# 25 YEARS

## OF CYBER JUSTICE

CYBER SECURITY
**COALITION**

IGO
IFJ

hosted in Brussels by

**BNP PARIBAS**
**FORTIS**

# Your hosts:

## Catherine Van de Heyning

Public Prosecutor; Professor
European Fundamental Right
University of Antwerp

## Baptiste Flumian

Cybercrime Reference Magistrate
Brussels Public Prosecutor's Office

CYBER SECURITY
COALITION

IGO
IFJ

hosted in Brussels by
BNP PARIBAS
FORTIS

**Despina Spanou**

Deputy Director-General

European Commission

**Miguel**
**De Bruycker**

Managing
Director General

Centre for
Cybersecurity
Belgium

CENTRE FOR
**CYBERSECURITY**
BELGIUM

# Lessons from 25 years of Belgian resilience

## The evolving battlefield

# 2000–2006:
## **Internet-scale** outbreaks & **first nation-state** hints

- Worm era: Code Red, Slammer, Blaster, Sasser
  - expose **patch-latency and monoculture risks**
- Early espionage: Titan Rain
  - intrusions against Defense & tech firms normalize long-dwell exfiltration.
- Conceptual shift:
  - From “incident response” to threat-centric protection
- BELNIS-platform for cybersecurity created in 2003
- Creation of the first BE Cyber Defense (2005)

# 2007–2011:
## Cyber meets geopolitics

- **Estonia (2007):**
  - Politically motivated DDoS attacks
- **Georgia (2008):**
  - Cyber ops synchronized with kinetic movement.
- **Stuxnet (2010):**
  - Precision OT intrusion → physical degradation.
- BUZA Hack (2011)

# 2012–2016:
## **APT professionalization** & hybrid playbooks

- National strategy on cybersecurity 1.0 (2012)
    - *Lost chapter …*
- Crime-as-a-service
- APTs mature:
    - Living-off-the-land becomes standard
    - Multi-year footholds in government/defense
    - **BUZA Hack (…2013…2014)**
    - **Belgacom Hack (2013)**
    - Bangladesh Bank hack (feb 2016)
- Creation of the CCB (2014 – Aug 2015)

# 2017–2021:
# **Crime professionalization**, supply chain wake-up

- **Ransomware at scale**:
  - WannaCry, NotPetya show the externality of poor hygiene
  - wormable vulns → systemic risk.
- **Cloud era**:
  - **Misconfigurations** and stolen tokens drive **identity-layer** compromises.
- Supply chain:
  - **SolarWinds (2020),** Hundreds of large organizations, incl. US Gov.
- National Cybersecurity Strategy 2.0 (2021)
  - *Make Belgium one of the least vulnerable countries in the EU*

# 2021–2025:
## Online Fraud **professionalization** & AI acceleration

- **Ukraine** (2022):
  - support from **U.S. hyperscalers & large cloud providers**.
- **Escalation in cybercriminal activity**
  - *$10 trillion in 2025*
  - **Ransomware & Online fraud epidemic**
- Rise of Operational Relay Box networks

# 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
  - …

CENTRE FOR
CYBERSECURITY
BELGIUM

Centre for Cybersecurity Belgium
*Under the authority of the Prime Minister*

# CCB Now & the next 5 years

## National cybersecurity Strategy 3.0

# Centre for Cybersecurity Belgium (CCB)

## General Management:

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

## Figures :

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

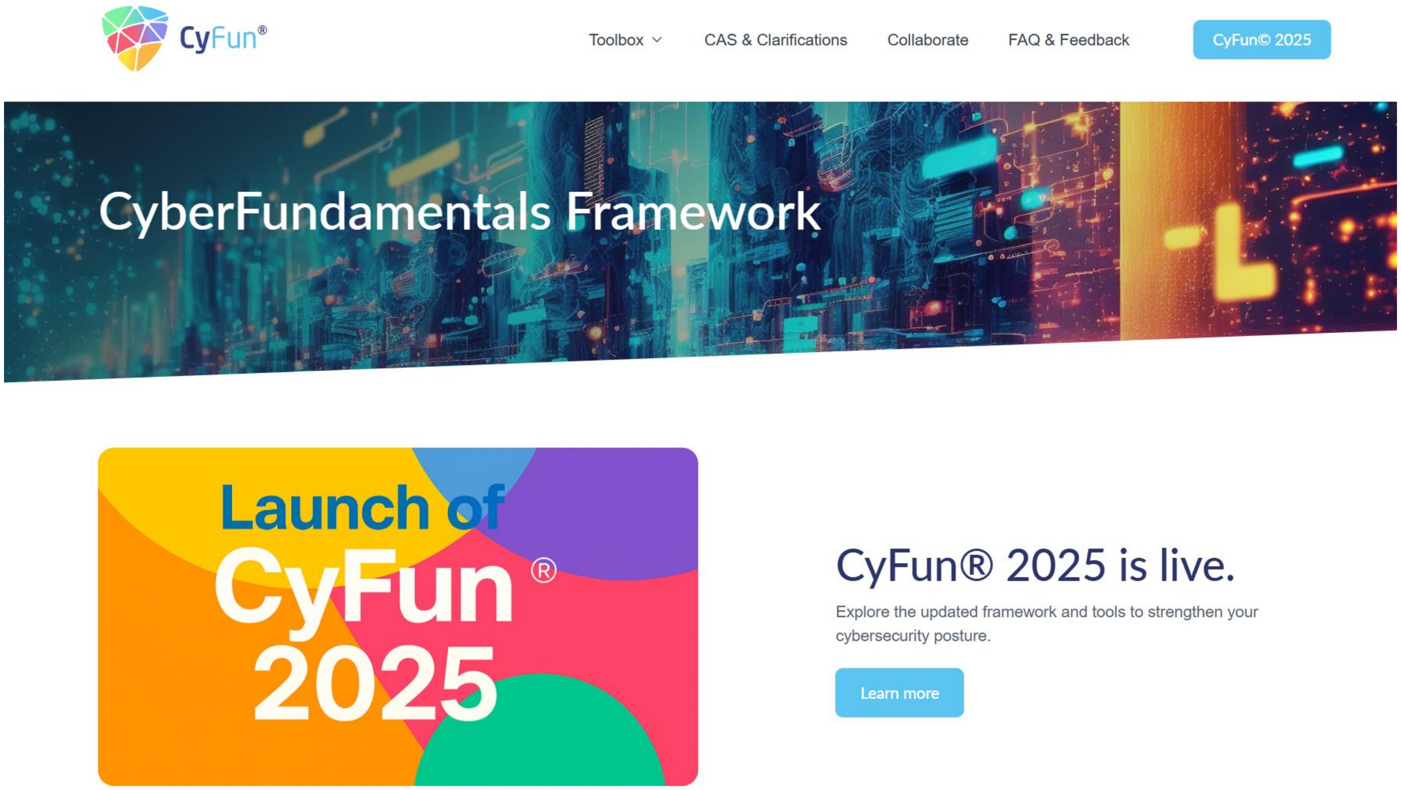
# As National Authority for Cybersecurity

