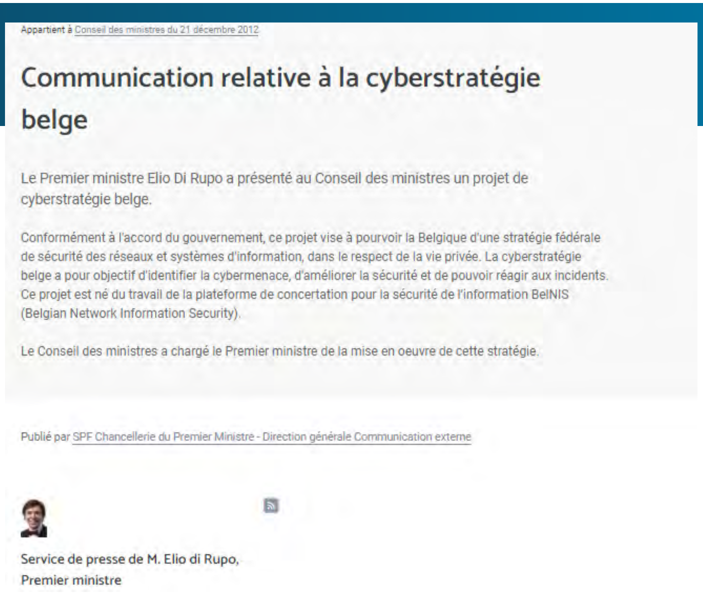
Deputy Director CCB

Agenda

- A new strategy! Why? Because the last (and first) one dates from 2012 !
- What did we do between 2012 and 2021?
  - CCB
  - Main realisations
- The new strategy!
  - Evolution of the cyber threat
  - We did a great job, but it’s time to evolve!
  - You want to know what’s in the new strategy? I’ll explain you!

The First One! Strategic objectives

- 2012!
- At this moment no Cybersecurity agency!
- In 2012 the cyber threat was already present and the Threat actors well identified (it doesn't change a lot)
- A safe and reliable cyberspace
  - Reliable working environment
  - Balance of rights and freedoms
  - Awareness of threats and responsibilities of all parties
- Optimal security and protection of critical infrastructure and government systems
  - Prevention of disruption or failure of critical infrastructure
  - Improved protection and monitoring of government systems
- Development of own cyber security capabilities
  - Own capacity => independent policy and incident management
  - In connection with international cooperation
  - Need for economic development with educational support



Appartient à Conseil des ministres du 21 décembre 2012

Communication relative à la cyberstratégie belge

Le Premier ministre Elio Di Rupo a présenté au Conseil des ministres un projet de cyberstratégie belge.

Conformément à l'accord du gouvernement, ce projet vise à pourvoir la Belgique d'une stratégie fédérale de sécurité des réseaux et systèmes d'information, dans le respect de la vie privée. La cyberstratégie belge a pour objectif d'identifier la cybermenace, d'améliorer la sécurité et de pouvoir réagir aux incidents. Ce projet est né du travail de la plateforme de concertation pour la sécurité de l'information BelNIS (Belgian Network Information Security).

Le Conseil des ministres a chargé le Premier ministre de la mise en oeuvre de cette stratégie.

Publié par SPF Chancellerie du Premier Ministre - Direction générale Communication externe

Service de presse de M. Elio di Rupo,
Premier ministre

RESULT?

- Guess what???

CENTRE FOR
CYBER SECURITY
BELGIUM

CERT.be
The Federal Cyber Emergency Team

Since January 2017

Legal basis

1. Monitoring, coordinating and supervising **the implementation of Belgian policy** on the subject;
2. Managing the various projects on the topic of cybersecurity using an **integrated and centralized approach**;
3. **Ensuring coordination** between the relevant government departments and governments, as well as the public authorities and the private or scientific sectors;
4. Formulating proposals aimed at **adapting the regulatory framework** in the field of cybersecurity;
5. **Ensuring crisis management** in case of cyber incidents in cooperation with the government's Coordination and Crisis Centre;
6. Preparing, disseminating and supervising the **implementation of standards, guidelines and security standards** for the various information systems of the governments and public institutions;
7. **Coordinating the Belgian representation in international cybersecurity forums**, coordinating the monitoring of international commitments and national proposals on this subject;
8. Coordinating the **security evaluation** and **certification** of information and communication systems;
9. **Informing and raising awareness** among users on information and communication systems.

Integration of the Computer Emergency Response team(Cert.be): new organisation (focus: incident handling- information sharing), more capabilities (24 FTE) – High level technical experts

Overview Main CCB Projects

1. Inform & Involve (home)

- Safeonweb.be
- BePhish: suspect@safeonweb.be
- Yearly Awareness campaign
- Election awareness

2. Empower & support (ovi)

- **Early Warning System**
- **Spear warning projects**
- Incident response
- Exercises
- Penetration testing for gov
- Technical Expert Training
- We help our hospitals

3. Guide & Assist (work)

- Cyber Security Reference Guide
- Baseline Information Security Guidelines
- Coordinated Vulnerability Disclosure Policy
- Vulnerability toolbox
- 5G/Supply Chain Guidelines
- Cyber Security Insurance
- Webinars

4. Govern

- National Strategy 2.0
- Cyber Emergency Plan
- NIS implementation
- Cybersecurity Act
- Cybersecurity Competence Centre
- Representation in international CS forums
- Cooperation with private and academic sector

But why a new strategy?

