Council of the
European Union

Brussels, 18 August 2017
(OR. fr, en)

8212/1/17
REV 1 DCL 1

GENVAL 43
CYBER 58

DECLASSIFICATION

of document:	8212/1/17 REV 1 RESTREINT UE/EU RESTRICTED
dated:	18 May 2017
new status:	Public
Subject:	Evaluation report on the seventh round of mutual evaluations 'The practical implementation and operation of the European policies on preventing and combating cybercrime' - Report on Belgium

Delegations will find attached the declassified version of the above document.

The text of this document is identical to the previous version.

Council of the
European Union

Brussels, 18 May 2017
(OR. fr, en)

8212/1/17
REV 1

RESTREINT UE/EU RESTRICTED

GENVAL 43
CYBER 58

REPORT

Subject:	Evaluation report on the seventh round of mutual evaluations 'The practical implementation and operation of the European policies on preventing and combating cybercrime' - Report on Belgium

ANNEX

Table of contents

1 SUMMARY

In general, the evaluation team believes that the Belgian authorities are aware of the challenges posed by cybercrime and are working to strengthen the country's capacity to prevent and combat the phenomenon in several areas (legal, procedural and institutional).
It should be noted that cybersecurity is one of the 10 main security issues covered by the 2016-2019 national security plan provided to the evaluation team after its visit.

However, the budget set aside for combating cybercrime is insufficient in terms of resources and training, while there is an increased shortage of police staff. In particular, this is true of the FCCU, which is responsible for technical and legal analyses of the files of the Central Office for Combating Economic and Financial Crime (OCDEFO) and the Central Office for the Repression of Corruption (OCRC) and the inspectorates, investigations into attacks on information systems and the training of regional police units. This complex role requires a sufficient budget, because nowadays digital investigation is of fundamental importance for all forms of criminal activities, including terrorism.

The lack of integration of statistics on cybercrime (police departments and judicial system - public prosecutors' offices and courts, and the national CERTs) is a matter requiring further reflection by the Belgian authorities. There is no harmonisation of the criteria for data collection and no link between the data collected.

As far as legislation on cybercrime is concerned, the evaluation team considers that the Belgian Criminal Code covers all relevant offences. At the time of the visit, the only planned change to fully implement Directive 2013/40 was to increase the severity of penalties in the event of non-authorised access (Article 550a) and illicit interception of communications (Article 314a). It should be noted that following the evaluation visit a bill[1] was published on 16 January 2017 providing for heavier penalties to implement Directive 2013/40.

The evaluation team would like to highlight the very thorough and high-quality work done by the FCCU and the federal prosecutor's office to develop a specialisation in the cybercrime approach.

In the law enforcement services, the units responsible for combating cybercrime or carrying out forensic analysis of digital evidence should adopt a strategic and unified approach, involving the federal and local police, in order to coordinate the work of the FCCU, the RCCUs and the LCCUs.

It would also be advisable for members of the judicial authorities, in particular examining magistrates, to develop their specialisation in cybercrime.

There are no rules governing coordination between federal and local police departments, however. This causes problems, due to the large number of police units working on cybercrime or forensic analysis of digital evidence - FCCU, RCCUs and LCCUs - without any strategic vision. It also explains the absence of technical and procedural standards for joint interventions, even when the two units concerned have concluded a 'gentlemen's agreement'.

1 http://www.dekamer.be/FLWB/PDF/54/2259/54K2259001.pdf

In Belgium, there are many public and private initiatives concerning paedophilia prevention campaigns.

An effort should be made to increase public awareness of the importance of reporting cyber-attacks, in order to strengthen Belgium's capacity to combat cybercrime.

The judicial training institute provides high-quality training on cybercrime for new judges. Such training could also be extended to more senior judges.

2 INTRODUCTION

Following the adoption of Joint Action 97/827/JHA of 5 December 1997[2], a mechanism was established for evaluating the national application and implementation of international undertakings in the fight against organised crime. In line with Article 2, the Working Party on General Matters including Evaluation (GENVAL) decided on 3 October 2013 that the seventh round of mutual evaluations should be devoted to the practical implementation and operation of the European polices on preventing and combating cybercrime.

Member States welcomed the choice of cybercrime as the subject for the seventh round of mutual evaluations. However, due to the broad range of offences which are covered by the term cybercrime, it was agreed that the evaluation would focus on those offences that Member States felt warranted particular attention. Accordingly, the evaluation covers three specific areas: cyber attacks, child sexual abuse/pornography online, and online card fraud; it is intended to provide a comprehensive examination of the legal and operational aspects of tackling cybercrime, cross-border cooperation and cooperation with relevant EU agencies. Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography[3] (date of transposition: 18 December 2013) and Directive 2013/40/EU on attacks against information systems[4] (date of transposition: 4 September 2015) are particularly relevant in this context.

2 Joint Action 97/827/JHA of 5 December 1997, OJ L 344, 15.12.1997, p. 7.
3 OJ L 335, 17.12.2011, p. 1.
4 OJ L 218, 14.8.2013, p. 8.

Moreover, the June 2013 Council conclusions on the EU Cybersecurity Strategy[5] reiterate the objective of ratification of the Council of Europe Convention on Cybercrime (the Budapest Convention)[6] of 23 November 2001 as soon as possible and emphasise in their preamble that 'the EU does not call for the creation of new international legal instruments for cyber issues'. The Budapest Convention is supplemented by a Protocol on the criminalisation of acts of a racist or xenophobic nature committed through computer systems[7].

Experiences from earlier evaluations show that the implementation of the relevant legal instruments is at different stages in the Member States. The current process of evaluation could also provide useful input to Member States that have not implemented all aspects of the various instruments. Nonetheless, the evaluation aims to be broad and interdisciplinary and not focus solely on implementation of various instruments for fighting cybercrime, but also on operational aspects in the Member States.

Therefore, apart from cooperation with prosecution services, it will also encompass how police authorities cooperate with Eurojust, ENISA and Europol/EC3 and how feedback from these bodies is channelled to the appropriate police and social services. The evaluation focuses on implementing national policies to stop cyber-attacks, online fraud and child pornography. It also covers operational practices in the Member States with regard to international cooperation and the support offered to persons who fall victim to cybercrime.

5 12109/13 POLGEN 138 JAI 612 TELECOM 194 PROCIV 88 CSC 69 CIS 14 RELEX 633 JAIEX 55 RECH 338 COMPET 554 IND 204 COTER 85 ENFOPOL 232 DROIPEN 87 CYBER 15 COPS 276 POLMIL 39 COSI 93 DATAPROTECT 94.

6 ETS No. 185, which was opened for signature on 23 November 2001 and entered into force on 1 July 2004.

7 ETS No. 189, which was opened for signature on 28 January 2003 and entered into force on 1 March 2006.

The sequence of visits to the Member States was adopted by the GENVAL Working Party on 1 April 2014. Belgium was the Member State to be evaluated during this round of evaluations. In accordance with Article 3 of the Joint Action, the Presidency drew up a list of experts for the evaluations to be carried out. Member States nominated experts with extensive practical knowledge in the field in response to a written request to delegations made by the Chair of GENVAL on 28 January 2014.

The evaluation teams consisted of three national experts, supported by two staff from the General Secretariat of the Council and observers. For the seventh round of mutual evaluations, GENVAL agreed with the Presidency's proposal that the European Commission, Eurojust, Europol/EC3 and ENISA should be invited as observers.

The experts charged with undertaking the evaluation of Belgium were Mr Alain Kleuls from the Grand Duchy of Luxembourg police, Mr Rui Batista (Portugal) and Mr Philippe Devred (France), together with Ms Claire Rocheteau from the General Secretariat of the Council.

This report was prepared by the expert team with the assistance of the General Secretariat of the Council, based on findings arising from the evaluation visit that took place in Belgium between 26 and 28 April 2016, and on Belgium's detailed replies to the evaluation questionnaire together with its detailed answers to subsequent follow-up questions.

3 GENERAL MATTERS AND STRUCTURES

3.1 National Cybersecurity Strategy

On 21 December 2012, the Cabinet adopted a national cybersecurity strategy for Belgium and entrusted the Prime Minister with coordinating its implementation. The aim is to provide Belgium with a federal strategy for network and information system security, with due regard for privacy. The Belgian cybersecurity strategy is intended to identify cyber threats, improve security and be able to respond to incidents. The strategy was developed on the basis of work done by the BelNIS consultation platform for information security created by the Cabinet on 30 September 2005. The following institutions meet periodically in the framework of BelNIS: the Belgian Commission for the Protection of Privacy, the National Security Authority, the General Intelligence and Security Service (SGRS), State Security, the Belgian Institute for Postal Services and Telecommunications (BIPT), the Federal Computer Crime Unit (FCCU), the Federal Public Service for the Economy, the Federal Public Service for Information and Communication Technology (Fedict), the Belgian business register, the Crisis Centre and the representative of the College of Principal Public Prosecutors.

After having assessed the situation as regards the cyber threat in Belgium, the strategy sets out three strategic objectives:

- to create a safe and reliable cyberspace which respects the values and fundamental rights of modern society;
- to ensure critical public infrastructure and systems are optimally secured and protected against the cyber threat;
- to develop independent cybersecurity capacities.