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

**NIS2**

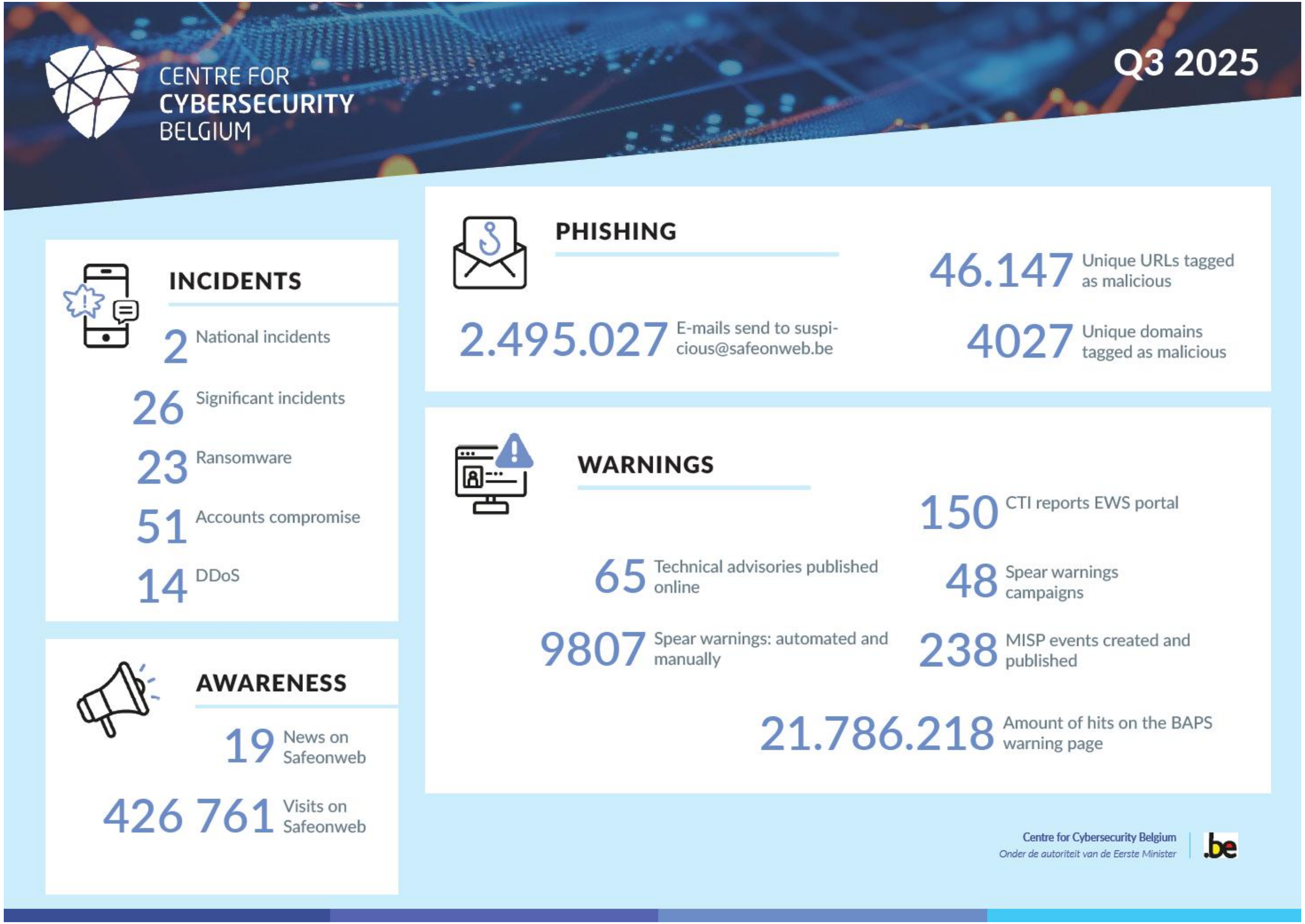
- National Cyber Security Incident Response Team (CSIRT)
- National Cyber Security Certification Authority (NCCA)
- National Coordination Centre (NCC)

# Cyber Fundamentals 2025



CyFun® 2025 is live.

Explore the updated framework and tools to strengthen your cybersecurity posture.



CENTRE FOR
CYBERSECURITY
BELGIUM

Q3 2025

## INCIDENTS

2 National incidents

26 Significant incidents

23 Ransomware

51 Accounts compromise

14 DDoS

## AWARENESS

19 News on Safeonweb

426 761 Visits on Safeonweb

## PHISHING

2.495.027 E-mails send to suspicious@safeonweb.be

46.147 Unique URLs tagged as malicious

4027 Unique domains tagged as malicious

## WARNINGS

150 CTI reports EWS portal

65 Technical advisories published online

48 Spear warnings campaigns

9807 Spear warnings: automated and manually

238 MISP events created and published

21.786.218 Amount of hits on the BAPS warning page

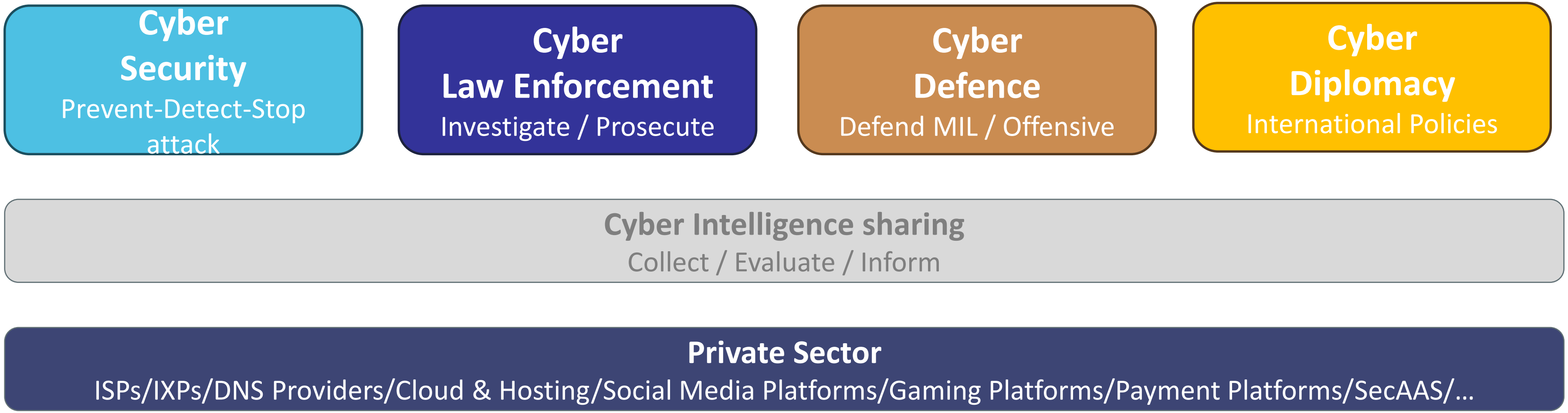
Centre for Cybersecurity Belgium
*Onder de autoriteit van de Eerste Minister*

.be

# 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/…

# New National Cybersecurity Strategy 3.0

CENTRE FOR CYBERSECURITY BELGIUM

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

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

**nis@ccb.belgium.be**

.be

## Jan Kerkhofs

Federal Magistrate

Head of the Cyber Unit of the Federal Prosecutor's Office

2000 – 2025

# A Quarter Century of Cyber Law in Action

*25 Years of the Belgian Cybercrime Law*

**Jan Kerkhofs**

Federal Magistrate • Head of Cyber Unit
Federal Prosecutor's Office

Cyber Security Coalition • IGO-IFJ

Brussels • 27 November 2025

# Why This Milestone Matters

> *"Belgium was among the first EU countries to implement comprehensive cybercrime legislation — a bold move that shaped European digital justice."*

**28**

**NOVEMBER 2000**

Belgium's foundational law on cybercrime

Wet van 28 november 2000 inzake informaticacriminaliteit, BS 3 februari 2001

**4**

**CORE OFFENCES**

Computer forgery, computer fraud, hacking, and sabotage criminalized

**4**

**NEW POWERS**

Data seizure, network search, duty to cooperate and electronic interception tools

THE ORIGIN

# The Bistel Case (1988)

Belgium's wake-up call for cybercrime legislation

### WHAT HAPPENED

Two young men — Halewyck & Panckoucke — hacked into BISTEL, the electronic communication system connecting Belgian cabinet ministers. Using PM Martens' unchanged password ("W.M. Wetstraat"), they accessed confidential ministerial agendas and mailboxes.