CENTRE FOR
CYBER SECURITY
BELGIUM

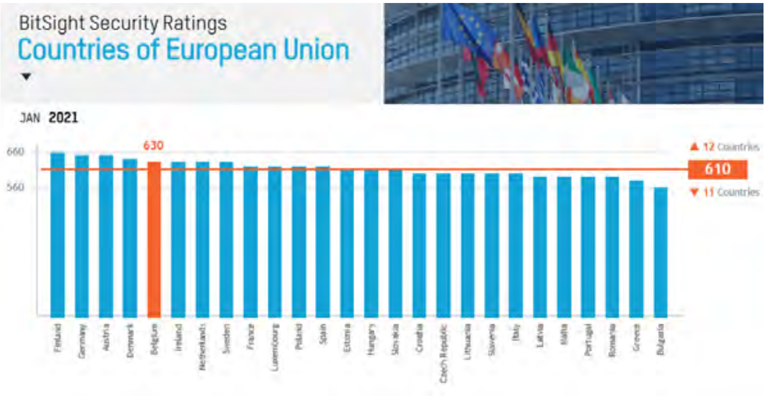
UNDER THE AUTHORITY OF
THE PRIME MINISTER

STRATÉGIE CYBERSECURITÉ
BELGIQUE 2.0
2021-2025

MAI 2021

.be

Since 2015, strong growth...



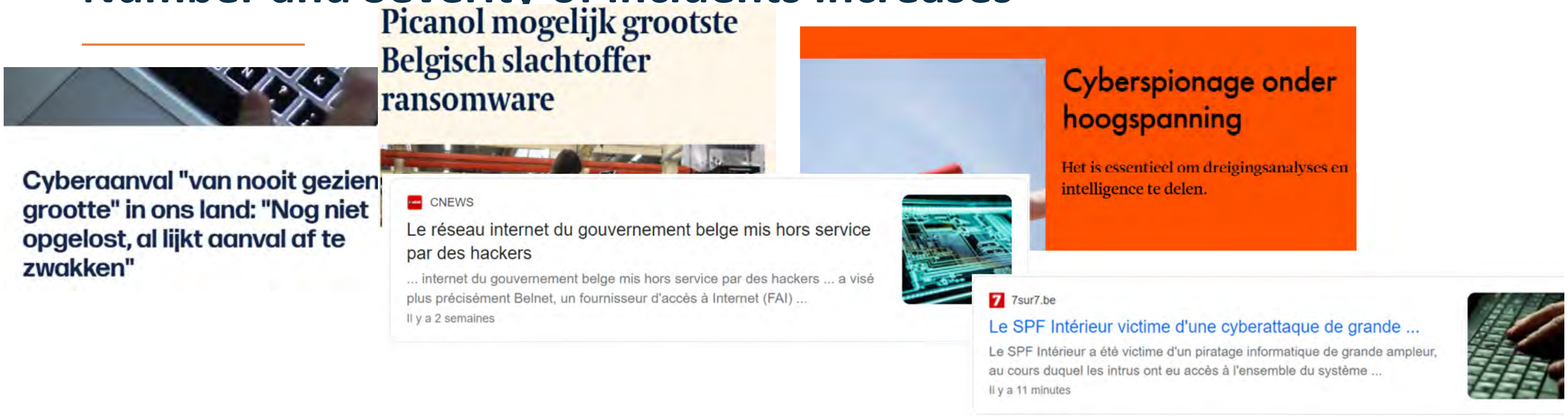
I genuinely believe **CCB is one of the leading European organizations in safeguarding cyberspace** and promoting public-private cooperation. Keep up the good work!

Costin Raiu, 15-01-2021

... but the threat is growing exponentially

facebook
Facebook helps you connect and share with the people in your life.
Sign Up
HACKED

Number and Severity of incidents increases



Cyberaanval "van nooit gezien grootte" in ons land: "Nog niet opgelost, al lijkt aanval af te zwakken"

Picanol mogelijk grootste Belgisch slachtoffer ransomware

Cyberspionage onder hoogspanning

Het is essentieel om dreigingsanalyses en intelligence te delen.

CNEWS

Le réseau internet du gouvernement belge mis hors service par des hackers

... internet du gouvernement belge mis hors service par des hackers ... a visé plus précisément Belnet, un fournisseur d'accès à Internet (FAI) ...