To achieve these three strategic objectives, the Belgian state has developed a number of specific lines of action:

- adopting a centralised and integrated cybersecurity approach;
- creating a legal framework;
- continuously monitoring the cyber threat;
- improving protection against the disruption or violation of computer systems;
- strengthening capacity to react to cyber incidents;
- adopting a specific cybercrime approach;
- contributing to the development of cybersecurity expertise and knowledge;
- stimulating technological development.

The text of the strategy is available online (in FR/NL): http://www.b-ccentre.be.
It should also be noted that a new framework note on integral security and a new national security plan are currently being drawn up, which will pay particular attention to cybercrime.

One example of good practice in the fight against cybercrime is the consultation platform: in the jurisdiction of Ghent, two cooperation agreements have been concluded on computer crime, one by the province of East Flanders, the prosecutors' offices of Ghent, Dendermonde and Oudenaarde, where matters are managed by the Dendermonde public prosecutor's office, and the other for the province of West Flanders, where the Veurne public prosecutor's office is responsible. Good practices are also circulated to the Antwerp and Liege public prosecutor's offices.

After the evaluation visit, a working group was set up in the CCB tasked with updating Belgium's cyber strategy, with a view to the transposition of the NIS Directive.
It should also be mentioned that the 2016-2019 framework note on integrated security[8] and the 2016-2019 national security plan[9] are also available; cybercrime and cybersecurity are priorities in both texts.

[8] http://jambon.belgium.be/sites/default/files/articles/Kadernota%20IV%20FR_DEF.pdf
[9] http://jambon.belgium.be/sites/default/files/articles/PNS_F.pdf

3.2 National priorities with regard to cybercrime

A number of priority measures have been agreed in the fight against cybercrime:

- The creation of the Centre for Cybersecurity Belgium (CCB), under the authority of the Prime Minister. One of its priorities is to manage incidents and cyber-attacks efficiently.
- Increasing the capacity of the federal judicial police's regional Computer Crime Units (CCUs), with more specialists dedicated to the fight against cybercrime. Until now the CCUs were mainly specialised in the technical and legal analysis of digital evidence and in increasing the capacity of the Federal Computer Crime Unit, the central unit in the federal judicial police, by providing additional specialists dedicated to combating cyber-attacks, with priority given to critical infrastructure.
- Strengthening the capacity of the General Intelligence and Security Service (SGRS) of the armed forces to protect national sites.
- The creation of appropriate legal tools. This collection of diverse legal provisions, some of which are still being drafted, covers:
    - internet patrols, 'undercover light' investigations;
    - intervention and seizure procedures;
    - certification of specialised investigators;
    - technical and legal investigation methods;
    - extending computer system searches and the issue of data encryption;
    - legal hacking by police forces;
    - problems with communications software suppliers (Skype, WhatsApp, etc.).

The following initiatives should also be mentioned:

- the implementation of legislation regarding interception on the internet;
- the continued implementation of Directive 2013/40/EU on attacks against information systems;
- the optimisation of operator identification of end-users of electronic communications;
- the action taken to make internet sites containing child pornography material inaccessible and to shut them down more quickly: 'notice and takedown';
- the creation of compensatory legislation on data retention, which continues to be an absolutely necessary and crucial instrument for the judicial authorities.

The evaluation team welcomes Belgium's legislative initiatives to improve specific search methods and a number of investigation measures for use with the internet, electronic communications and telecommunications, in particular the confidential memo listing all internet search activities, indexed and classified according to the level of intrusion into citizens' privacy, with an indication of whether they are permissible in the proactive and/or reactive phase.

3.3 Statistics on cybercrime

Given that the institutions each use different definitions and a different methodology, it is impossible to compare and link the statistics they produce. The recording and classification of incidents also depend on the police officer's level of knowledge of the subject matter. Moreover, when an incident is recorded, there is no way to distinguish between the different types of cybercrime.

3.3.1 Main trends leading to cybercrime

Major trends with regard to cybercrime

We see that some *operating methods* have recently been used with increasing success, namely:

- APTs (Advanced Persistent Threats): the first APT case to be examined by the Belgian police concerned the hacking of a major telecoms operator in 2012. The number of APT cases has continued to rise since then. The use by organised crime (acquisition/purchase via the Internet) of (parts of) state-sponsored malware has also been observed.
- digital extortion:
  - crypto ransomware (such as CryptoLocker and CTB Locker) encrypt files on PCs (since 2013 with growing success) and demand payment to recover the files;
  - extortion by threatening to publish hacked data (since 2012).
- malware on mobile devices: it has emerged that this malware, which has appeared in recent investigations in Belgium and elsewhere, targets critical infrastructure with increasing frequency (date collection or takeover).

We have also seen that the list of (known) cases of hacking targeting Belgian authorities and important political figures has grown continuously longer since the first in 2012: the President of the European Council, the Prime Minister, a major telecommunications operator, a professor (cryptography expert), the Federal Public Services Foreign Affairs and Economy, embassies in Brussels, the European Union, universities, etc.

Lastly, mention should be made of the appearance of a worrying trend, namely increasing cooperation between cybercriminals and traditional organised crime: in 2012, for the first time in Belgium, a case was brought to light that involved the use of professional hacking on the drugs scene.

Cybercrime in relation to the total criminality picture

Over the last three years computer crime has accounted for between 1.7 and 2% of crime as a whole in Belgium (source: Police crime statistics 2000-2014, federal police).

Following the initial attacks on on-line banking systems in 2007, action was initiated by the federal prosecutor's office, with support from the FCCU's investigative services and the Central Office for Combating Economic and Financial Crime (OCDEFO), in cooperation with the sector in question (FEBELFIN and the five large banks). We note that while these attacks were halted for several years, they have in recent months led to a further increase in the damage caused.

Furthermore, it should be pointed out that the fact of such acts not being reported to the judicial authorities, because of a lack of capacity in local police forces to record incidents affecting members of the public (awareness of the problems, international dimension, links with ordinary crime, classification of the acts) and because of a fear, on the part of companies, of a loss of confidence, largely explains why this type of crime is a 'hidden statistic'. The efforts made, especially as regards the corporate sector, to encourage it to react and report events is slowly bringing a cultural change that has yet to produce results.

3.3.2 Number of registered cases of cybercrime

Statistics on cybercrime are not integrated. Each institution/body compiles them independently. At present it is generally not possible to read the statistics from the federal prosecutor's office together with the police statistics and those for convictions, deferred sentences and confinements. There are in fact fundamental differences in terms of methodological options and substance.

Police statistics

The basic data on recorded crime statistics are provided by the preliminary official reports drawn up by the services of the integrated police which is organised at two levels (local police and federal police), regardless of whether the offence in question has been attempted or completed. Police statistics are available on http://www.stat.policefederale.be/statistiquescriminalite/.

Public prosecution service statistics

The statistical analysts at the public prosecution service can generate statistical data from the service's central database. This database contains the information recorded in the computerised REA/TPI system by the criminal matters section of the prosecutor's and registrar's offices at the courts of first instance.

Statistics on convictions, deferred sentences and confinements

These statistics can be subdivided according to the type of criminal offence. It is important to know that a judgment handed down by a court and entered for an individual in a convictions bulletin can concern several criminal offences. Moreover, an individual can be convicted several times a year and therefore have several conviction bulletins a year. Hence the total number of convictions, deferred sentences or confinements per criminal offence is much higher than the total number of conviction bulletins per court or per jurisdiction and the total number of convictions.

While reliable and representative figures are available for 1995-1996, the statistical data on convictions for 2006-2012 underestimate the reality on account of the backlog in recording conviction bulletins at the Central Criminal Register.

Statistics produced by CERT

Rather than compiling statistics on cybercrime, CERT is concerned with the notification of incidents, many of which in recent years have turned out to be increasingly often linked to cybercrime.

These incidents are screened then examined internally and classified. This classification will soon be reviewed to improve data transmission and respond to attacks more effectively. It will also take into account the impact of the incident as well as its origin (root cause).

These figures are published on https://www.cert.be/fr/chiffres, although some are not communicated to third parties..

There is however cooperation between the Federal Computer Crime Unit, and other services may also be notified if the number of such incidents rises unexpectedly.

With the focus on cybercrime detection, data also needs to be forwarded at high level to the judicial authority, but this procedure has not yet been formalised.

Police crime statistics

Year	Number of computer-related criminal offences: Article 210*a* (computer forgery), Article 504*c* (computer fraud), *Article 550a (hacking) and Article 550b (computer sabotage).*
2005	4 322
2006	5 736
2007	7 741
2008	9 112
2009	11 668
2010	14 476
2011	15 763
2012	22 023
2013	18 002
2014	16 561

Source: Police crime statistics 2000-2014, federal police

The 2015 statistics and an update of the other figures are available at: http://www.stat.policefederale.be/assets/pdf/crimestat/nationaal/rapport_2016_trim1_nat_belgique_fr.pdf.

