CENTRE FOR
CYBERSECURITY
BELGIUM

Cyber security: current and future threats & actions

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

.be

Centre for Cybersecurity Belgium (CCB)

CENTRE FOR CYBERSECURITY BELGIUM

General Management:

- **Miguel de Bruycker**, Director General
  - **Phédra Clouner**, Deputy Director General
  - Comity of Directors

Figures :

- Created in **August 2015**
- Under the authority of **the Prime Minister**
- **135 FTE (2/3 Egov)**

As National Authority for Cybersecurity

Law of 26 April 2024 establishing a framework for the cybersecurity of network and information systems of general interest for public security.

NIS2

- Leadership and Coordination
- NIS2 Identification, Registration, and Supervision
- Policies, Standards and Guidelines (CyFun.eu)
- National and International Cooperation
- Awareness and Support
- Proposing Legislative Reforms

As National CSIRT

NIS2

- **Respond to incidents** and assist affected entities.
  - Conduct **forensic analysis** and maintain situational awareness.
  - Participate in the **EU CSIRT network** and offer mutual assistance.
  - Promote **standardized practices** for incident response & crisis management
- **Collaborate, collect and share information** with relevant communities
  - Issue **early warnings** and alerts about cyber threats and incidents (EWS).
  - Perform **proactive vulnerability scans** upon request from entities.
  - **Detect and analyze** cybersecurity issues.
- **Coordinate vulnerability disclosures**
- Build **partnerships with private sector** stakeholders.

Current and future threats

A lot of uncertainty if we do not change course soon

Primo: Societal control mechanisms

CENTRE FOR CYBERSECURITY BELGIUM

Laws	Define prohibited behaviors	National laws on cybercrime
Law Enforcement Police	Surveillance of violations	Very poor Cyber Surveillance
	Identify suspected actor & acts	No digital identity
Criminal Justice System Courts	Determine guilt	Rare convictions
	Impose sanctions or punishment	Rare enforcement of sanctions

“Without balanced Cyber Control Mechanisms,
we will never be able to protect our citizens, enterprises, and governments.”

AI-Driven Cyber Threats

CENTRE FOR CYBERSECURITY BELGIUM

- **87% security experts encountered AI-driven cyberattacks** the past year.
- AI-enhanced malware now exhibits **31.7% greater propagation rates**
  - and achieves an average dwell time of **97 days before detection**,
    compared to 42 days for conventional threats.
- **Adaptive malware** that mutates in real-time using machine learning
- **AI-supported phishing campaigns**
  - **80%** of observed social engineering
  - Deepfake Attacks (already IN Belgium !)

Cybercrime damages are expected to hit $10 trillion in 2025

AI Empowerment

- BAD
  - Lowered skill barrier
  - Zero Day discovery
  - Malware development
  - Deep Fakes/phishing
  - Automated attacks
  - Automated victim selection
  - …

- GOOD
  - AI empowered detection
    - But no data access
  - Intelligent Information Sharing
    - Blocked by rules (GDPR…)
  - Fast adoption
    - Budget & Procurement procedures
  - …

Geographical Threat Rebalancing

- Nation-state actors focus on critical infrastructure
  - Telecom, energy, transport and healthcare sectors
  - Much more resources for espionage and sabotage
- We focus more on physical threats and military operations
  - Drones, missiles, ships …
- Political priorities
  - Budget driven

Weakened cyber defenses

- 54% of large organizations view **supply chain challenges**
  - as the biggest barrier to achieving cyber resilience
- The rise of **Ransomware-as-a-Service (RaaS)** models
- **Cloud security** incidents from 24% **to 61%** in the past 12 months
- **Quantum computers** capable of breaking 2048-bit RSA encryption
  - **unlikely before 2055-2060**
  - But already "Harvest Now, Decrypt Later"
- Huge IoT **Operational Relay Box** networks