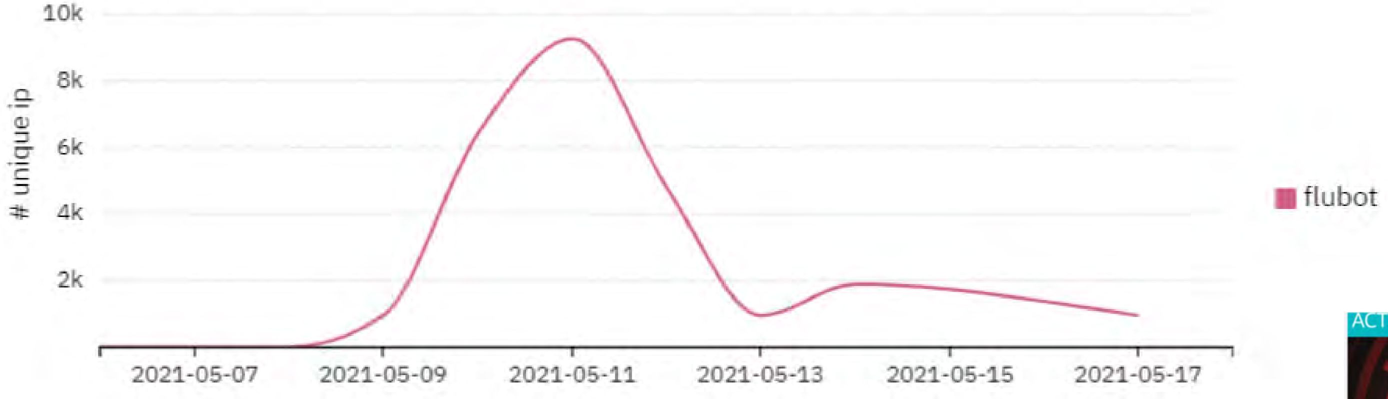
Il y a 2 semaines

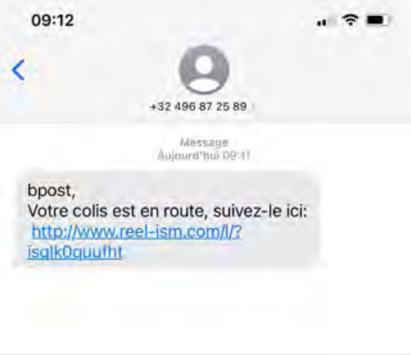
7sur7.be

Le SPF Intérieur victime d'une cyberattaque de grande ...

Le SPF Intérieur a été victime d'un piratage informatique de grande ampleur, au cours duquel les intrus ont eu accès à l'ensemble du système ...

Il y a 11 minutes





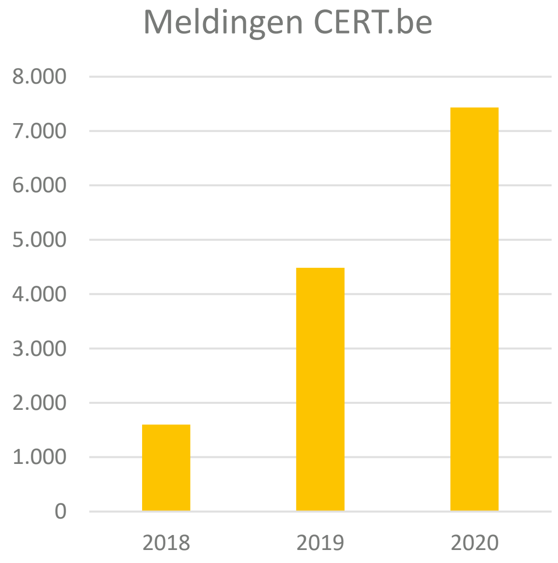
bpost,
Votre colis est en route, suivez-le ici:
http://www.reel-ism.com/l/?isqlk0quufht

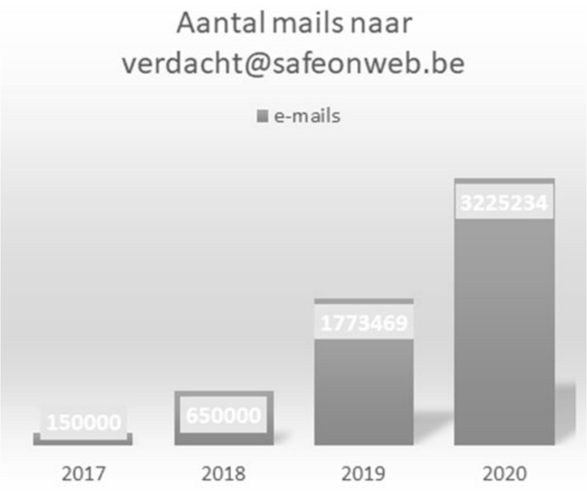
ACTU DES SOC

Attaques Hafnium-ProxyLogon : le rançongiciel DearCry sévit désormais sur Exchange

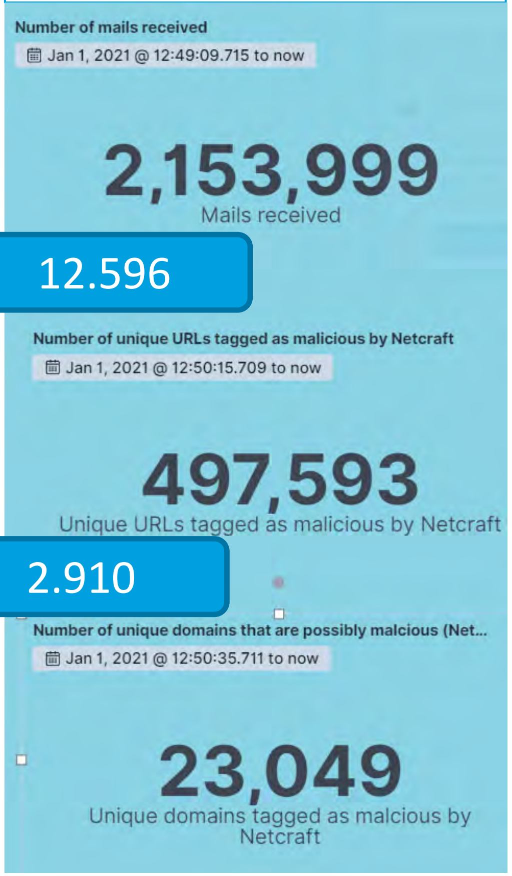
CENTRE FOR CYBER SECURITY BELGIUM

The cyber has become one of the most significant threats





2021



Number of mails received

Jan 1, 2021 @ 12:49:09.715 to now

2,153,999

Mails received

12.596

Number of unique URLs tagged as malicious by Netcraft

Jan 1, 2021 @ 12:50:15.709 to now

497,593

Unique URLs tagged as malicious by Netcraft

2.910

Number of unique domains that are possibly malcious (Net...