Public prosecution service statistics

Number of computer-related criminal offences:						
	2013		2014		Total	
	N	%	N	%	N	%
Computer forgery	1 024	4.79	1 538	7.16	2 562	5.97
Computer fraud	16 890	78.94	15 962	74.28	32 852	76.60
Hacking	662	3.09	721	3.36	1 383	3.22
Computer sabotage	778	3.64	222	1.03	1 000	2.33
Refusal to cooperate (in connection with a computer system search, e.g. information as to how the system works) when requested by an examining magistrate or obstructing a search of the computer system ordered by an examining magistrate	3	0.01	3	0.01	6	0.01
Computer forgery, including counterfeit bank cards.	393	1.84	443	2.06	836	1.95
Other	1 646	7.69	2 600	12.10	4 246	9.90
Total	21 396	100.00	21 489	100.00	42 885	100.00

Statistics on convictions, deferred sentences and confinements

As mentioned in the reply to question 6, the statistical data for 2006-2012 concerning convictions underestimate the reality and are therefore not often used. They are given below:

Year	Number of computer-related criminal offences: Article 210*a* (computer forgery), Article 504*c* (computer fraud), Article 550a (hacking) Article.550*b* (computer sabotage) of the Criminal Code
2005	369
2006	441
2007	528
2008	464
2009	519
2010	561
2011	628
2012	743
2013	624

Source: Criminal Policy Service *FPS Justice*

CERT.be statistics

The number of incidents reported to CERT.be between 2010 and 2014 is given below:

	2010	**2011**	**2012**	**2013**	**2014**
Total reports received	2 135	2 609	3 866	6 678	10 812
Total of them that were incidents	**1 389**	**1 494**	**1 981**	**4 070**	**9 866**
Incidents related to worms and viruses	13.0 %	4.6 %	6.0 %	22.0 %	29.5 %
Scan incidents	5.0 %	26.1 %	29.0 %	20.0 %	30.5 %
System incidents	24.0 %	24.1 %	21.0 %	14.5 %	3.5 %
Phishing incidents	8.0 %	14.7 %	17.0 %	14.0 %	5.5 %
Incidents related to spam	7.0 %	14.8 %	4.5 %	13.0 %	5.0 %
Other incidents	10.0 %	3.1 %	11.0 %	10.5 %	3.5 %
Incidents reporting vulnerabilities	0 %	0.7 %	2.0 %	3.0 %	21.0 %
Incidents with denial-of service attacks	0 %	2.4 %	1.5 %	1.5 %	0.5 %
Incidents/questions about internet security related topics	1.0 %	4.3 %	4.0 %	1.0 %	0.5 %
Incidents with accounts	32.0 %	5.2 %	4.0 %	0.5 %	0.5 %

Secondly, 'computerised' sources (sensors) automatically report incidents; in the first half of 2014 this system made it possible to pick up over 750 000. Analysis of these sources based on a new methodology is currently under way. In 2013 the analysis found that a large number of incidents were linked to computers forming part of a botnet.

The police and public prosecution service statistics and the figures for convictions do not give a precise idea of the number and type of cyber offences recorded and/or punished, or the number of people investigated, prosecuted or convicted for cybercrimes.

The CERT statistics already go into greater detail by classifying the offences. To improve the statistics, this classification is reviewed to in order take into account both the impact and the origin of the incident.

Like many other countries, Belgium has difficulty quantifying with sufficient precision an expanding criminal phenomenon which encompasses both offences which are legally defined as having a cybercriminal aspect and ordinary offences committed using information technology.

The evaluation team welcomes the effort made by Belgium to change the computer system so as to link up the different databases of the various bodies that record the statistics. The aim is to provide figures from the time the incident took place to the point at which the guilty party is convicted.

The 'hidden statistic' of cybercrime, i.e. the failure to report the acts to the law enforcement agencies, is high. In the opinion of the Belgian authorities, the reason for this is that the local police forces lacked the capacity to record incidents affecting members of the public (awareness of the problems, international dimension, links with ordinary crime, classification of the acts) and because companies feared a loss of confidence.

3.4 Domestic budget allocated to prevent and combat cybercrime and EU financial support

There is no comprehensive approach to budgeting for the fight against cybercrime. Belgium provided the following information:

- The federal police have a separate investment budget that is used for purchasing ICT equipment specifically for scientific/forensic purposes for the Computer Crime Units (FCCU and RCCU). In 2015 this budget amounted to EUR 511 333.
- In 2015 the Centre for Cyber Security Belgium (CCB), which was established on 17 August of that year, was granted a budget of approximately EUR 719 000 for operational and organisational purposes. The budget is not specifically allocated to the fight against cybercrime. The Centre uses interdepartmental provisions to fund cybersecurity projects.
- BRAIN-be (Belgian Research Action through Interdisciplinary Networks, which incorporates federal research funding instruments) has released funds totalling EUR 684 731 for the project 'Measuring Cost and Impact of Cybercrime in Belgium'. This multidisciplinary research is however still in progress (it lasts from 1 December 2013 to 28 February 2018). Conducted over a four-year period, this research will give a broader and scientifically -based overview of the impact of the cyber threat, thanks to a model that is specific to the country that makes it possible to measure the cost and impact of cybercrime. The research will also provide strategic directives and guidelines so that policy makers can decide how the principles set out in the Belgian cybersecurity strategy should be taken forward.

3.5 Conclusions

Belgium has a national cybersecurity strategy which was adopted on 21 December 2012. This strategy (http://www.b-ccentre.be) is defined by three objectives:

- a safe and reliable cyberspace which respects the values and fundamental rights of modern society;
- ensuring critical public infrastructure and systems are optimally secured and protected against the cyber threat;
- the development of Belgian cybersecurity capabilities and several concrete action lines:
- a centralised and integrated cybersecurity approach;
- the creation of a legal framework;
- permanent monitoring of the cyber threat;
- improving protection against the disruption or violation of computer systems;
- strengthening capacity to react to cyber incidents;
- a specific approach to cybercrime;
- contributing to the development of cybersecurity expertise and knowledge;
- stimulating technological development.

The 2016-2019 national security plan presented after the visit includes cybersecurity as one of the 10 main security issues.

The evaluation team regards it as important that the Centre for Cyber Security Belgium (CCB),which was set up in October 2014, is tasked with implementation and coordination. The CCB is under the authority of the Prime Minister. At the time of the evaluation the CCB was being set up. Hence it is important to ensure that specialists are recruited and retained in the long term.

The evaluation team noted that there was a project concerned with centralisation and research in the area of cybercrime and cybersecurity - the B-CCENTRE (Belgian Cybercrime Centre of Excellence) - that had been launched in 2011 by the Catholic University of Leuven. This project is no longer supported. Its role was to bring together all the main players, support information exchange in the area of cybercrime, provide training and carry out certain activities forming part of the national cybersecurity strategy. While the intention is for the CCB to take over from the B-CCENTRE, the already existing expertise should be supported and incorporated. After the evaluation visit the CCB, along with the Home Affairs FPS, began taking the necessary steps to apply to the EU for the subsidies necessary to take over the B-CCENTRE. A call for applications will be launched at universities to manage the subsidies.

The evaluation team identified a lack of communication between the actors involved (the CCB and the B-CCENTRE). The efforts already made should therefore be integrated.

Standards and norms should be defined so that the different authorities' statistics can be compared. This recommendation applies to all Member States, not only to Belgium. The systems currently used to record offences are unable to provide a quantitative overview of reported cybercrime, either as a whole or broken down by type of offence. It can only identify overall trends. The hidden statistic of cybercrime in Belgium stems from a failure to systematically report offences to the competent authorities.

The evaluation team believes that Belgium should review the funding rules - the means and the human resources - that cover the fight against cybercrime, especially as regards the acquisition of technical devices or software and the fees paid to experts.

This is even more of a problem in the federal police because the officers responsible for combating cybercrime at central level are less well paid than at regional level.

4 NATIONAL STRUCTURES

4.1 Judiciary (prosecution and courts)

4.1.1 Internal structure

The institutions responsible for crime-fighting and prevention are, in brief:

- the federal police;
- the Public Prosecution Service;
- the Belgian Centre for Cybersecurity (CCB);
- the federal Cyber Emergency Team (CERT.be), funded by the ....Chancellery of the Prime Minister and the CCB, consists of a coordinator, a press/communications officer, a dedicated system manager and five information security analysts. There are still vacancies for a deputy coordinator and three analysts;
- BELNET provides support on legal matters, human resources and administrative management and technical support for infrastructure;
- the Federal Public Service for Information and Communication Technology (Fedict);
- the Belgian Institute for Post Services and Telecommunications (IBPT);
- the armed forces intelligence service (SGRS, General Intelligence and Security Service);
- the Commission for the Protection of Privacy.

The public prosecution service has a central position in the Belgian judicial system. It is made up of public prosecutors acting for the state and defends the interests of society. They prosecute offenders in court, lead criminal inquiries, pursue perpetrators and call for the court to sentence suspects.

The public prosecution service is made up of a number of different types of entity. At the courts of first instance (at provincial level), the public prosecutor's offices do this work. There are 12 judicial districts with 14 prosecutor's offices. There is no specialisation in cybercrime at that level; all the prosecutors can deal with it. It is the public prosecution service's wish that all judges should have a basic knowledge of cybercrime matters. It should be noted that each public prosecutor's office has a designated judge for cybercrime matters.

At the appeal court level, this Service is represented by the principal public prosecutor's offices. There are five principal public prosecutors, who constitute between them the College of Principal Public Prosecutors.

At federal level, the Public Prosecution Service is represented by one federal prosecutor, who deals with complex matters that transcend the boundaries of the judicial districts, such as human trafficking, terrorism, organised crime and money laundering. He is also responsible for facilitating international cooperation and supervising the running of the federal police.

Cybercrime is in the remit of the Antwerp principal public prosecutor, coordinating with the federal prosecutor.

Cybercrime is part of the remit of the federal police (FCCU, federal computer crime unit). All files on attacks on critical and sensitive sites are centralised at the FCCU while other major attacks of regional impact are handled by the RCCUs.