### THE LEGAL VACUUM

No specific computer crime laws existed. Prosecutors improvised with: forgery (using someone's password = "false document"), theft of computer energy, and interception of telecommunications.

### THE OUTCOME

First instance: conviction on three counts. Appeal court: largely overturned — existing law insufficient for computer crimes. Verdict: 9,000 BEF fine + 3 months suspended.

### THE LEGACY

*This case exposed the urgent need for specific cybercrime legislation — directly inspiring the 2000 Cybercrime Law we celebrate today.*

*August – October 1988: The hack that changed Belgian law*

# The 1990s: A Legal Vacuum

Why new legislation became urgent

## THE CHALLENGE

- No specific cybercrime provisions — prosecutors used general Criminal Code articles
- Internet and e-commerce boom creating new vulnerabilities
- Lack of procedural tools for digital evidence seizure and network investigation
- Council of Europe preparing Budapest Convention — Belgium wanted to lead

## THE RESPONSE

**ART. 210BIS**

Computer-related forgery

**ART. 504QUATER**

Computer fraud

**ART. 550BIS**

Illegal access (hacking)

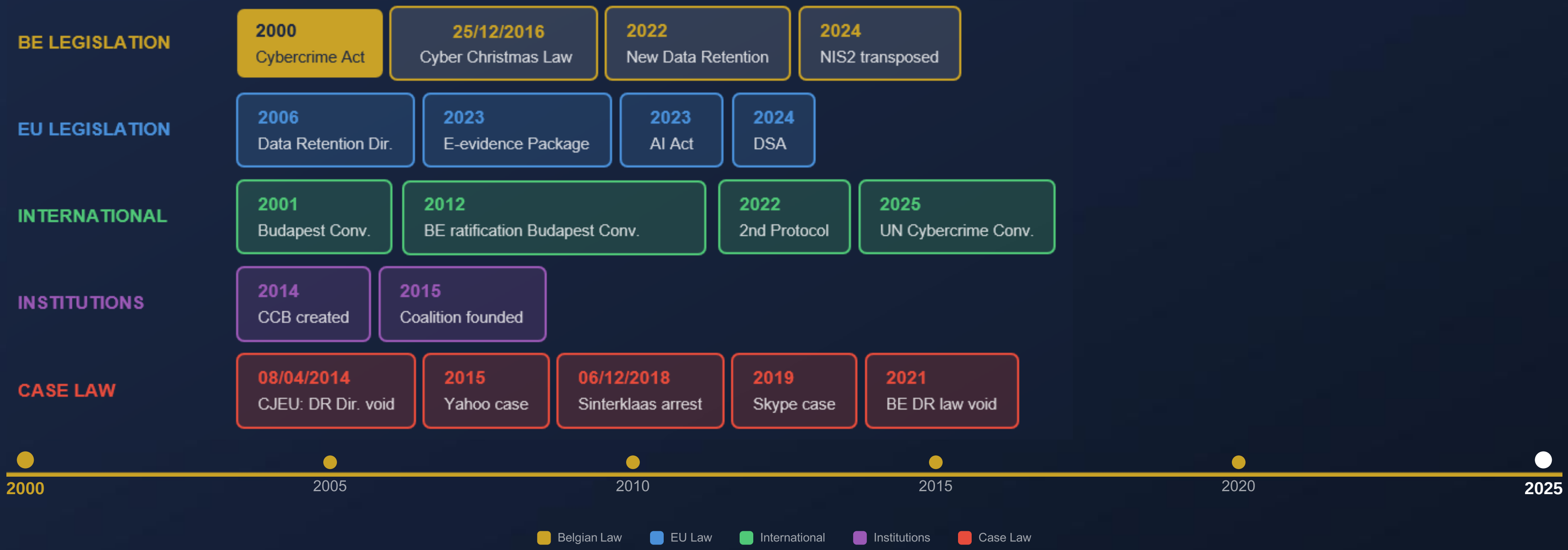
**ART. 550TER**

Data and system sabotage

Belgium implemented these provisions before the Budapest Convention opened for signature (November 2001)

# 25 Years of Evolution

Key legislative, judicial, and institutional milestones



**BE LEGISLATION**

- 2000 Cybercrime Act
- 25/12/2016 Cyber Christmas Law
- 2022 New Data Retention
- 2024 NIS2 transposed

**EU LEGISLATION**

- 2006 Data Retention Dir.
- 2023 E-evidence Package
- 2023 AI Act
- 2024 DSA

**INTERNATIONAL**

- 2001 Budapest Conv.
- 2012 BE ratification Budapest Conv.
- 2022 2nd Protocol
- 2025 UN Cybercrime Conv.

**INSTITUTIONS**

- 2014 CCB created
- 2015 Coalition founded

**CASE LAW**

- 08/04/2014 CJEU: DR Dir. void
- 2015 Yahoo case
- 06/12/2018 Sinterklaas arrest
- 2019 Skype case
- 2021 BE DR law void

# The Budapest Convention Framework

First international treaty on cybercrime — Belgium (fully) aligned since 2001, but only ratified in 2012

**81**
STATES RATIFIED

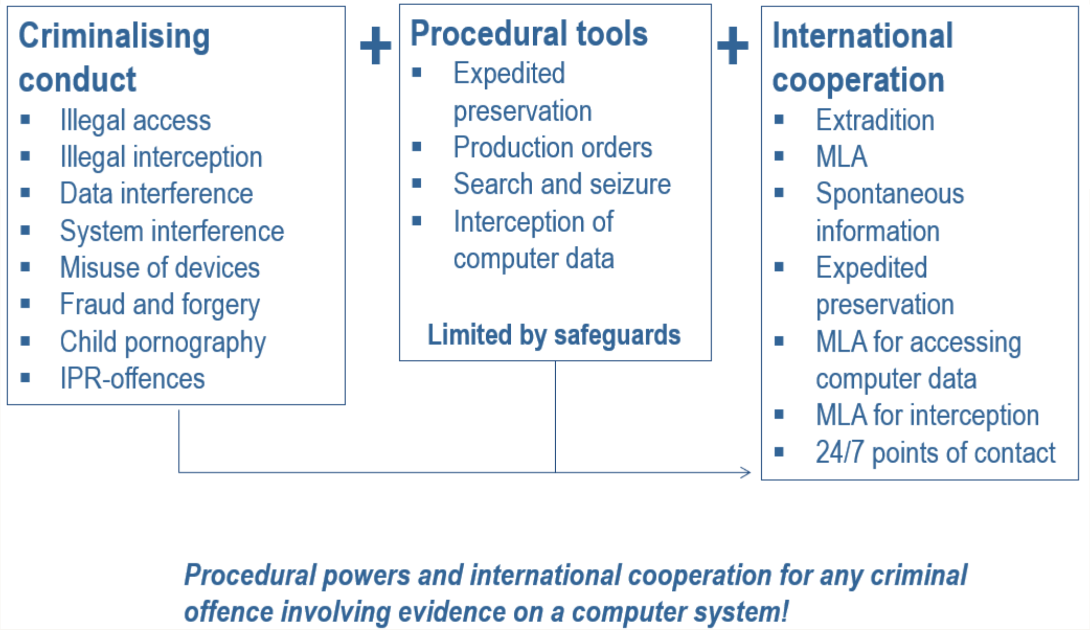
**16**
SIGNED or INVITED

as of 27/11/2025

KEY DATES

| | |
|---|---|
| Opened | **23 Nov 2001** |
| In force | **1 Jul 2004** |
| 2nd Protocol | **12 May 2022** |