Jan 1, 2021 @ 12:50:35.711 to now

23,049

Unique domains tagged as malcious by Netcraft

And… 2.800.000 hits per month (redirect)

CENTRE FOR
CYBER SECURITY
BELGIUM

Important Threats

The 5 Most Important Threats in Belgium

- Phishing
  - Daily threat -> verdacht@safeonweb.be
  - Retrieval of login data
- DDoS (distributed denial-of-service)
  - Recent incidents: Belnet etc
  - Interruption of services
- Mobile Malware
  - Android Malware: Flubot & Teabot
  - SMS with link to install malicious application
  - Attacks on banking applications
- Ransomware Attacks
  - Ransomwares: Avaddon, Ruyk, Eight
  - Hijacking of IT systems with the aim of ransomware and/or stealing data
- Advanced Persistent Threats
  - Recent case

Impact of Cyber attacks

- Every 40 seconds, a company in the world falls victim to a planned and organised attack, which is usually only discovered after an average of 200 days.
- 60% of Belgian companies have already been hacked at one time or another and almost 30% expect to be hacked in the near future“ (Agoria)
- In 2018, the number of cyber attacks targeting Belgian SMEs increased by 194%.
- According to the insurer Hiscox, Belgian companies misjudge the cost of a cyber security incident. According to them, a hacker attack costs 9,000 euros, whereas in reality, the damage amounts to an average of 136,000 euros. A cyber attack can cost a small Belgian company with a turnover of EUR 500,000 up to EUR 133,000 (2020°
  - It’s difficult for the victims to evaluate the cost of a cyber incident! (direct and indirect)
- Not all companies report cyber attacks.