Meeting those involved has revealed that there is no clear-cut approach to the assignment of responsibility for dossiers . Decisions seems to be taken on a case-by-case basis. There is no hierarchy between the FCCU and the RCCUs.

4.1.2 Available capacity and obstacles to successful prosecution

Basic training on cybercrime, which is compulsory for second-year judicial trainees, aims to raise the awareness of judges regarding computer crime.

Specialist cybercrime training, which is aimed specifically at judges, judicial trainees and prosecution service lawyers, can provide in-depth expertise on the use of social media in proactive and reactive criminal investigations, on special investigation methods in a virtual environment, international cooperation in criminal matters (particularly with the USA), especially as regards digital traces and evidence, and on territorial powers and jurisdictions in cyberspace.

An experts' network has also been set up in the College of Principal Public Prosecutors.

In 2008, the College of Principal Public Prosecutors, setting out policy on cybercrime, decided there should be at least one designated judge for the field at the levels of public prosecutor's office, principal public prosecutor's office and Federal Prosecutor's office. These judges are expected to study the subject and undertake specialist training.

The College of Principal Public Prosecutors has created a cybercrime experts' network with representatives of the federal, principal and first-instance public prosecutor's offices, the federal police (FCCU), the CCD and, by invitation, examining judges, to increase the relevant expertise of the Public Prosecution Service, facilitate communications and documentation and facilitate contact with institutions outside the Public Prosecution Service. That network of expertise has no operational tasks (investigations).

Only the judges of the prosecutor's offices are assigned to investigate and prosecute offences. They may assign an examining magistrate to lead the investigation.

In general it is the police (local or federal) that carry out criminal investigation police work and report to the prosecutor's offices.

The main obstacles to the successful prosecution of cybercrime offences noted by the Belgian authorities are the following:

- inability to intercept VoIP communications;
- encryption issues (quantity of encrypted material);
- Lack of clear rules and (European) guidance on the jurisdiction of operators actively providing services in Europe;
- data retention issues;
- use of tools preventing identification (TOR);
- use of hidden internet (dark net);
- slowness of mutual judicial assistance, regardless of what the authorities concerned want;
- scarcity or absence of incident reports and complaints from victims;
- enforcement methods unsuitable for dealing with mass phenomena;
- long, complex investigations, often requiring international cooperation;
- heterogeneity of national laws;
- overburdening of specialist services;
- amount of data to be analysed;
- shortage of qualified staff.

The judicial authorities (prosecutor's offices and courts) that have to investigate cybercrime cases are not always aware of their importance. This is due to lack of knowledge of the mechanisms involved, which are indeed complicated, and to a lack of training and specialisation in the cybercrime field.

4.2 Law enforcement authorities

The departments specialising in the prevention of cybercrime are as follows:

- The Federal Computer Crime Unit (FCCU), the central unit attached to the directorate for the fight against serious and organised crime (DJSOC), is responsible for investigations connected to cyber-attacks on critical infrastructure, cyber-attacks and other investigations into cybercrime in support of the RCCUs (Regional Computer Crime Units). With a staff of 44 investigators, the FCCU has inter alia an eight-member team for taking judicial action in response to cyber-incidents and a six-member team dedicated to intelligence gathering and processing;
- The Regional Computer Crime Units investigate cyber attacks and provide technical and legal support in non-specific crime investigations. RCCU staffing numbers are set by regional directors of the federal judicial police and vary from three to more than 30, all of whom have taken the basic 'CCU investigator' training.
- The Federal Public Service for the Economy has a section of investigators assigned to prosecutions related to i economic offences committed via the internet;
- In the Federal Public Service for Finance, the Belgian Internet Service Center (BISC) has an investigation section responsible for prosecutions concerning financial fraud and the detection of internet fraud mechanisms. This department also carries out technical and legal research.

The first responders on crime scenes are the officers of the local police with responsibility for sealing off the crime scene and preserving the IT media involved. According to the head of the FCCU, a network of first responders has yet to be established.

As to numbers, the FCCU has a staff of 28 rather than the theoretical strength of 44 colleagues. The RCCUs employ 180 people rather than the 260 they are supposed to have.

One criticism made by chiefs is that the FCCU and RCCU police currently have only seven or eight personnel with the operational capability to perform a specialist analysis. The units are also overloaded with work, with a substantial backlog.

Another point raised during the visit was that specialists are rarely involved in the cases and often do not have the knowledge that the investigator needs.

The lack of a clear demarcation of tasks among the various agencies (FCCU and RCCUs) involved was also mentioned.

Different RCCUs brought up the same problems, namely: understaffing, insufficient training, unacceptable delays in dealing with files, and inappropriate recruitment procedures. The budget is not even sufficient to renew the exist licences for the software used to operate the IT tools under forensic examination.

The budget for outside training on cybercrime is just EUR 3 000 for the entire Criminal Investigation Department.

4.3 Other services and public-private partnership

In addition to the federal prosecutor's office and the federal CID , the following entities may be called on to take part in detection, prevention and response in cybercrime cases, under their legally established remits:

- The cyber experts of the General Intelligence and Security Service (SGRS) of the armed forces, attached to the Federal Public Service for Defence.

These experts also take part in national and international exercises.

- CERT.be

CERT.be is the federal cyber emergency team, managed by Belnet, the Belgian national scientific network, at the request of the Federal Public Service of the Chancellery of the Prime Minister. CERT.be is part of a worldwide network of experts in cyber security and deals with internet security problems by coordination, information and awareness raising

ICT professionals can approach CERT.be free of charge and confidentially to report IT problems (data and network infrastructure piracy, phishing, cyber-attacks etc.). CERT.be gives advice on how to deal with such incidents as quickly as possible and coordinates the actions of all the businesses and/or other organisations concerned.

CERT.be also gives advice to individuals and businesses to make their internet use secure. Businesses can find this information on www.cert.be, while the general public can consult the new site www.safeonweb.be.

CERT.be takes part in national and international exercises.

- Federal Intelligence and Security Agency

The Federal Intelligence and Security Agency is the Belgian intelligence service; It operates under the supervision of the intelligence committee (Comité R), which reports to the Prime Minister.

- The sectoral authorities responsible for critical infrastructure

The critical infrastructure operators are required to develop and implement internal security plans containing uninterrupted security measures (at all times) and gradual security measures (dependent on threat level). Those measures cover both the physical security of the infrastructure and the security of the networks and computer systems.

The sectoral authorities can specify the particular measures for critical infrastructures for which they are responsible and are required to arrange regular monitoring of the plans.

In Belgium, the five critical sectors are at present the following:

- the energy sector (sectoral authority: the Minister for Energy);
- the transport sector (sectoral authority: the Minister for Mobility);
- the finance sector (sectoral authority: the National Bank of Belgium):

- the electronic communications sector (sectoral authority: the IBPT, delegated by the minister whose responsibilities include electronic communications);
- the space sector (limited to the ground stations within the Galileo and EGNOS programmes) (sectoral administrative authority: the Belgian High Representation for Space Policy; authority responsible for supervision: the National Security Authority).

The Crisis Centre is responsible for coordination policy for critical infrastructure.

- The Belgian Institute for Post Services and Telecommunications (IBPT)[10];

The IBPT is the regulator for telecommunications and thus for internet access providers, but also for radio devices (wi-fi etc.).

- Fedict (Federal Public Service for Information and Communication Technology)
- The Federal Public Service for the Economy (FPS Economy)
- The BISC investigation unit of the Federal Public Service for Finance (FPS Finance)
- Since the end of 2015, the CCB, described in more detail above.

[10] http://www.ibpt.be/fr.

The following entities may be called on to intervene in cases of cybercrime detection, prevention and response:

- The cyber experts of the General Intelligence and Security Service (SGRS) of the armed forces, attached to the Federal Public Service for Defence. These experts also take part in national and international exercises.
- CERT.be: CERT.be is the federal cyber emergency team, managed by Belnet, the Belgian national scientific network, at the request of the Federal Public Service of the Chancellery of the Prime Minister. CERT.be takes part in national and international exercises.
- The Federal Intelligence and Security Agency is the Belgian intelligence service;
- The sectoral authorities with responsibilities for critical infrastructure: critical infrastructure operators are required to develop and implement internal security plans containing uninterrupted security measures (at all times) and gradual security measures (dependent on threat level). Those measures cover both the physical security of the infrastructure and the security of the networks and computer systems.
- The Belgian Institute for Post Services and Telecommunications (IBPT): the IBPT is the regulator for telecommunications and thus for internet access providers, but also for radio devices (wi-fi etc.);
- Fedict, the Federal Public Service for Information and Communication Technology;
- The Federal Public Service for the Economy (FPS Economy);
- The BISC investigation unit of the Federal Public Service for Finance (FPS Finance);
- The CCB, since 2015.

In the context of cooperation with different private enterprises with their head offices in third countries, this takes place on a negotiated and voluntary basis, but with mixed results. There are 'individual' agreements with some big private companies, but it is still a balancing act. These private companies also have to comply with national legislation, which in some cases bars transmission of data to third countries. When appropriate, we use international letters rogatory, which are a cumbersome and slow procedure.

The private companies may be subjected to binding measures such as search warrants. In addition, telecommunications service providers may be asked to help or face penalties for non-cooperation (cf. the Yahoo case).