Council of Europe Convention on Cybercrime, ETS No. 185



**Criminalising conduct**

- Illegal access
- Illegal interception
- Data interference
- System interference
- Misuse of devices
- Fraud and forgery
- Child pornography
- IPR-offences

+

**Procedural tools**

- Expedited preservation
- Production orders
- Search and seizure
- Interception of computer data

**Limited by safeguards**

+

**International cooperation**

- Extradition
- MLA
- Spontaneous information
- Expedited preservation
- MLA for accessing computer data
- MLA for interception
- 24/7 points of contact

***Procedural powers and international cooperation for any criminal offence involving evidence on a computer system!***

**2nd Additional Protocol (2022):** Direct cooperation with service providers, emergency MLA, joint investigation teams — Belgium was among the first 22 signatories on 12 May 2022

PROSECUTION SERVICE STRUCTURE

# The Public Prosecutor's Office & Cybercrime

Building expertise within the Belgian prosecution service

## EVOLUTION

**2006-2007** Working Group Internet Investigation

Addressed operational and legal questions in the digital investigation environment

**2008** College of Prosecutors-General Decision

Each district and Federal Prosecutor's Office must appoint cybercrime reference magistrates

**2015** REN Cybercrime Established

Working Group evolved into **Cybercrime Cel** in 2013 and finally in the Expertise Network (REN) Cybercrime under College of Prosecutors-General

**2018** Federal Prosecutor's Cyber Unit

Dedicated unit established: 4 magistrates + 3 lawyers/legal assistants

## CURRENT STRUCTURE

**REN Cybercrime**

College of Prosecutors-General | Coordination: PG Antwerp, AG Robrecht De Keersmaecker

**Federal Prosecutor**

Cyber Unit

4 magistrates + 3 lawyers/legal assistants

**District Offices**

Reference Magistrates

Min. 1 per district

**Local Cyber Units**

Some local prosecutor's offices have dedicated cyber units

**THE CHALLENGE**

General cyber-savviness among prosecutors remains low to moderate

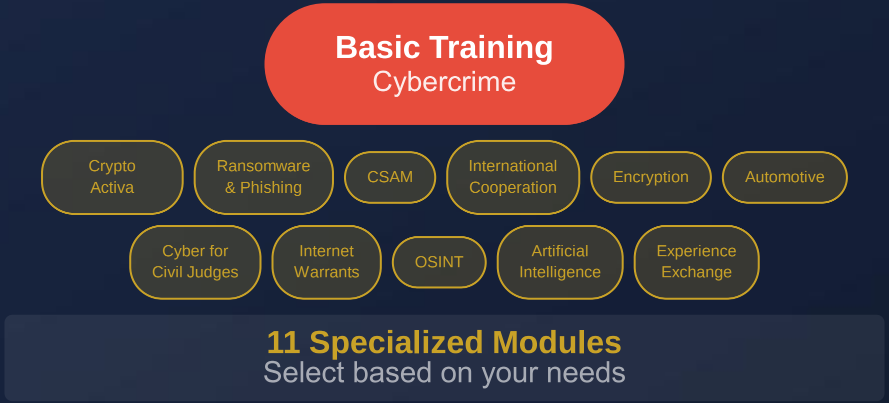
**THE RESPONSE: TRAINING**

Comprehensive training curriculum developed with IGO (Judicial Training Institute)

TRAINING STRATEGY

# From 2024: Modular Approach for cybercrime and electronic evidence training for judges and prosecutors

Cybercrime training curriculum developed with IGO



**Basic Training**
Cybercrime

- Crypto Activa
- Ransomware & Phishing
- CSAM
- International Cooperation
- Encryption
- Automotive
- Cyber for Civil Judges
- Internet Warrants
- OSINT
- Artificial Intelligence
- Experience Exchange

**11 Specialized Modules**
Select based on your needs

## BASIC TRAINING

KNOWLEDGE KERNEL: What every magistrate should know or be aware of. The essential foundation.

## TWO DAYS INSTEAD OF THREE

More accessible format with flexibility to return. More accessible for judges too.

## HALF-DAY MODULES AT IGO

Quick response to emerging issues. Annual updates without repeating basic training.

## TAILORED LEARNING

Select modules based on what you need. No one-size-fits-all approach.

*From static curriculum to dynamic, needs-based professional development*

# Building Enforcement Capacity

From scattered units to a structured cyber justice ecosystem

## POLICE SPECIALIZATION

| | |
|---|---|
| 1992 | Computer Crime Units (CCU) created within Judicial Police |
| 1995 | Gendarmerie establishes BOGO team |
| 1997 | National Computer Crime Unit at National Brigade (JP) |
| 2001 | **Police reform:** BOGO + NCCU merge into Federal Computer Crime Unit (**FCCU**) |

## CURRENT ECOSYSTEM

### Federal Computer Crime Unit (FCCU)

National level • Critical infrastructure • Policy • Training • International contact point

### 14 Regional Computer Crime Units (RCCU)

One per judicial district • Forensic investigation • Operational support • First responders

### CCB (Cyber Security Centre Belgium): CERT – CyTRIS - NCCN

National cyber security authority (2014)

### Cyber Security Coalition

unique partnership between players from the academic world, the public authorities and the private sector to join forces in the fight against cybercrime.(2015)

THE CAPACITY GAP

# FCCU: Then and Now

Federal Computer Crime Unit capacity vs. cybercrime reporting growth

## 2000

Central Judicial Reporting Point (FCCU)

**14** FCCU staff

**10** cyber agents

**50** reports/day

**2,359** reports/year (large dark number of course)

343 criminal cases identified, 322 child abuse related. Acute staff shortage noted.

## 2010

**33** FCCU staff

+136% growth from 2000

## 2019

**44** positions

**~20** filled

55% vacancy rate

## 2025

Safe on Web (CCB) handles now most citizen phishing/fraud reports (not complaints)

**70** positions

**~31** filled

55% vacancy rate

Handles critical infrastructure attacks, AI, crypto, encryption, darkweb, anonymizers...

## CCB-SAFE ON WEB 2024

**9,000,000** reports per year

**25,900** per day

**1.6M** links blocked

**44%** of citizens report

## THE DISPARITY

**3,815x** more reports

Citizen reports grew 3,815x since 2000

## FCCU CAPACITY GROWTH

**3x** more (effective) staff

14 (2000) to ~31 filled (2025)

*Reports grew 3,815x while capacity grew 3x. The math speaks for itself.*

High tech crime of the present and the future - Cybercrime as a Service (CaaS)

# Encrypted Communications

Belgian-led international cooperation in action

## SKY ECC – a new level

| | |
|---|---|
| 1B+ | communications |
| 70K | users |
| 650+ | new investigations opened or enriched (BE) |
| 160+ | judgements |
| 3100+ | years of prison sentence |

## Demonstrating Capabilities

### INTERNATIONAL JIT

Belgium, France, Netherlands — coordinated via Eurojust & Europol

### TECHNICAL INNOVATION

Live decryption of encrypted platform communications

### OPERATIONAL SCALE

200+ house searches, 1,500+ officers deployed on action day (March 9, 2021)

### ONGOING LEGAL DEBATES

Proportionality, cross-border evidence sharing, defence rights, …

THE CHALLENGE

# We Live in Extraordinary Times

## THE DATA EXPLOSION

**12 EB** 12 billion GB before 2000

All data humanity created in its entire history

**180 ZB** 180,000 EB in 2025

15,000× more than all pre-2000 data combined

**90%**

of all data ever created was generated in the last 10 years

> *"Data is becoming ever larger, more complex and, paradoxically, increasingly misunderstood."*

### THE MAGISTRATE'S REALITY

Armed with an (surgically adapted) 1808 code of criminal procedure, we remain stuck in outdated ways of thinking — **while cybercriminals effortlessly cross borders and hide behind encryption**.

