Crime prevention policy	
EU- priority	Cybercrime
Country	Belgium
Year	2018

1. Overview of the field

Definition of cybercrime

Belgian law describes four offenses relating to computer crime:
1) forgery in IT
2) computer fraud
3) data manipulation
4) the "hacking"

Assessment of trends and developments

The Belgian landscape of cybercrime is closely linked to the European cybercrime landscape described in the 'Internet Organized Crime Threat Assessment (iOCTA) 2015' document.

It is about the increasingly aggressive and challenging evolution of cybercrime, the emergence of the important endemic threat of 'Crime-as-a-Service' and malware.

The main developments in cybercrime are:
- state espionage or economic espionage;
- Hacking and malware for the purpose of extortion/data theft.

Recent overview of statistics and research

Type	2013a	2013b	2014a	2014b	2015a	2015b	2016a	2016b
Hacking	1.679	66	1.984	71	2.106	65	2.277	69
Forgery	490	6	641	6	780	14	732	20
Fraud	13.254	1.376	12.717	1.187	13.339	1.328	15.174	1.369
Sabotage	1.143	43	412	19	416	10	441	39

a= Facts
b= Attempts
These are the official figures of the Police. Dark number is surely higher.

2. Crime strategy and coordination

Objectives of the crime strategy

Increase cybersecurity and tackle cybercrime:

- by providing management and actions for the prevention, detection and response to cyber incidents in Belgium;
- by anticipating, at the national and international levels, good harmonization between the partners concerned in terms of cyber-security in order to foster coordinated action;
- by proposing capacity building so that the actors concerned are sufficiently armed in their fight against cybercrime
- by adapting the regulatory framework in its complex and international context of cyber-threats
- by anticipating a quick and effective police response to cyber incidents
- by ensuring effective administration of evidence in cyberspace when computerized means are used to commit criminal acts

Role of prevention in the crime strategy on state/regional/local level

- Raising awareness of the citizen on cyber-threats and cyber-vulnerabilities as well as potentially dangerous behavior on the Internet
- Raising awareness of business sector on issues such as cyber-threats and cyber-vulnerabilities
- Increase protection of vital sectors

Implementation of the policy (which level is responsible for the implementation and how is the implementation coordinated?)

The Centre for Cybersecurity Belgium tasks are:

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

Stakeholders (working groups, specialised agencies, partners, etc)

Federal Police, Universities, Private Sectors

Participation in European/ international networks, working groups, etc.

Not known but surely.

3. Good practices

Overview of recent good practices, prevention programs, etc.

https://cyberguide.ccb.belgium.be/en

https://safeonweb.be/fr

www.amow.be , Facebook -pagina 'NETFLIK AMOW'