As to the resources allocated to enhancing cooperation with the private sector, it should be pointed out that at federal CID level, the 'integral and integrated' approach of the new strategy supports enhanced cooperation with the private sector. The resources earmarked for this cooperation are measured purely in terms of human resources; no financial resources are available.

Collaboration with academia, initiated in 2011 with the creation of a centre of excellence, the B-CCENTRE, has meant that anti-cybercrime needs, as expressed by the judicial authorities (through the participation of the Judicial Training Institute) and the police (through the participation of the FCCU), have been taken on board in projects on training, R&D and prevention (especially for enterprises)[11].

[11] http://www.b-ccentre.be/

There has been over ten years of active cooperation with the Federation of Belgian Enterprises (FEB) in drawing up standards and guides to good practice and to carry out awareness and prevention campaigns (targeted especially at business).

Those two partners (B-CCENTRE and FEB) also have the benefit of the experience acquired by the federal police in drafting the Belgian cybersecurity guide. The guide can be downloaded in English, French and Dutch.

Lastly, it is worth mentioning investment in participation in international initiatives on training (ECTEG) and R&D, such as the FREETOOLS project, under which Europol/EC3 made forensic tools available to specialised investigators free of charge.

Cooperation can be launched on an ad hoc basis, as circumstances require For example, following attacks on on-line banking systems, cooperation with the industry, via FeBelFin, and the five major banking entities in Belgium, in collaboration with the National Bank of Belgium (previously with the CBFA) has reduced the losses sustained by banks and individuals and resulted in new security standards, imposed by the regulatory body (the National Bank).

4.4 Cooperation and coordination at national level

The Centre for Cybersecurity Belgium (CCB) was set up in 2015 and should become operational during 2016.

Its responsibilities include:

- supervising, coordinating and ensuring implementation of Belgium's cybersecurity strategy;
- managing the various cybersecurity-related projects, in an integrated and centralised way;
- ensuring coordination among the services and authorities concerned and between public authorities and the private sector and the scientific community;
- making proposals on adapting the legal and regulatory framework governing cybersecurity matters;
- cyber incident crisis management (together with the Government Coordination and Crisis Centre);
- developing and distributing security standards, guidelines and norms for the various types of IT systems used by public authorities and other public bodies and seeing that they are applied;
- coordinating Belgium's representation in international fora on cybersecurity, keeping track of international obligations and presenting Belgium's views;
- coordinating the security evaluation and certification of ICT systems;
- informing and raising the awareness of users of information and communication systems.

In the course of time, the CCB, working together with the relevant actors and authorities, will establish procedures to simplify incident management and communication between the various actors in the event of incidents or attacks. It will play a leading role in coordinating the authorities and actors with responsibility for tackling cyber threats.

The Belgium Network Information Security (BELNIS) provides a forum for federal bodies to consult one another on national information security challenges and on what should be done about them. BELNIS is the only forum where those actually involved on the ground can meet one another. Its permanent members include: the strategy unit of the Minister/State Secretary in charge of state digitalisation, the Privacy Commission, the National Security Authority, the Social Security Register, the Belgian Institute of Postal Services and Telecommunications, the Federal Computer Crime Unit, the General Intelligence and Security Service (FPS Defence), the FPS for the Economy, Fedict, the Crisis Centre (FPS for the Interior), the Federal Intelligence and Security Agency, the Public Planning Service for Science Policy, the FPS Justice, the Federal Public Prosecutor's Office, the College of Principal Public Prosecutors and the Coordination Unit for Threat Assessment (risk assessment). BELNIS can call on outside experts if needed. The working party's meetings are held as and when the need arises.

BELNIS does not play any role in the operational management of security incidents, but obviously such incidents inform the discussions of the experts involved.

The Federal Public Prosecutor's Office: the public prosecutor and/or the examining magistrate investigating the offences organise law enforcement as between the various national authorities. If critical infrastructure comes under attack, action is coordinated by the Federal Public Prosecutor's Office.

At the time of the visit, the CCB was still in the process of defining its role and recruiting staff. As yet its role is not fully defined, and the flow of information in the event of an incident is not clearly defined either. The evaluation team is also unclear as to who will trigger the crisis response in the event of a major incident. In our view it will be hard to involve academia, as the B-CCENTRE university project has been abandoned.

4.4.1 Legal or policy obligations

The reporting of cybercrime offences is covered by ordinary criminal procedure. As a general rule, Belgian law does not require individuals or undertakings to report cybercrime incidents or offences.

Where critical infrastructure is concerned, Article 14 of the law of 1 July 2011 on the security and protection of critical infrastructure requires operators to notify the relevant authorities of any incident which might threaten the (physical or IT) security of their infrastructure.

There is no legal obligation, but the government has set up a centre (the federal cyber emergency team) to centralise information and provide assistance to businesses (https://www.cert.be/fr).

The CCB is currently working with all the bodies concerned (FCCU/CCU/CERT/SGRS, etc.) to draw up a procedure for the management of national cyber incidents and cyber crises, with a clear definition of the procedures to follow and the roles and responsibilities of each body.

After the evaluation visit an emergency national cyber plan was approved by the National Security Council, subject to the approval of the Council of Ministers. The plan sets out procedures to be followed and protection measures to be taken in the event of cybersecurity incidents. Three levels are identified: national cybersecurity crisis situations, cybersecurity incidents and minor cybersecurity incidents.

The federal police's FCCU takes part in the working party on internet banking security, which studies the vulnerabilities and threats associated with on-line banking fraud. As part of plans to improve the federal police, it was decided that there should be no national follow-up on other forms of payment card fraud, as these cases are dealt with the by federal police services in the judicial districts, which also have good contacts with the industry, but more on a case-by-case basis.

Under Article XII.17 of the economic legislation, operators can be ordered to adopt certain methods of freezing data. If they find that an offence has been committed or if an offence is reported to their services, they have a duty to preserve all the data and make them available to the public prosecutor.

4.4.2 Resources allocated for improving cooperation

As regards the federal CID, there is a sustained effort to boost cooperation with the private sector. The resources earmarked for this cooperation are measured purely in terms of human resources; no financial resources are available.

Collaboration with academia, begun in 2011 with the creation of a centre of excellence, the B-CCENTRE, has meant that anti-cybercrime needs, as expressed by the judicial authorities and the police, have been taken on board in projects on training, R&D and prevention.

There has been over ten years of active cooperation with the Federation of Belgian Enterprises (FEB) in order to draw up standards and guides to good practice and to carry out awareness and prevention campaigns (targeted especially at business).

Lastly, it is worth mentioning investment in participation in international initiatives on training (ECTEG) and R&D, such as the FREETOOLS project, under which Europol/EC3 made forensic tools available to specialised investigators free of charge.

Cooperation can be launched on an ad hoc basis, as new phenomena emerge. For example, following attacks on on-line banking systems, cooperation with the industry, via FeBelFin, and the five major banking entities in Belgium, in collaboration with the Belgian central bank (previously with the CBFA) has reduced the losses sustained by banks and individuals and resulted in new security standards, imposed by the regulatory body (the central bank).

4.5 Conclusions

The FCCU is the specialised police service for combating cybercrime at federal level, in charge of major investigations in the area. There are also specialised federal police bodies, the RCCUs, at regional level. The evaluation team noted that cybercrime also came within the remit of local police services, and that they had also set up some specialised units, the LCCUs. The evaluation team noted that there was some unease about a lack of clarity and hierarchy regarding the bodies set up by the federal police and the local police services.

The evaluation team is aware that digital evidence is needed for a large number of offences. Given that these offences come within the remit of the regional units of the federal police or of local police services, the latter call on the RCCUs for technical support, which means that the RCCUs spend 90% of their time on this support role.

Owing to a lack of human resources in the RCCUs, the LCCUs carry out inquiries involving digital evidence without having the necessary expertise, and, at the same time, the RCCUs are unable to conduct their own enquiries.

As there is a high probability that inquiries may suffer as a result, the Belgian authorities should seek to remedy the situation by giving the FCCU a coordinating role and the task of laying down a set of good practices and compulsory training courses for all the units concerned.

To do this, however, the FCCU and RCCU budget would need to be increased, bearing in mind that expertise in digital evidence is needed not only for offences specifically linked to cybercrime, but also for every other type of offence including terrorism and other forms of organised crime.

It should be noted that one of the fundamental points of the new national security plan for 2016-2019, entitled '*Aller ensemble à l'essentiel*' [Working together to tackle essentials] is to *improve the police approach to IT crime, taking into account developments in terms of the internet, innovation and new technologies.* To this end, it recommends organising coordinated measures in the approach to cybercrime and cyber security and increasing expertise and knowledge of these areas in the police services.

During the evaluation visit, a number of critical points were raised with the evaluation team in discussions with various federal, regional and local police services. The most salient points are as follows:

- shortage of staff;
- recruitment procedures not geared to the required profile;
- too few training courses;
- failure to plan ahead when colleagues are due to leave;
- inappropriate pay levels (a conventional police officer earns more than a central-level specialist);
- competition between the various services (FCCU, RCCUs and LCCUs);
- inadequate equipment (for example, only one (SLOW) internet access for 10 investigators in the CSAM section);
- a manifestly inadequate training budget.

At least the above problems were clearly identified by practitioners.

The national security plan for 2016-1019 contains a specific reference to improving the police approach to combating cybercrime. This is a priority, and the political authorities will therefore be obliged to respond by giving law enforcement agencies the staff and resources to enable them to carry out their tasks satisfactorily.