### LET'S NOT KID OURSELVES

**Electronic evidence does not love us** — it lies and deceives, hiding behind uncooperative providers, VPNs and encrypted devices.

### LOSS OF LOCATION

**Shouldn’t we reinvent jurisdiction?** — who knows where data is and is it even still relevant?

> *"Data doesn't care about jurisdiction, but defence lawyers do — often armed with legal thinking from when the earth was still flat.“*

THE PARADOX

# The Earth is still flat?

**We are still stuck in the past**: outdated understanding of concepts of jurisdiction, proportionality and rule of law

### THE AGE-OLD DEFENSE STRATEGY

*"If you can't hit the rider, shoot the horse."*

When evidence is overwhelming, attack the procedure. Hide in the mass of data. Use encryption and jurisdictional chaos to bog down the system.

### THE PROPORTIONALITY PARADOX

Proportionality was conceived as a safeguard against state power that goes too far — but is now used as a shield for crime that goes too far.

The principle is not broken, but the context has imploded. Proportionality had meaning in an analogue world. In a world of 180 zettabytes, it becomes a semantic weapon rather than a guarantee of the rule of law.

### PROPORTIONALITY REDEFINED

Proportionality must be weighed against the precision of the investigative measure, the safeguards surrounding the use of that data, the finality of what you do with that data, and the seriousness of what you are trying to solve.

### 'HUMAN RIGHTS' HAS AN 'S'

Privacy is fundamental, but not the only right. There is also: the right to life of murder victims, the physical integrity of victims, the right of citizens to protection against organized crime.

### THE MAGISTRATE'S BURDEN

The noble but complex duty: to carefully weigh all interests and fundamental rights against each other, and this for all citizens. No high mass at the altar of a single fundamental right.

*"Justice takes no pleasure in interfering with fundamental rights, just as a surgeon takes no pleasure in cutting open a person to remove a tumor. But sometimes it is strictly necessary to save lives."*

*“Have we really evolved that much? We still treat the earth as if it were flat - we are just seeding more sophisticated crops."*

# Lessons from 25 Years & call to action

What worked — and the challenges ahead

## ✓ SUCCESS FACTORS

### Proactive Legislation

Belgium legislated before Budapest Convention — ahead of the curve, not catching up

### Continuous Updates

Regular amendments (2006, 2016, 2024) kept pace with threats and international standards

### Public-Private Partnership

A solid public-private cooperation routine has been established

### International Alignment

Full Budapest compliance; early NIS2 transposition; active in EJCN and T-CY

Panel discussions today will explore these challenges in greater depth

## PERSISTENT CHALLENGES

### AI preparedness

**AI-enabled crime demands AI-enabled (legal) response**

A deepfake attack every 5 minutes: AI powered phishing, voice/video cloning, synthetic evidence, AI generated CSAM…

### Capacity Constraints

Specialized units face staffing pressure vs. explosion in digital evidence volume and emerging challenges

### Data Retention issues

**Justified concerns, but a distorted debate**

The EC is preparing initiatives to go towards a new data retention regime in the EU

### (End-2-end) Encryption

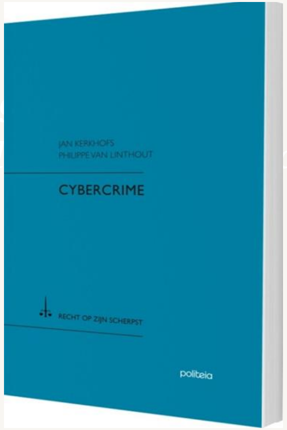
How to deal with encryption in harmony with fundamental rights concerns

### Public-private and international cooperation & cross border e-evidence gathering

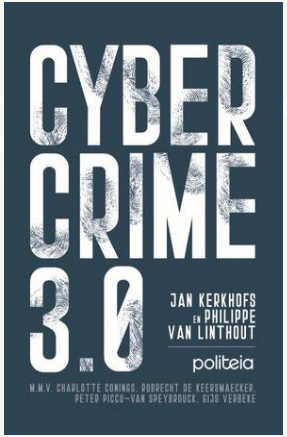
Implementation of the EU E-evidence package – implementation 2AP Budapest Convention – Implementation UN Convention

# The handbook

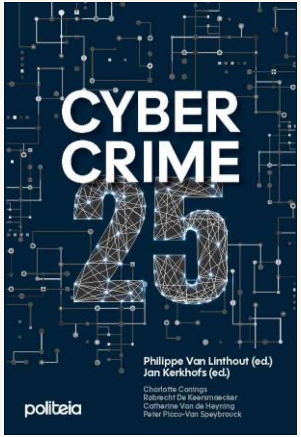
"Bel the first EU countr comprehensive cyb — a bold d European digital



2013


CYBER CRIME 3.0
JAN KERKHOFS EN PHILIPPE VAN LINTHOUT
politeia
M.M.V. CHARLOTTE CONINGS, ROBRECHT DE KEERSMAECKER, PETER PICCU-VAN SPEYBROUCK, GIJS VERBEKE

2019



2025

politeia

# Thank You

*Questions & Discussion*

**Jan Kerkhofs**

Federal Magistrate • Head of Cyber Unit

Federal Prosecutor's Office

Belgian representative to the European Judicial Cybercrime Network (EJCN)
National and International Cybercrime Trainer • Council of Europe Expert

# Coffee break

See you back
at 11:45 AM !

## Luuk Dekkers

Postdoctoral Researcher

The Hague University of Applied Sciences

Centre of Expertise Cyber Security

# Cybercrime offenders: who are they?

Dr. Luuk Bekkers
Postdoctoral researcher

The Hague University of Applied Sciences
Netherlands Institute for the Study of Crime and Law Enforcement (NSCR)

# Broader trends

- Society is digitizing, and so is crime
- Digital environment offers new opportunity structure
  - New crimes *and* changes in the crime script
- Crime always has an online and offline component!

# Definitions

- “Any crime that is facilitated or committed using a computer, network, or hardware device” (Gordon & Ford, 2006)

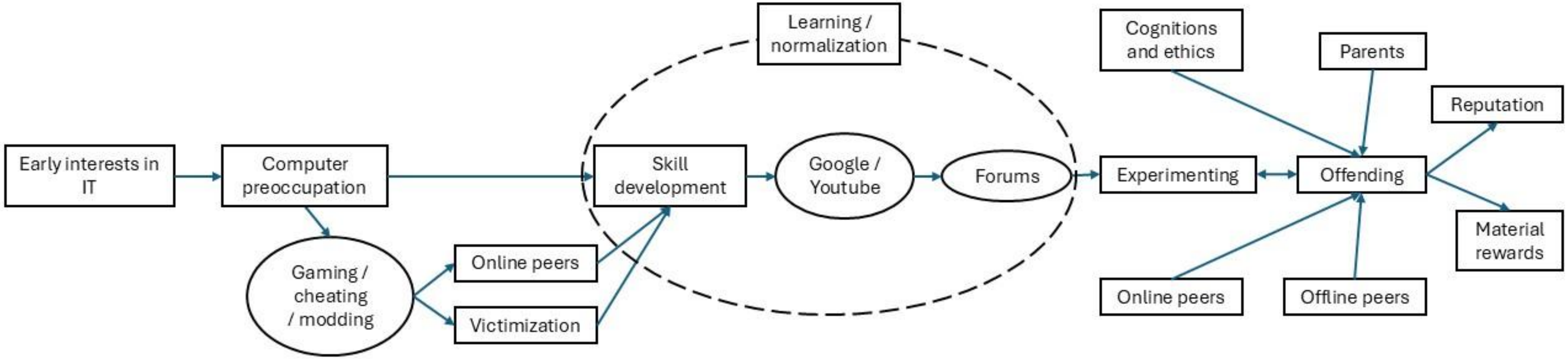
- Cyber-dependent crimes -> committed with and aimed at IT
  - DDoS attacks, ransomware, hacking, etc.