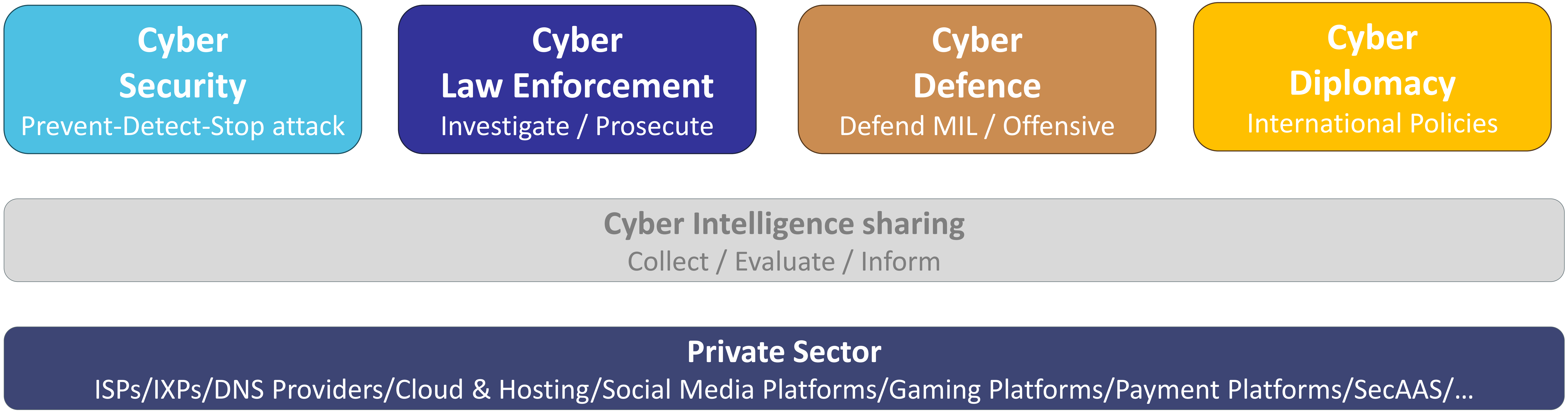
Trying to find solution

National Cybersecurity Strategy 3.0

BE Cyber **Governance**

CENTRE FOR
CYBERSECURITY
BELGIUM

Federale Politie
Police Fédérale



Cyber Security
Prevent-Detect-Stop attack

Cyber Law Enforcement
Investigate / Prosecute

Cyber Defence
Defend MIL / Offensive

Cyber Diplomacy
International Policies

Cyber Intelligence sharing
Collect / Evaluate / Inform

Private Sector
ISPs/IXPs/DNS Providers/Cloud & Hosting/Social Media Platforms/Gaming Platforms/Payment Platforms/SecAAS/…

Cyber Domains

Cybersecurity

- **Protecting the networks and computer systems** of citizens, businesses, government services (excluding Defence systems), and vital organisations, increasing resilience.
- The key actions are identifying & **detect threats, technically handling incidents**, and coordinating warnings and assistance.
- The competent authority is the **Centre for Cybersecurity Belgium (CCB)**.

Cyber Law Enforcement

- **Identification and prosecution of** computer-related **crimes and their actors**.
- The goal is to punish cyber-related offences in Belgium, thereby stopping or deterring criminal actors and, where possible, disrupting infrastructure used for criminal purposes.
- The lead authority in this domain is the Public Prosecutor's Office

Cyber Domains

Cyber Defence

- **Military intelligence and security operations** in and from the cyberspace operational domain.
- It involves conducting operations in cyberspace, monitoring cyber threats from state actors, **technical attribution of incidents to state actors**, and overseeing the **cybersecurity of Defence networks and weapons systems.**
- The competent authority is **Cyber Command**

Cyber Diplomacy

- **Diplomatic means to promote international agreements and norms of behaviour** in the cyber domain
- **Safeguard Belgian** political, economic, and/or cultural **interests** ; and to discourage, prevent, and remedy the escalation of cyber conflicts.
- **Political attribution and potential sanctions** also fall under this domain.
- The competent authority is **Foreign Affairs**

Detect more in order to protect better

CENTRE FOR CYBERSECURITY BELGIUM

Domain	Actions
Identify Threats & Vulnerabilities	Extend **vulnerability scanning** Extend **threat intelligence** (buy & exchange) Capacity Building - Innovation & Training (Cyber Ranges & Exercises) **Awareness Raising**
Protect all systems	**CyFun for all** **Security by design** (EU CRA implementation) **Digital Trust** ➔ **Digital Identity**, **E-Fraud Coordination** **Quantum Safe Crypto**
Detect attacks	**AI powered detection tools** **Extend Spear Warning** with **Netflow data** to detect communication with malicious infrastructure and send warning Improved **collaboration with cloud providers**
Respond & stop attack	**Block access to malicious infrastructure** Part of the solution or part of the problem Collaboration with **Online Law Enforcement**
Recover	**Resilience** **Public – Private – Partnerships** **Financial Support for Third Parties** (FSTP)