As regards institutional matters, the evaluation team acknowledges the efforts made by the Public Prosecution Service to support specialisation by a number of judges in the federal and regional prosecution services.

One decision that should be highlighted is that giving Antwerp's principal public prosecutor responsibility for cybercrime coordination, centralising cybercrime expertise at the federal public prosecutor's office, in conjunction with the FCCU (circular 9/2009), creating an expert network at the College of Principal Public Prosecutors and appointing specialist cybercrime judges at every regional public prosecutor's office.
On the judicial side, the evaluation team found that training for judges was inadequate, in particular for examining magistrates, especially given their investigative responsibilities.

5 LEGAL ASPECTS

5.1 Substantive criminal law pertaining to cybercrime

5.1.1 Council of Europe Convention on Cybercrime

The Kingdom of Belgium is party to the 'Budapest Convention' which it ratified by the law of 3 August 2012 approving the Convention on Cybercrime, done at Budapest on 23 November 2001. This law was published in the Belgian Official Gazette on 21 November 2012 and officially entered into force on 1 December 2012.

The Belgian government entered a number of reservations and statements on the Convention. The reservations chiefly concern Article 22 of the Budapest Convention, which lays down rules on jurisdiction which parties must establish for any criminal offence established in accordance with the convention. Another reservation concerns internal hacking offences (Article 550bis(2) of the Criminal Code) and computer fraud (Article 210bis of the Criminal Code), which have a narrower interpretation in Belgian law, as they must be have been committed with fraudulent intent or intent to cause damage.

5.1.2 Description of national legislation

A/ Council Framework Decision 2005/222/JHA on attacks against information systems and Directive 2013/40/EU on attacks against information systems

Title IXbis of Book II of the Criminal Code on offences against the confidentiality, integrity and availability of computer systems and the data stored, processed or transmitted by those systems contains the offences of hacking and sabotage of data and systems.

1. Hacking (Article 550bis of the Criminal Code)
Hacking covers:

a) external hacking (Article 550bis(1) of the Criminal Code); b) internal hacking (Article 550bis(2) of the Criminal Code); c) offences relating to 'hacking tools' (Article 550bis(5) of the Criminal Code); d) incitement to hacking (Article 550bis(6) of the Criminal Code); d) handling data obtained by hacking (Article 550bis(4) of the Criminal Code); f) manipulating data in a computer system (Article 550ter(1) of the Criminal Code).

2. Sabotage of data and systems (Article 550ter of the Criminal Code)

Sabotage covers:

a) offences relating to tools for the sabotage of data or systems (Article 550ter(4) of the Criminal Code);

b) illegal interception of computer data (Articles 259bis and 314bis of the Criminal Code).

This category also includes the criminal interception of data during transmission (eavesdropping offences) referred to in Article 259bis and 314bis of the Criminal Code, and the criminal interception of data before, during or after transmission (Article 550bis(1) and (2) and the first indent of (3) of the Criminal Code).

The ordinary law rules on the criminal liability of legal persons apply. Pursuant to Article 5 of the Criminal Code, under Belgian criminal law legal persons bear separate criminal liability for their acts, irrespective of the conduct of the natural person through whom they act.

Legal persons can, in principle, be held criminally liable for any offence, including an IT offence. The legislator has not placed any limits on this liability.

Pursuant to the first subsection of Article 5 of the Criminal Code, it is possible for an (IT) offence to be attributed (substantively) to a legal person (this is the objective element determining whether a person is the perpetrator of an offence), but only where there is an intrinsic link between the offence and the legal person, in other words, where the offence was committed to attain the corporate body's object (as set out in its articles of association) or in defence of its interests, or where concrete evidence shows that the offence was committed on its behalf. These are alternative criteria, although this does not of course rule out the possibility that the substantive element of liability may also be present if several criteria are met. This does not imply, however, that any substantive event involving an intrinsic link with a corporate body's object or the defence of its interests, or which was committed on its behalf, can automatically be attributed to it.

As with natural persons, a legal person must be responsible for the (IT) offence (the subjective element determining whether a person is the perpetrator of an offence). In other words, it must be possible to blame the offence on the legal person. This means that just like a natural person, a legal person can be held criminally liable only if both the objective and subjective elements of the offence are present. It is thus criminal-law logic which is followed: it is the person who committed the offence who is punished for it. Even if the legal person's fault is closely connected with the natural person's fault, a pertinent criminal fault must be established on the part of both persons. The court must also find that the legal person is at fault. The case law of the Court of Cassation confirms that legal persons do have a will of their own, which can be the source of an offence, even though *de facto* they act through individuals. In order for an offence to be attributed to a legal person (attributability), its intent must also be demonstrated; it cannot simply be deduced from the intent of the natural person.

Article 7bis of the Criminal Code lays down the penalties for offences committed by legal persons. The main punishment is therefore a fine. Article 41bis of the Criminal Code lays down a mechanism for converting custodial sentences for natural persons into fines for legal persons. Article 7bis of the Criminal Code also lays down a number of specific supplementary penalties.

Belgian law does not provide for criteria such as high economic, political or social impact, the number of affected systems or level of damage. On the other hand, Article 550ter(3) of the Criminal Code makes it an aggravating circumstance to partially or completely prevent the computer system concerned or any other computer system from working properly.

There are no 'minor cases' in the Belgian Criminal Code. It is for the prosecuting authority to judge whether a particular offence should be prosecuted. The Public Prosecution Service can decide whether or not it is appropriate to prosecute and/or can also propose alternative means of dispute settlement (mediation in criminal cases, compromise settlement, judicial probation, etc.) .

In addition to the cybercrime offences already mentioned, there are a number of acts of cybercrime which constitute criminal offences, but do not come under any of the three categories of the GENVAL evaluation. In this context, it is worth mentioning the offences provided for in the law on electronic communications.

There are a number of IT offences in the specialised legislation, as laid down in the law of 13 June 2005 on electronic communications, which give rise to a vast array of criminal provisions, some of which are not so easy to classify, while the distinction between these provisions and the criminal provisions in Book II of the Criminal Code does not always seem clear (Article 145(3bis), 124(1) and (4) of the law of 13 June 2005 on electronic communications [12]). There is also the Code of Economic Law, Book XII, Law of the electronic economy (formerly the law of 11 March 2003 on certain legal aspects of information society services; Articles 21 and 26 of the law of 11 March 2003).

The Justice Minister's 'Justice' plan expresses a determination to implement the most urgent changes in terms of cybercrime and crime using the internet.

A bill designed to increase the penalties in Articles 314bis and 550bis of the Criminal Code has been submitted to the Justice Minister's strategy unit. It is designed to incorporate the whole of Directive 2013/40/EU into Belgian law.

[12] Moniteur Belge [Belgian official gazette] 20 June 2005.

Belgian law is mostly in line with the provisions of the Directive. A correlation table has already been forwarded to the European Commission. A bill designed to increase the penalties in Articles 314bis and 550bis of the Criminal Code has been submitted to the Justice Minister's strategic unit. These are the only amendments needed for full compliance with the Directive.

The recent Article 371/1 of the Criminal Code, on voyeurism, criminalises spying, either directly or by some technical means, on a person in a state of nakedness or engaged in an explicit sexual act, and also distributing a video or audio recording of a person in a state of nakedness or engaged in an explicit sexual act, without the consent of or unknown to the person concerned, even if the person agreed to its production.

B/ Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA

Almost the whole of Directive 2011/93/EU has been incorporated into Belgian law. A few minor amendments were still needed. Accordingly, on 16 October 2015, at the suggestion of Justice Minister Koen Geens, the Council of Ministers approved a draft bill supplementing implementation of the European requirements on the sexual exploitation of children, child pornography, human trafficking and facilitation of unauthorised entry, transit and residence.

The draft bill has a three objectives:

- to continue bringing Belgian legislation into line with European Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims;
- to make selective changes to criminal law and criminal procedure to comply more fully with the requirements of European Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography;
- to continue bringing Belgian legislation into line with Directive 2002/90/EC defining the facilitation of unauthorised entry, transit and residence and strengthen the criminal law framework to enforce the law against facilitating unauthorised entry, transit and residence.

In this context, a solution is also proposed for removing websites, in order to meet the requirements of Article 25(1) of the Directive, in accordance with which such removal must be rapid.

The preliminary draft bill has now been submitted for opinion to the Council of State, and it will then be subject to debate in parliament.

Conventional sexual offences apply in particular when information and communication technologies are abused in order to adopt criminally punishable sexual behaviour towards minors.

The offences concerned are, therefore, indecent assault and rape (Articles 372-378bis of the Criminal Code), incitement to sexual offences against minors, corruption of young people and prostitution (Articles 379-382quater of the Criminal Code) and the possession or production of child pornography (Article 383bis of the Criminal Code).

Specific mention should be made in this connection of two laws which are part of a trend towards modernisation of the Criminal Code concerning sexual offences against children and young people, using internet or other information and communication technologies.

The law of 30 November 2011 amending the legislation on improving the approach to sexual abuse and child pornography offences in a relationship of authority (Articles 7 and 12 of the law of 30 November 2011) introduced an expanded offence of child pornography which has been applicable since 30 January 2012. In addition to 'punishable possession', 'access to [child pornography]' has also become punishable. Further to this law, anyone who knowingly accesses child pornography, via a computer system or any other technological means, risks the same penalties as a person in possession of child pornography material. This comes in the context of implementation of the Lanzarote Convention on the protection of children against sexual exploitation.