- Cyber-enabled crimes -> crimes that are supported by IT
  - Financially-motivated cybercrime / online frauds
  - Interpersonal cybercrime
  - Sex crimes

Are we dealing with a new offender group?

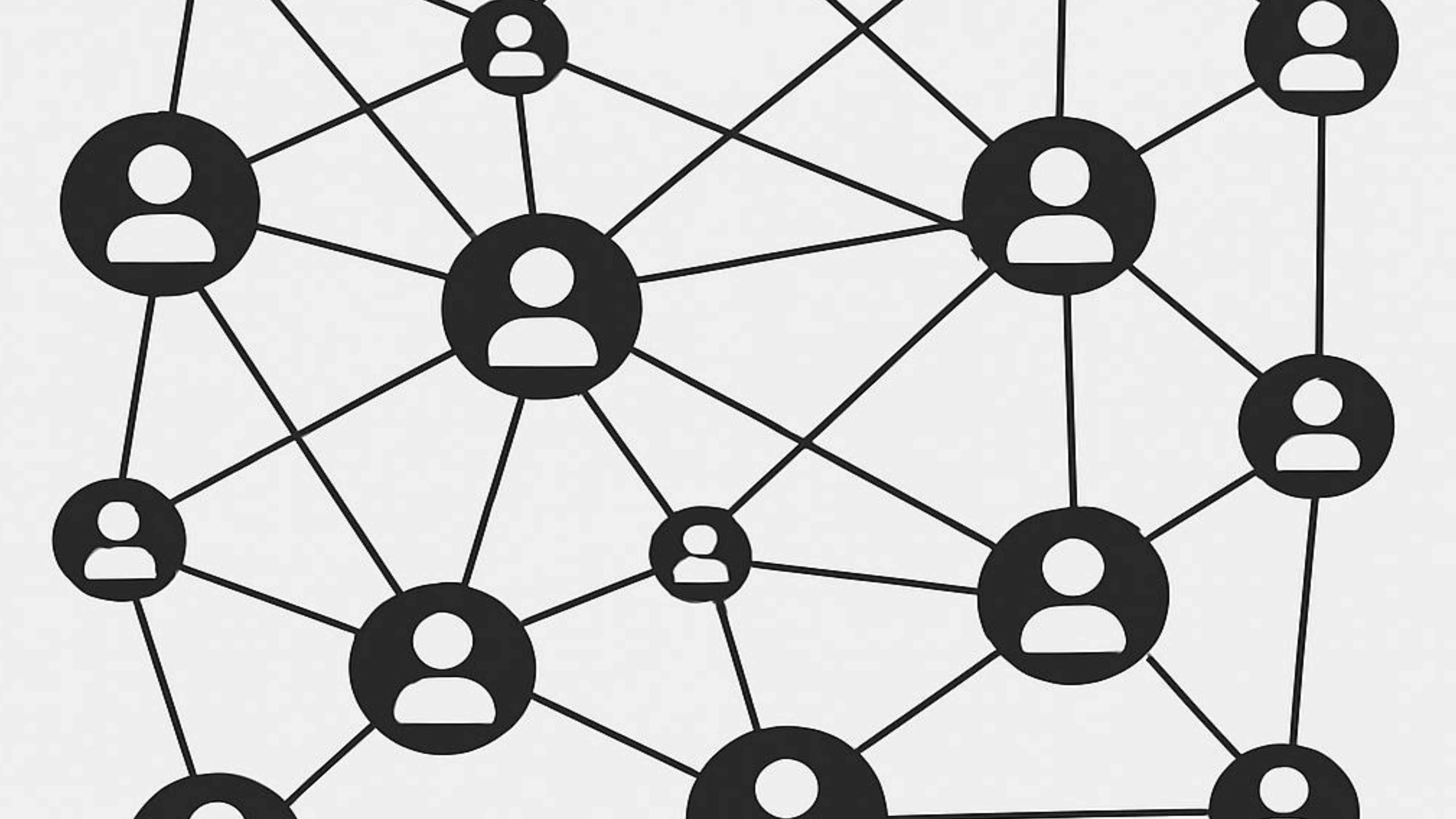
# Hackers

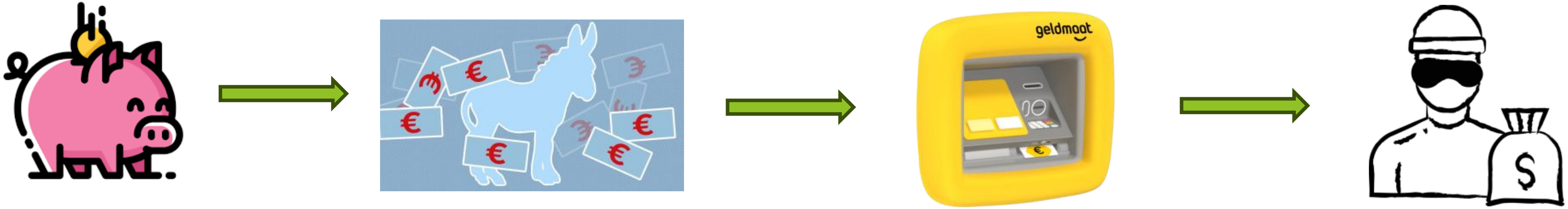
- What was considered protective may actually provide opportunity for hacking:
  - Higher levels of self-control
  - Jobs/educations in IT
  - Programming skills
- But also:
  - Lack of online parental supervision
  - Exposure to deviant peers online and offline
- Tend to specialize in cybercrime


Early interests in IT
Computer preoccupation
Gaming / cheating / modding
Online peers
Victimization
Learning / normalization
Skill development
Google / Youtube
Forums
Cognitions and ethics
Parents
Reputation
Experimenting
Offending
Material rewards
Online peers
Offline peers

# Financial cybercrime offenders

- More like traditional offenders
  - Higher in Dark Triad traits
  - Suspended from school
  - Lack of leisure activities
  - Deviant peer influences




geldmaat

# Financial cybercriminal networks

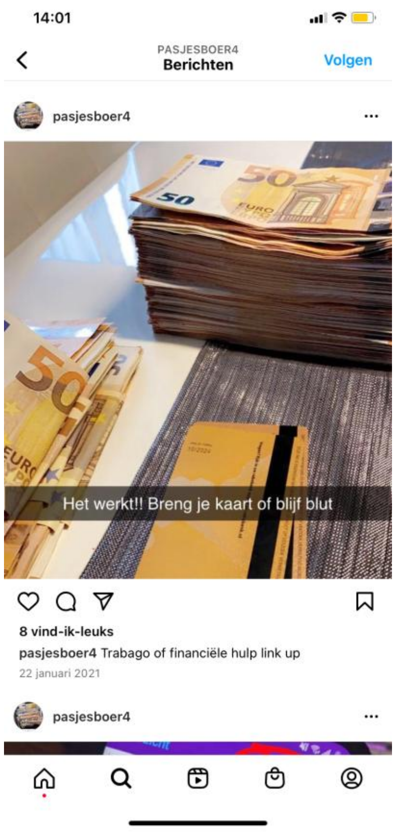
- No uniform network but in my analysis of 15 police cases:
  - 1 to 12 suspects (but sometimes with 400 money mules)
  - Damages varied from 20.000 to 4 million per case
  - Active in a period of weeks, months or years
- Cybercrime on the menu?
- Suspect arrested for a robbery with a machete and a gun in 2019 and for online fraud in 2022

# Local embeddedness

- Financial cybercriminal networks originate and grow in the local neighborhood!
  - Money mules are recruited, in the park, homeless shelter, etc.
  - Core members know each other from their past
- Social relationships provide trust in a criminal “jungle”
- Manage to cross geographical boundaries -> victims and co-offenders in Belgium, Germany, etc.