Content

1 Policy context

2 4 Stakeholders

3 Vision & Mission

4 4 Threats– 3 risks

5 6 Objectives

6 Collaboration

7 Ressources

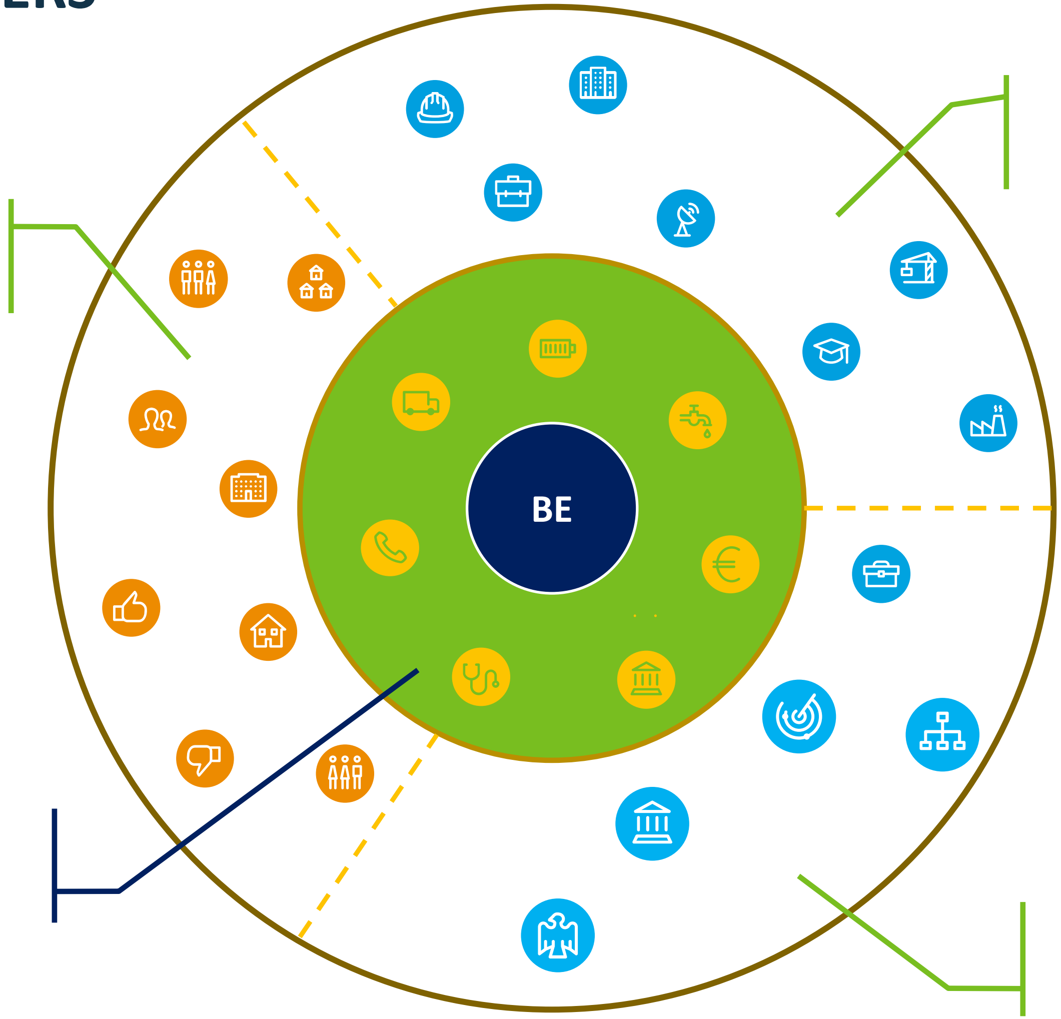
CENTRE FOR CYBER SECURITY BELGIUM

STRATÉGIE CYBERSECURITÉ BELGIQUE 2.0 2021-2025

MAI 2021

.be

STAKEHOLDERS



Population

- All citizens

Companies

- Self-employed
- SME
- Large companies & establishments

Organizations of Vital Interest

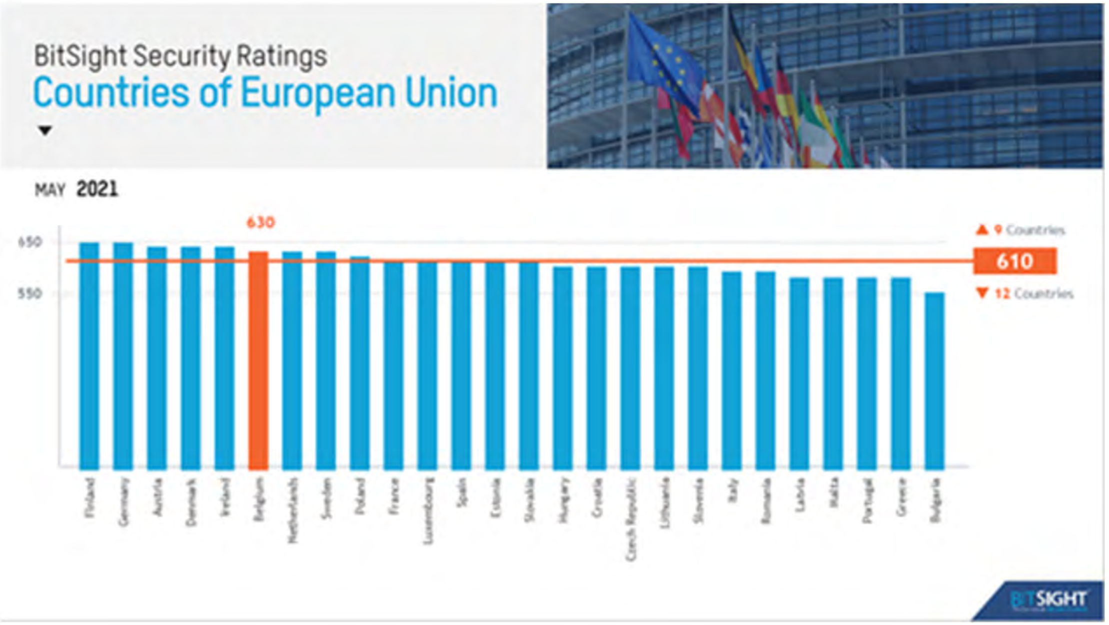
- Operators of Essential Services & DSP
- Critical Infrastructure
- Nuclear Installations

Government Services

Vision

An open, free, and secure cyberspace where citizens and companies can fully develop themselves, where they can engage internationally, and where fundamental rights are safeguarded and protected. We advocate a shared responsibility approach and indicate Cybersecurity as crucial to guarantee for society's trust in the digital space.

Make Belgium one of the least cyber vulnerable countries in Europe by 2025



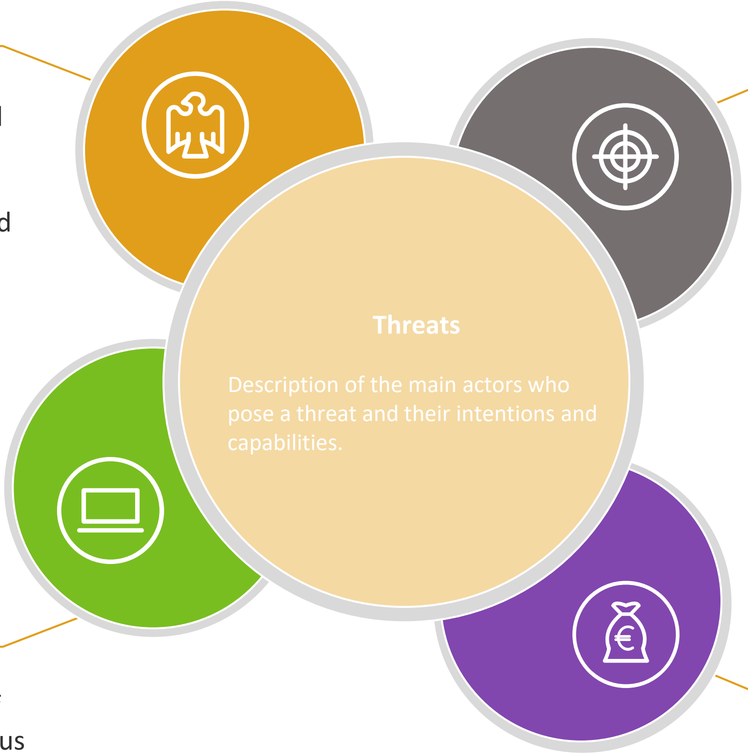
4 Threat actors

Foreign military and intelligence services

Countries have plenty of physical weapons, an offensive cyber arsenal and intelligence with which to inflict economic damage on other states, with a view to political instability and weakening their defences.

Terrorism

Cyber terrorists use the internet to commit acts of violence for the purpose of gaining a political advantage and instilling fear in the population.