With the same objective and pursuant to the Council of Europe's Lanzarote Convention and the EU Directive on combating sexual abuse (Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011, OJ L of 17 December 2011), the Law of 10 April 2014 on the protection of minors against grooming with a view to the perpetration of sexual offences inserted, in the chapter of the Criminal Code relating to 'indecent assault' and 'rape' offences, a new aggravating circumstance for the offence of (online) grooming (Articles 377ter and 377quater of the Criminal Code). This same law also introduced the new offence of cyberstalking (Article 433bis/I of the Criminal Code).

The new specific criminal law provisions incontestably prove their usefulness in practice vis-à-vis conventional offences in connection with combating child abuse via internet or other information or communication technologies, but also, unfortunately, contribute towards growing confusion between Belgian criminal law governing sexual offences in general and criminal law on sexual offences aiming to protect minors in particular.

C/ Online payment card fraud

Citizens and private companies almost always report payment card fraud to the (local) police because banks require a copy of the report/declaration made to the police in order to refund the amount involved in the fraud.

The federal police's FCCU is involved in the working group on 'Internet banking security', which focuses on weaknesses and threats concerning online bank fraud. As part of plans to improve the federal police, it was decided that there should be no national follow-up on other forms of payment card fraud; these cases are dealt with by the federal police services in the judicial district, which also have good contacts with the industry, but more on a case-by-case basis.

Offences relating to online payment card fraud include:
- computer forgeries and use of such forgeries (Article 210 bis of the Criminal Code)
(a) computer forgeries (Article 210bis(1) of the Criminal Code)
(b) use of false computer data (Article 210bis(2) of the Criminal Code)
- computer fraud (Article 504quater of the Criminal Code)
- identity theft (no specific offence).

It should be pointed out in this respect that identity theft is not a specific offence in Belgium, but it may be prosecuted on the basis of other criminal law provisions. For instance, it is described as assuming a false identity (Article 231 of the Criminal Code) and forged documents.

D/ Other cybercrime phenomena

Belgian legislation applicable with regard to cybercrime is confined to three major categories of offences:

- computer forgeries and use of such forgeries;
- computer fraud and offences against confidentiality;
- offences against the integrity and availability of computer systems and stored data (sabotage, hacking, etc.).

According to the evaluation team, Belgium's body of legislation is fairly satisfactory in that it encompasses most types of harmful conduct perpetrated on and with the aid of the internet.

5.2 Procedural issues

5.2.1 Investigative techniques

All the investigative techniques mentioned in the GENVAL questionnaire are authorised under Belgian law.

- **searches and seizure of IT information/data systems**

Under Belgian law there is, first and foremost, the possibility of seizure of data hardware in accordance with Article 35 et seq. of the Code of Criminal Procedure. Seizure of data is also possible in accordance with Articles 39bis and 89 of the Code of Criminal Procedure. There is also the possibility of searching the network in accordance with Article 88ter of the Code of Criminal Procedure.

- **real-time interception/collection of traffic/content data**

Belgian law allows for data capture during transmission or 'eavesdropping', as provided for in Article 90ter of the Code of Criminal Procedure.

- **retention of computer data**

In accordance with Article 88bis of the Code of Criminal Procedure, it is possible to record internet communications or the use of internet.

The legal rules on data retention have been transposed into Belgian law and were set out in Article 126 of the law on electronic communications. However, this legislation was annulled by judgment No 84/2015 of the Constitutional Court of 11 June 2015. The Constitutional Court thus followed the assessment in the judgment of the Court of Justice of 8 April 2014 (CJEU, 8 April 2014, C-293/12 and C-594/12), giving rise to the annulment of the Directive on data retention.

New domestic regulations are currently being drafted on the subject.

- **orders to produce stored traffic/content data**

A distinction should be made between the recording and retention of data by the telecommunications provider, on the one hand, and a request for such data during a criminal investigation by the competent judicial authority, on the other.

On the basis of Article 88bis of the Code of Criminal Procedure, the location data and traffic data may legitimately be requested by the competent authority.

In accordance with Article 126(2) in fine of the law of 13 June 2005 on electronic communications, the data collected during data retention should be transmitted on request. There is currently no obligation regarding communication, in view of the annulment of the 'data retention' provision.

- **orders to communicate data on users**

The identification of subscribers/users and services/means of communication (Articles 46bis and 56(1) of the Code of Criminal Procedure).

These provisions are rather outdated as they were initially designed for tracking and tapping telephone calls; a reform linked to the transposition of the Directive on data retention (2006/24/EC) was censured by a judgment of the Constitutional Court of 11 June 2015.

Since the law of 4 February 2010[13] (amending the organic law on intelligence and security services of 20 November 1998), the Belgian intelligence and security services (the 'Sûreté de l'État' (State Security Service) and the 'Service général du renseignement et de la sécurité' (General Intelligence and Security Service)) have been entitled to take ordinary (Articles 14 to 18), specific and exceptional (Article 18/I to 18/18) measures to collect data and achieve the objectives assigned to them.

These articles make provision in particular for the following special investigative techniques: the possibility of identifying a subscriber to or user of an electronic communications service, telecommunications interception and hacking.

[13] Belgian Official Gazette, 4 February 2010.

The particular search methods which can be used by the competent judicial authorities are listed in Articles 47ter et seq. of the Code of Criminal Procedure. These methods are observation and infiltration and the use of informers.

In major cybercrime cases, and certainly those in which the banking sector is the victim, financial gain for the cybercriminals is a very important factor. Belgium used this as a starting point for opening some cases. The cybercrime investigation is also accompanied by a financial investigation . In this connection, the work of the cybercrime and financial investigators within multidisciplinary teams proves useful.

5.2.2 Forensic examination and encryption

The police services, particularly the Federal Computer Crime Unit and the Regional Computer Crime Units, carry out digital forensic examinations, including remotely.

Encryption poses a real and constantly increasing problem, not only in forensic examinations but also in all other types of investigation:

- inability to analyse 'TrueCrypt' encrypted volumes without the suspect's cooperation;
- use of means of communications such as 'WhatsApp' and 'Telegram', mainly on smartphones;
- use of HTTPS protocols for the most common websites (Google, Facebook, etc.);
- in certain cases, the encryption key is not available to service providers (software vendors), but is generated and managed solely by the users;
- the appearance of 'second proxy' technology installed by major service providers such as Facebook and Google, which even incorporate it into their Android and Chrome systems. This technology replaces the DNS requests made by the device used by the end user by making all requests within the HTTPS encrypted tunnel, no longer leaving any unencrypted data available for the investigation.

5.2.3 E-evidence

Belgian law contains no specific provisions on e-evidence. In general, copies of data used as evidence are made on DVD or hard disk. In this respect, reference may be made to the confidential circular COL 16/2004 of the College of Principal Public Prosecutors, to which a technical annex has been attached, which sets out the guidelines on forensic examinations and on the processing of digital information.

Evidence in criminal matters is governed by the Code of Criminal Procedure and the legal principles of criminal procedure. The taking of evidence is generally free (principle of evidence by all means). There are no particular conditions of admissibility for e-evidence.

Article 32 of the Preliminary Title of the Code of Criminal Procedure sets out the criteria applied with regard to admissibility of evidence: '*An item of evidence obtained in an irregular manner is determined to be invalid only if:*
- the formal conditions that apply have not been observed , or;
- the irregularity committed has harmed the reliability of the evidence; or
- the use of evidence conflicts with the right to a fair trial'.

Article 13 of the law of 9 December 2004 on international mutual legal assistance in criminal matters[14] governs the situation regarding evidence abroad: '*Within the framework of a case before a Belgian court, no use can be made of evidence: 1. which was unlawfully gathered in a foreign country if the unlawfulness: - bears the mark of manifest illegality on account of infringement of essential procedural requirements according to the law of the State where the evidence was gathered; - harms the reliability of the evidence; 2. of which the application would imply an infringement of the fundamental right of a fair hearing.'*

[14] Belgian Official Gazette, 24 December 2004.

5.3 Protection of human rights/fundamental freedoms

The Belgian Constitution guarantees the fundamental rights inspired in particular by the Declaration of the Rights of Man and of the Citizen. There is no specific legislation concerning these principles for the internet.

The surge in new media and computerised data is taken into consideration by the Commission for the Protection of Privacy (CPP) which, in parallel to awareness-raising activities, has coercive and enforcement tools. The publications, including the annual report, are available on the CPP's website[15].

Apart from that, the investigation, prosecution and judgment of computer crime offences represent a significant encroachment on fundamental rights, as does the use of information and communication technologies (ICTs) in criminal proceedings and the establishment of informative positions,. We are perfectly aware of this in the Belgian legal system. The following principles are respected as far as possible in Belgian law:

- Any restriction of the right to privacy must be laid down by law and must be proportionate, legitimate and necessary in a democratic society.

- The use of ICTs in criminal proceedings and the establishment of informative positions must respect the right to data protection. The objectives of crime prevention and the criminal investigation are balanced against the infringement of fundamental rights to data protection.

[15] https://www.privacycommission.be/fr.

- The purpose limitation principle is respected, particularly when personal data are forwarded electronically to the law enforcement authorities. The purpose limitation principle means that the personal data may only be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.