# The role of social media

- Criminal networks locally anchored, but they also use social media as an extension of the social network
- Telegram, Instagram and Snapchat emerged as online offender convergence setting
  - New members, leads of victims, knowledge of ICT, money mules
- Key pathway into (cyber)crime



14:01

PASJESBOER4
Berichten

Volgen

pasjesboer4

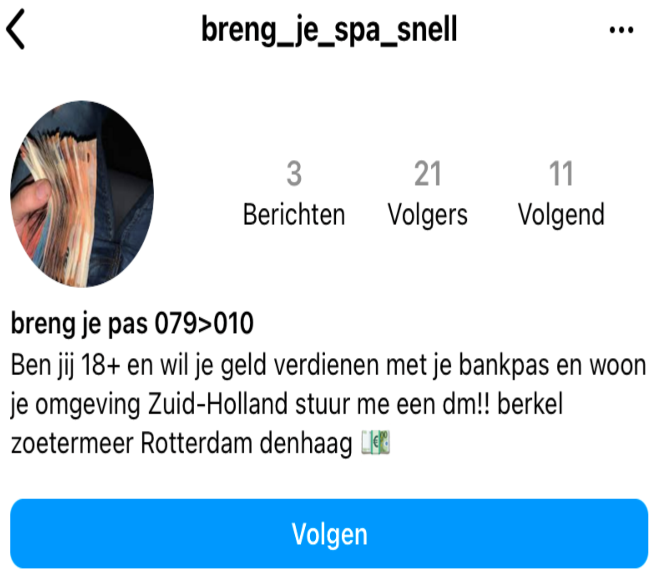
Het werkt!! Breng je kaart of blijf blut

8 vind-ik-leuks

pasjesboer4 Trabago of financiële hulp link up

22 januari 2021

pasjesboer4



breng_je_spa_snell

| 3 | 21 | 11 |
|---|---|---|
| Berichten | Volgers | Volgend |

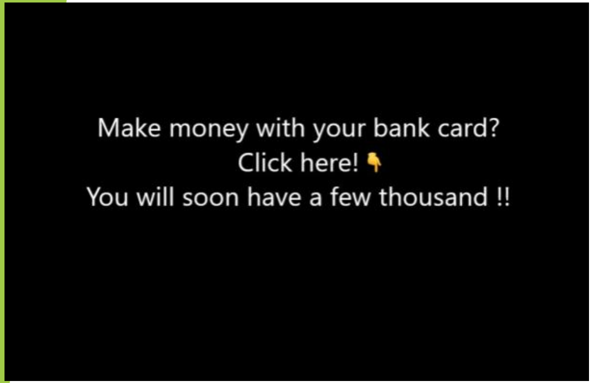
**breng je pas 079>010**

Ben jij 18+ en wil je geld verdienen met je bankpas en woon je omgeving Zuid-Holland stuur me een dm!! berkel zoetermeer Rotterdam denhaag 💶

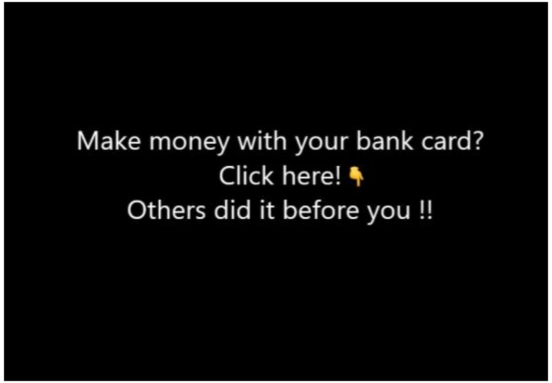
Volgen

# Evidence-based intervention: an example

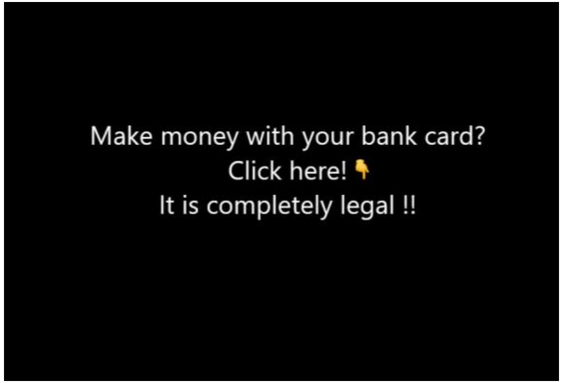
- Intervention on social media targeted on money mules
  - Social media: promising medium to reach the target group
- Developed our own “ads” and landing pages
- Pilot:
  - Measure reach and level of engagement with the ads -> actual behavior!
  - Advertised on behalf of “company” MoneymakerNL
  - Showed ads to young people for a month



Make money with your bank card?
Click here! 👇
You will soon have a few thousand !!



Make money with your bank card?
Click here! 👇
Others did it before you !!

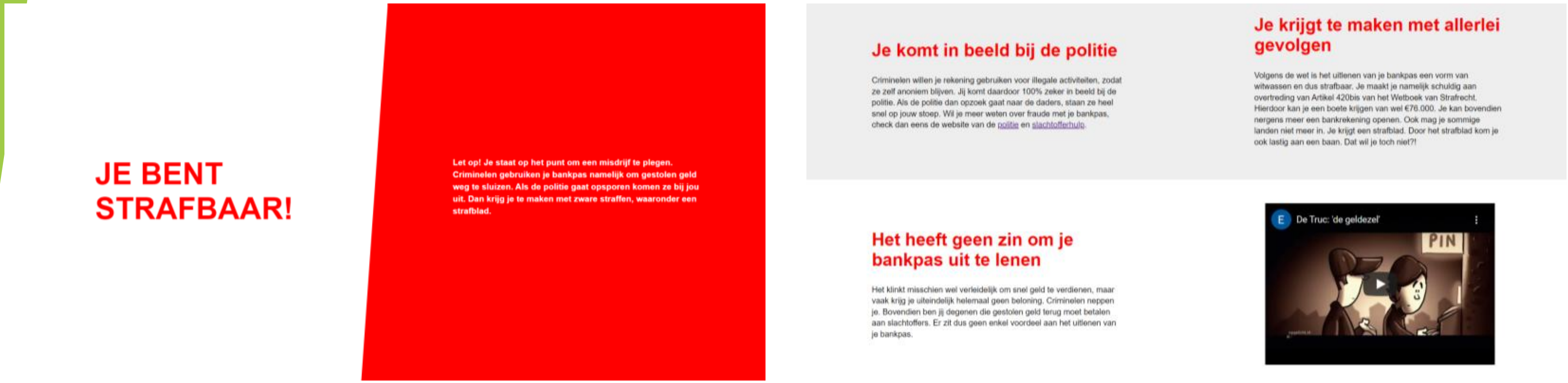


Make money with your bank card?
Click here! 👇
It is completely legal !!

Ad type A
“Luxury lifestyle”

Ad type B
“Normalization”

Ad type C
“Neutralization”



# JE BENT STRAFBAAR!

Let op! Je staat op het punt om een misdrijf te plegen. Criminelen gebruiken je bankpas namelijk om gestolen geld weg te sluizen. Als de politie gaat opsporen komen ze bij jou uit. Dan krijg je te maken met zware straffen, waaronder een strafblad.