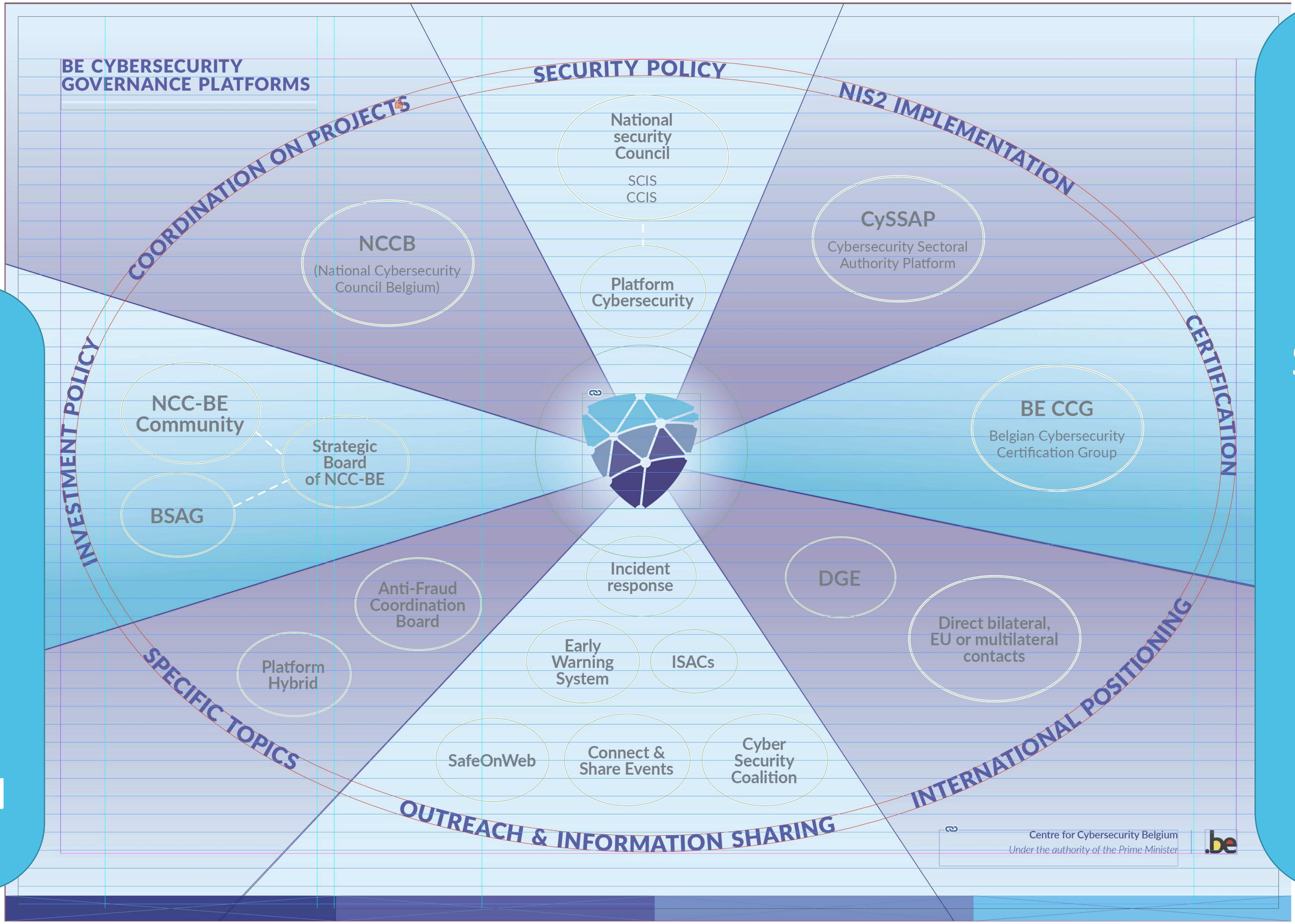
CCB collaborations

CENTRE FOR
CYBERSECURITY
BELGIUM

The main Challenge remains to

BUILD:

TRUST
RESPECT
COLLABORATION
GOVERNANCE


BE CYBERSECURITY
GOVERNANCE PLATFORMS
SECURITY POLICY
NIS2 IMPLEMENTATION
CERTIFICATION
INTERNATIONAL POSITIONING
OUTREACH & INFORMATION SHARING
SPECIFIC TOPICS
INVESTMENT POLICY
COORDINATION ON PROJECTS
National security Council
SCIS
CCIS
Platform Cybersecurity
CySSAP
Cybersecurity Sectoral Authority Platform
NCCB
(National Cybersecurity Council Belgium)
BE CCG
Belgian Cybersecurity Certification Group
NCC-BE Community
Strategic Board of NCC-BE
BSAG
Anti-Fraud Coordination Board
Platform Hybrid
Incident response
Early Warning System
ISACs
DGE
Direct bilateral, EU or multilateral contacts
SafeOnWeb
Connect & Share Events
Cyber Security Coalition
Centre for Cybersecurity Belgium
Under the authority of the Prime Minister
.be

NCSC
CSIRTs
Law Enforcement
Defense
Intelligence
Sectorial Authorities
Telecom
Financial
Economy
Consumer Prot.
Regions
Private Sector Org
Anti-Scam Org
Academia

CENTRE FOR
CYBERSECURITY
BELGIUM

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

Rue de la Loi / Wetstraat 18 - 1000 Brussels

www.ccb.belgium.be

.be