Threats

Description of the main actors who pose a threat and their intentions and capabilities.

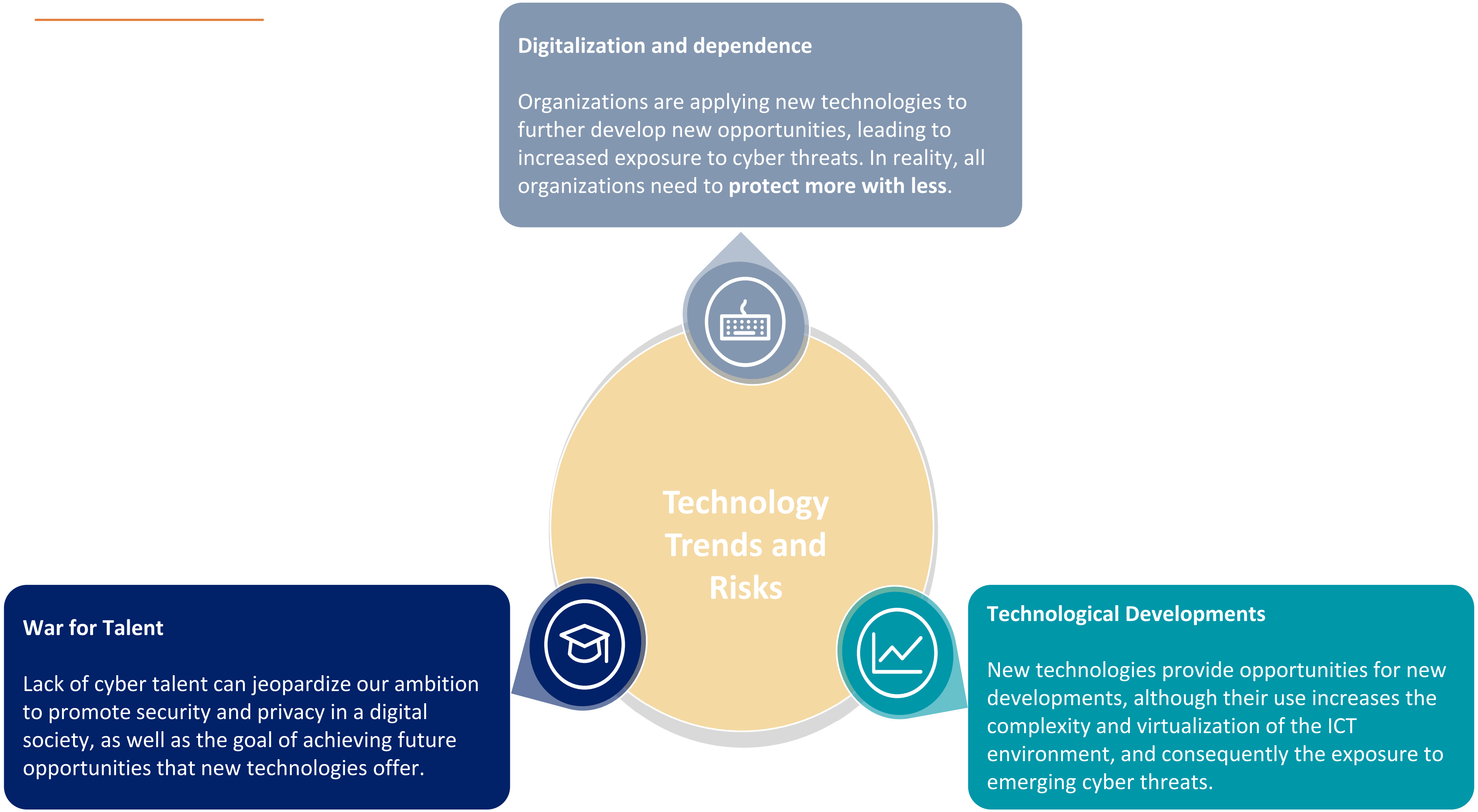
Hacktivism

Hacktivism is performing intentional cyber activities with the intention of promoting a political agenda, religious belief or social ideology.

Cybercrime

The goal of cyber criminals is to misuse computers, the internet or networks for financial gain.

3 Technology trends and risks



Digitalization and dependence

Organizations are applying new technologies to further develop new opportunities, leading to increased exposure to cyber threats. In reality, all organizations need to **protect more with less**.

Technology Trends and Risks

War for Talent

Lack of cyber talent can jeopardize our ambition to promote security and privacy in a digital society, as well as the goal of achieving future opportunities that new technologies offer.

Technological Developments

New technologies provide opportunities for new developments, although their use increases the complexity and virtualization of the ICT environment, and consequently the exposure to emerging cyber threats.