## Je komt in beeld bij de politie

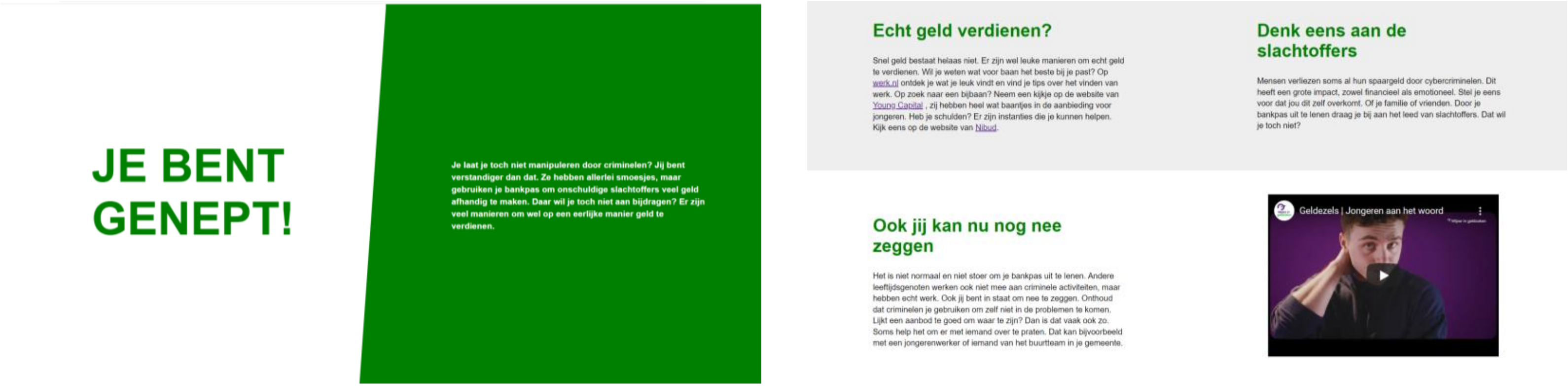
Criminelen willen je rekening gebruiken voor illegale activiteiten, zodat ze zelf anoniem blijven. Jij komt daardoor 100% zeker in beeld bij de politie. Als de politie dan opzoek gaat naar de daders, staan ze heel snel op jouw stoep. Wil je meer weten over fraude met je bankpas, check dan eens de website van de politie en slachtofferhulp.

## Je krijgt te maken met allerlei gevolgen

Volgens de wet is het uitlenen van je bankpas een vorm van witwassen en dus strafbaar. Je maakt je namelijk schuldig aan overtreding van Artikel 420bis van het Wetboek van Strafrecht. Hierdoor kan je een boete krijgen van wel €76.000. Je kan bovendien nergens meer een bankrekening openen. Ook mag je sommige landen niet meer in. Je krijgt een strafblad. Door het strafblad kom je ook lastig aan een baan. Dat wil je toch niet?!

## Het heeft geen zin om je bankpas uit te lenen

Het klinkt misschien wel verleidelijk om snel geld te verdienen, maar vaak krijg je uiteindelijk helemaal geen beloning. Criminelen neppen je. Bovendien ben jij degenen die gestolen geld terug moet betalen aan slachtoffers. Er zit dus geen enkel voordeel aan het uitlenen van je bankpas.



# JE BENT GENEPT!

Je laat je toch niet manipuleren door criminelen? Jij bent verstandiger dan dat. Ze hebben allerlei smoesjes, maar gebruiken je bankpas om onschuldige slachtoffers veel geld afhandig te maken. Daar wil je toch niet aan bijdragen? Er zijn veel manieren om wel op een eerlijke manier geld te verdienen.

## Echt geld verdienen?

Snel geld bestaat helaas niet. Er zijn wel leuke manieren om echt geld te verdienen. Wil je weten wat voor baan het beste bij je past? Op werk.nl ontdek je wat je leuk vindt en vind je tips over het vinden van werk. Op zoek naar een bijbaan? Neem een kijkje op de website van Young Capital , zij hebben heel wat baantjes in de aanbieding voor jongeren. Heb je schulden? Er zijn instanties die je kunnen helpen. Kijk eens op de website van Nibud.

## Denk eens aan de slachtoffers

Mensen verliezen soms al hun spaargeld door cybercriminelen. Dit heeft een grote impact, zowel financieel als emotioneel. Stel je eens voor dat jou dit zelf overkomt. Of je familie of vrienden. Door je bankpas uit te lenen draag je bij aan het leed van slachtoffers. Dat wil je toch niet?

## Ook jij kan nu nog nee zeggen

Het is niet normaal en niet stoer om je bankpas uit te lenen. Andere leeftijdsgenoten werken ook niet mee aan criminele activiteiten, maar hebben echt werk. Ook jij bent in staat om nee te zeggen. Onthoud dat criminelen je gebruiken om zelf niet in de problemen te komen. Lijkt een aanbod te goed om waar te zijn? Dan is dat vaak ook zo. Soms help het om er met iemand over te praten. Dat kan bijvoorbeeld met een jongerenwerker of iemand van het buurtteam in je gemeente.

| | REACH | VIEWS | CLICKS | CLICK RATE |
|---|---|---|---|---|
| **Campaign 1** | | | | |
| **A-Feed** | 9.300 | 9.529 | 21 | 0.0023 (0.23%) |
| **A-Stories** | 8.644 | 8.717 | 33 | 0.0038 (0.38%) |
| **B-Feed** | 9.350 | 9.599 | 18 | 0.0019 (0.19%) |
| **B-Stories** | 9.554 | 9.613 | 13 | 0.0014 (0.14%) |
| **C-Feed** | 8.859 | 9.115 | 21 | 0.0023 (0.23%) |
| **C-Stories** | 9.453 | 9.545 | 30 | 0.0032 (0.32%) |
| | | | | |
| **Campaign 2** | | | | |
| **A-Feed** | 5.616 | 20.915 | 97 | 0.0173 (1.73%) |
| **A-Stories** | 6.203 | 27.938 | 182 | 0.0293 (2.93%) |
| **B-Feed** | 6.033 | 23.725 | 75 | 0.0124 (1.24%) |
| **B-Stories** | 6.724 | 32.338 | 133 | 0.0198 (1.98%) |
| **C-Feed** | 6.779 | 25.796 | 152 | 0.0224 (2.24%) |
| **C-Stories** | 6.448 | 30.855 | 131 | 0.0203 (2.03%) |
| | | | | |
| **TOTAL** | 92.963 | 217.685 | 906 | 0.0097 (0.97%) |

# Thanks!

dr. Luuk Bekkers

l.m.j.bekkers@hhs.nl

+31615440037

# Panel: Prosecuting cybercrime in practice

**Moderator:**
**Prof. Frank Verbruggen**
KU Leuven

**Fabrice Clément**
Proximus

**Kris Derkoningen**
FCCU

**Robrecht De Keersmaecker**
Prosecutor's General Office Antwerp

**Geert Baudewijns**
Secutec

# Statement 1:

After a cyberattack, preserving volatile digital evidence must come first—even at the cost of business continuity—yet slow legal processes and conflicting priorities between victims and justice hinder effective action.

## Statement 2:

When paying ransom becomes the only lifeline for a business, justice offers little solace—yet when judicial systems depend on monopolised private expertise, justice itself becomes a hostage.

## Statement 3:

Justice must abandon chasing low-level scams and instead strike at the heart of criminal networks—because in cybercrime, the best defence is a decisive offence.

# Any questions ?

## Networking lunch

See you back at 2:00 PM !

# 25 YEARS OF CYBER JUSTICE

CYBER SECURITY COALITION

IGO IFJ

hosted in Brussels by

BNP PARIBAS FORTIS