Belgian National Cybersecurity Strategy 2021-2025

6 Strategic Objectives

1. Strengthening the digital environment, and increasing trust in the digital environment
2. Arm users and administrators of computers and networks
3. Protecting Organizations of Vital Interest (OVI) against all cyber threats
4. Responding to the cyber threat
5. Improving public, private, and academic partnerships
6. A clear international commitment

Strategic objectives

1) Strengthen the digital environment and increase trust in the digital environment

1.1 Investing in a secure network infrastructure → **resilience**

1.2 Establishing a Cyber Green House → innovation

1.3 Foster expertise and knowledge → knowledge

1.4 Cybersecurity Certification and Labelling → trust & supply chain

1.5 Strengthening the skills of intelligence and security agencies → be capable

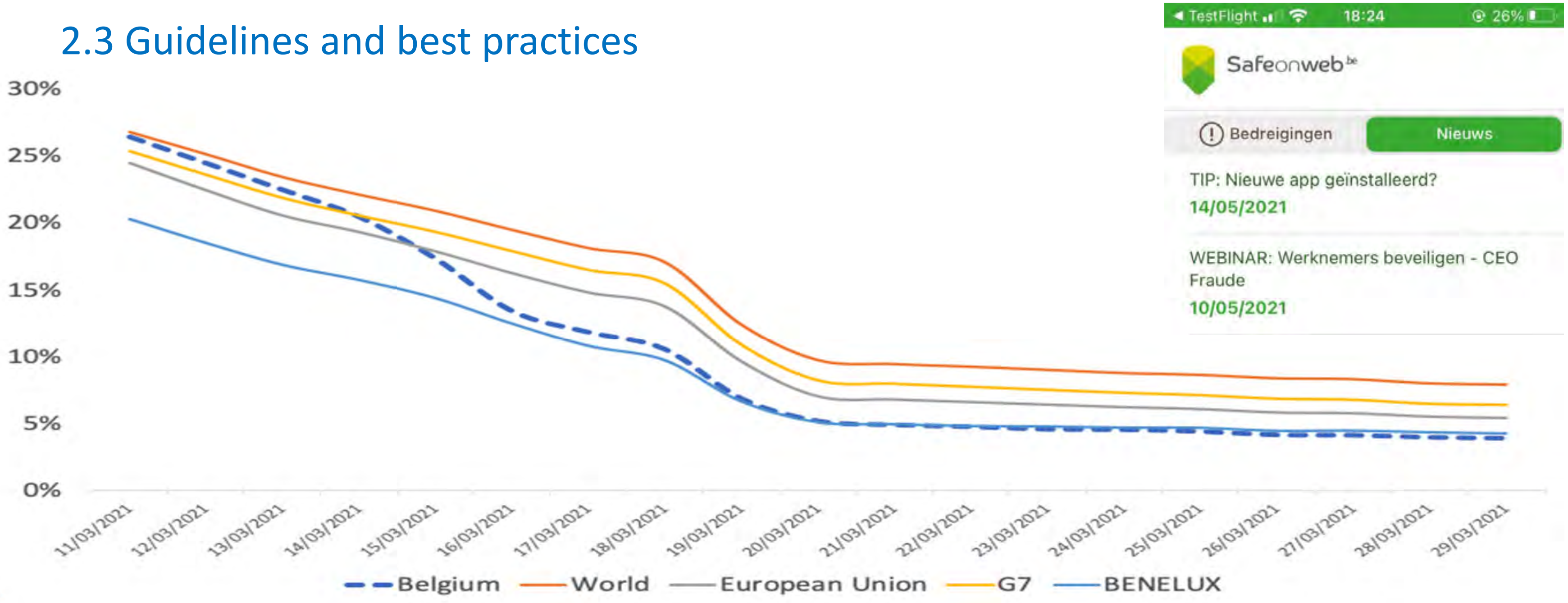
Strategic objectives

2) Arming users and administrators of computers and networks

2.1 Raise awareness and involve

2.2 Informing about threats & vulnerabilities ➔ **spear warning**

2.3 Guidelines and best practices



TIP: Nieuwe app geïnstalleerd?
14/05/2021

WEBINAR: Werknemers beveiligen - CEO Fraude
10/05/2021

CENTRE FOR CYBER SECURITY BELGIUM

BITSIGHT

Strategic Objectives

3) Protect Organizations of Vital Interest against all cyber threats

3.1 Information exchange and alerts -> Early Warning System

3.2 Protection for international institutions -> Operators of Essential Services

3.3 Being able to handle incidents with national impact

3.4 Exercises

Strategic Objectives

4) Responding to the cyber threat

4.1 Mapping the international threat -> Cyber intelligence

4.2 Disrupting criminal cyberinfrastructure -> active filtering

4.3 Appropriate repressive capacity -> high tech crime response

4.4 Appropriate Defence capability -> Cyber in military operations

4.5 Attribution -> diplomacy

STRATEGIC OBJECTIVES

5) Improve public, private and academic collaborations

5.1 Coordination and cooperation

➔ The internet is no public space

5.2 Supporting the Cyber Security Coalition

CYBER SECURITY
COALITION.be

6) A clear international commitment

6.1 Role of the EU, NATO and other relevant international organizations

* An open, free and secure cyber-environment

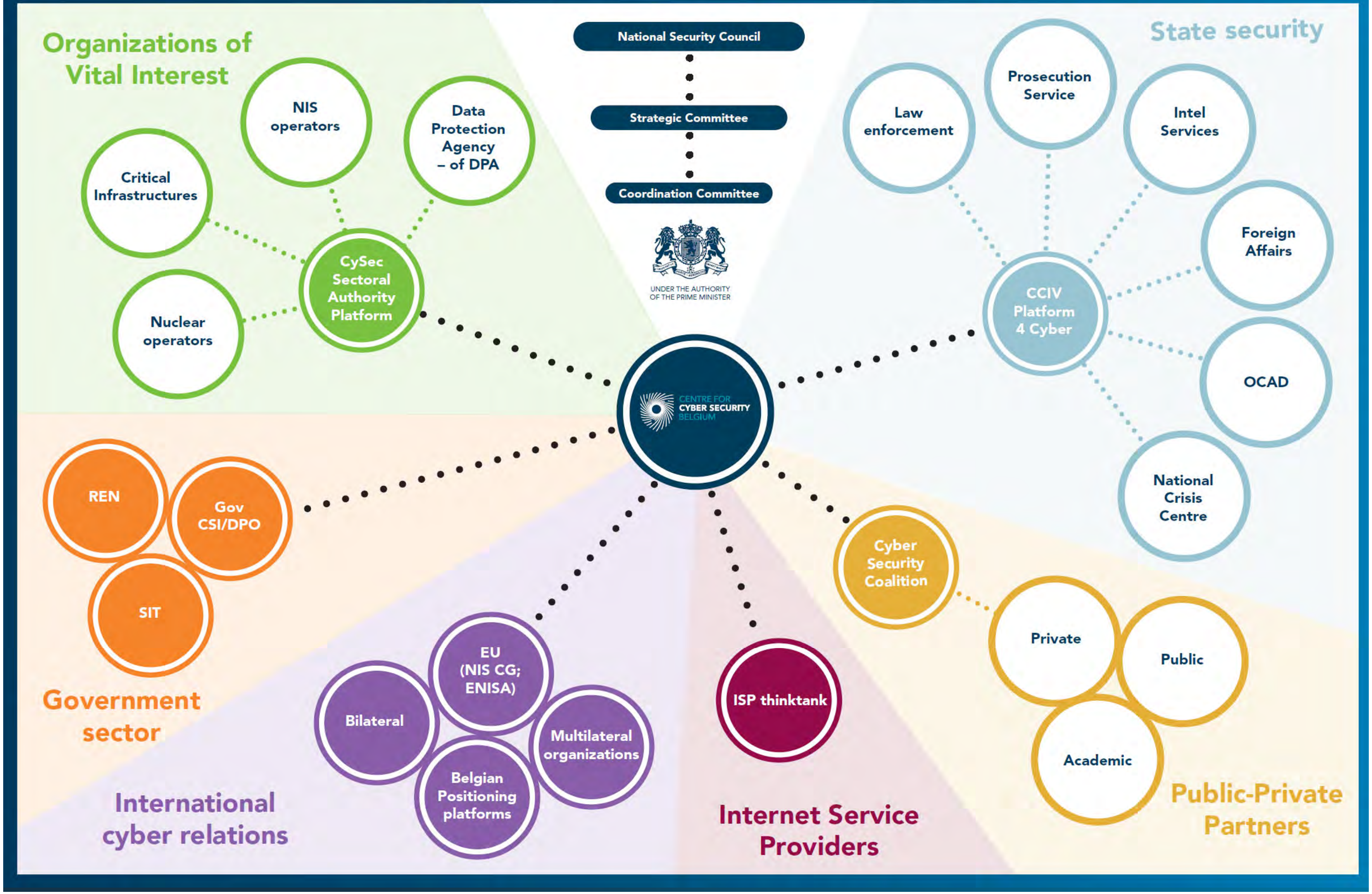
* The European Cyber Security Agency: ENISA

6.2 Bilateral cooperation

Responsibilities

- The Centre for Cyber Security Belgium (CCB)
- The Federal Police
- The Public Prosecutor's Office
- Defense
- The National Crisis Centre (NCCN)
- State Security Service (VSSE)
- The Federal Public Service Foreign Affairs
- The National Security Administration (NVO)
- The Coordination Unit for Threat Assessment(CUTA- ocam)
- Sectoral authorities
- The Belgian Institute for Postal Services and Telecommunications (BIPT)
- Federal Public Service Economy

Belgian Cybersecurity Governance



National Security Council

Strategic Committee

Coordination Committee

UNDER THE AUTHORITY OF THE PRIME MINISTER

CENTRE FOR CYBER SECURITY BELGIUM

Organizations of Vital Interest

- CySec Sectoral Authority Platform
- Critical Infrastructures
- NIS operators
- Data Protection Agency – of DPA
- Nuclear operators

State security

- CCIV Platform 4 Cyber
- Law enforcement
- Prosecution Service
- Intel Services
- Foreign Affairs
- OCAD
- National Crisis Centre

Government sector

- REN
- Gov CSI/DPO
- SIT

International cyber relations

- EU (NIS CG; ENISA)
- Bilateral
- Multilateral organizations
- Belgian Positioning platforms

Internet Service Providers

- ISP thinktank

Public-Private Partners

- Cyber Security Coalition
- Private
- Public
- Academic

National Cybersecurity Strategy 2.0

Let's make Belgium one of the least vulnerable countries in Europe!

[*https://ccb.belgium.be/nl/nieuws/een-cyberstrategie-20-om-van-belgi%C3%AB-een-van-de-minst-kwetsbare-landen-van-europa-te-maken*](https://ccb.belgium.be/nl/nieuws/een-cyberstrategie-20-om-van-belgi%C3%AB-een-van-de-minst-kwetsbare-landen-van-europa-te-maken)

[*https://ccb.belgium.be/fr/actualit%C3%A9/une-cyberstrat%C3%A9gie-20-pour-propulser-la-belgique-au-rang-des-pays-les-moins-vuln%C3%A9rables-d*](https://ccb.belgium.be/fr/actualit%C3%A9/une-cyberstrat%C3%A9gie-20-pour-propulser-la-belgique-au-rang-des-pays-les-moins-vuln%C3%A9rables-d)

CENTRE FOR CYBER SECURITY BELGIUM

Questions?

Phedra.clouner@ccb.belgium.be