- A derogation from the purpose limitation principle may be made only in exceptional cases, provided for by law, in which the transfer of data to the law enforcement authorities is necessary for the prevention, investigation or prosecution of a serious crime and respects the proportionality principle.

- The legal framework must ensure, more generally and as far as possible, that adequate means and thresholds for access to and disclosure of stored data are established and monitored by an independent authority. If an obligation to update, retain and despatch computer data lies with a public and/or private undertaking, the latter must respect the right to data protection.

- The use of ICTs in criminal proceedings must not infringe the rights of the defence, in particular the right to a public hearing, the right to cross-examination and to confrontation, the right of access to a file and the right to the assistance of experts specialising in the field of e-evidence, in order to ensure the principle of equality of arms.

5.4 Jurisdiction

5.4.1 Principles applicable to investigations of cybercrime

When one of the constituent elements of a what is defined as an offence can be located on Belgian territory, the Belgian authorities have jurisdiction.

Even so, there are two aspects to the response, i.e. whether the computer offences were committed in part or in full on Belgian territory.

(a) For computer offences committed **in part** outside the territory of the Kingdom, we can invoke the **principle of territoriality**. Article 3 of the Criminal Code states that 'an offence committed on the territory of the Kingdom, by Belgians or by foreigners, must be punished in accordance with Belgian law.' Article 3 of the Criminal Code therefore respects the principle of territoriality with regard to the scope of positive criminal law: criminal law applies solely to national territory, apart from exceptions arising from provisions of domestic law of international conventions.

In principle, Belgium therefore has jurisdiction if the offence in its entirety was committed on Belgian territory but also if it was partly committed there. The principle of territoriality as a criterion of jurisdiction has in fact developed from single-territory jurisdiction to partly territorial jurisdiction or a concept of extended territoriality.

In Belgium we apply the theory of objective ubiquity to multi-territory actions. If an offence occurs on the territory of various States (multi-territory offence), Belgium has jurisdiction if one of the constituent (objective) elements (parts of the material element) of what is defined as a Belgian offence can be located in Belgium. It may only be located on the territory by locating elements which constitute the offence. Thus, the result of the offence will lead to territorial jurisdiction only if that result is a constituent element of the offence (the *constitutive* result). That of course depends on the specific article of law.

Furthermore, Belgian case law considers that Belgian courts also exercise their territorial jurisdiction when they deem that an offence committed abroad forms an indivisible whole with an offence located in Belgium. Thus, Belgian courts consider that they have jurisdiction, for example, in the case of foreigners taking part in a Belgian offence or of punishable actions committed abroad which form an indivisible whole with punishable acts committed in Belgium (continuous offences and, less obviously, continued offences). They consider that they have jurisdiction when part, or an inseparable aspect, of the offence occurs on Belgian territory. They interpret this as also referring to the consequences which become evident only once the offence has been committed, but which nevertheless form an indivisible whole with the offence. This sometimes leads to 'disguised' extraterritorial applications of Belgian criminal law. Under the territorial application of criminal law, Belgian criminal law applies to offences committed abroad. Its *ratione loci* scope therefore extends beyond Belgian territory. A legal construct is thus created in which the offences are assumed to have been committed in Belgium. The combining by Belgian case -law of the theory of objective ubiquity and the theory of indivisibility may lead to a de facto application of the theory of effects. At this level, the criminal court takes into consideration not only the constituent effects of the offence, but also the other effects eliminated.

(b) For computer crime which is committed **in its entirety** outside the territory of the Member State, the rules of ordinary law on the applicability of Belgian criminal law apply to offences committed abroad. Article 4 of the Criminal Code states that 'An offence committed outside the territory of the Kingdom, by Belgians or by foreigners, shall be punished in Belgium only in those cases determined by law'.

The exceptions are indicated primarily in Articles 6 to 14 of the Preliminary Title of the Code of Criminal Procedure. These exceptions are based on a number of principles.

The **personality principle or the active nationality principle**, based on the nationality of the perpetrator, leading to the application of Belgian criminal law to Belgians who have committed crimes or offences abroad (Articles 7 and 9 of the Preliminary Title of the Code of Criminal Procedure). This principle is linked to that according to which States do not generally extradite their own nationals.

The **protective principle or the passive nationality principle**, based on the victim's nationality, leading to the application of Belgian criminal law to foreigners who have committed abroad certain crimes or offences against a Belgian national. It was introduced only by the law of 12 July 1981 (Article 10(5) of the Preliminary Title of the Code of Criminal Procedure). It applied beforehand only to offences committed in wartime (Article 10(4) of the Preliminary Title of the Code of Criminal Procedure).

The **principle of State protection**, based on the idea that the domestic social order is firstly disturbed by offences committed abroad when the Belgian State is the direct victim of the offences committed, leading to the application of Belgian criminal law to offences against State security or against Belgian monetary values or the euro, committed by any Belgian or foreign person outside Belgian territory (Article 6(1) and (2) and Article 10(1) and (2) of the Preliminary Title of the Code of Criminal Procedure). The principle of State protection is also linked to the fact that such offences are not always punishable under the *lex locus delicti*.

The **principle of universality**, based on the nature of the offence and the interests of the international community. The Law of 16 July 1993 had given this principle broad scope for covering serious violations of international humanitarian law. In response to American pressure the law was repealed by the Law of 5 August 2003. The principle of universality now mainly covers foreign currency offences (Articles 6(3°) and 10(3°) of the Preliminary Title of the Code of Criminal Procedure) and, following the laws of 13 April 1995 and 28 November 2000, sexual offences (Article 10*ter* of the Preliminary Title of the Code of Criminal Procedure).

5.4.2 Rules in case of conflicts of jurisdiction and referral to Eurojust

As indicated under question 1, material territorial jurisdiction or the *locus delicti* in cyberspace is established mainly through applying the 'theory of objective ubiquity' and the 'theory of indivisibility', based on Article 3 of the Criminal Code.

Based on this concept of an enlarged territory, there are indeed cases where Belgium and other states have equal jurisdiction over the same offences. If a number of different states apply this approach it can cause some difficulties. It is indeed possible to be working simultaneously on the same suspects or groups of perpetrators or for certain offences to be subject to criminal proceedings in Belgium despite their not being punishable according to another state involved in the matter.

In the event of conflicts over jurisdiction, where two or more Member States could open an investigation or initiate proceedings against the same perpetrator, consultations are held with the Member States in question, if necessary through Eurojust, with a view to reaching workable agreements.

Moreover, the general legal principle of "*ne bis in idem*" also applies to cybercrime in Belgium.

A number of cybercrime-related cases have already been submitted to Eurojust on provisions related to Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings, and the results have been positive. In some cases this has led to the establishment of a joint investigation team (JIT).

5.4.3 Jurisdiction for cybercrime offences committed 'in the cloud'

Extraterritorial data searches are allowed where such data cannot be collected in Belgium. The data may only be copied (not blocked).
The Ministry of Justice must be notified and subsequently informs the competent authorities in the relevant Member State.

5.4.4 Belgium's view on the legal framework for combating cybercrime

The international mutual legal assistance instruments are inadequate, since the volatile nature of evidence available from the internet requires quick reactions and flexible arrangements.

5.5 Conclusions

Belgium's laws are broadly suitable for combating cybercrime. The evaluation team welcomes the country's efforts towards preparing a law to improve specific search methods and a number of measures for investigations concerning the internet, electronic communications and telecommunications.

The evaluation team also welcomes the Belgian courts' perseverance in the controversial case with the American company Yahoo. Belgian courts may contact Yahoo directly to obtain identification data in connection with an investigation.

Whilst the evaluation was taking place, the government was examining issues related to the data retention law, which the Constitutional Court had declared unconstitutional (decision of 11 June 2015). On 18 July, following the evaluation visit, the the law of 29 May 2016 on data collection and retention in the telecommunications sector was promulgated
We would stress the need for EU harmonisation in this area, and also as regards the duties incumbent on service providers that enable access to European territory to cooperate directly, without the mutual legal assistance arrangements (Yahoo case law).

Following the evaluation visit the Belgian authorities informed the evaluation team that the Belgian legislation on specific methods had been updated by the '*Law of 25 December 2016 amending the Code of Criminal Procedure and the Criminal Code in order to improve specific search methods and a number of investigation measures for use with the internet, electronic communications and telecommunications and establishing a voice-print database*'.

The main changes to the Code of Criminal Procedure are as follows:

- clarification and improvement of the rules governing non-confidential searches in an IT system;
- implementation of the Convention on Cybercrime through the creation of a procedure on data freezing;
- extension of discreet visual surveillance;
- creation of a specific measure covering interaction or infiltration that occurs exclusively on the internet;
- with regard to interception of telecommunications: merging of confidential searches in an IT system with interception of telecommunications, and extension of the list of offences for which the measure can be used;
- legal basis for a database containing voice prints that feature in intercepted telecommunications.

An amending law was adopted on 29 May 2016 (*law on data collection and retention in the electronic communications sector*). Several actions for annulment of that law have been lodged with the Constitutional Court following the Court of Justice's judgment of 21 December 2016.

The '*law of 31 May 2016 completing the implementation of EU obligations in the field of child sexual exploitation, child sexual abuse material, trafficking in human beings and facilitation of unauthorised entry, transit and residence'* finalises the transposition of Directives 2011/93/EU (sexual abuse and sexual exploitation of children), 2011/36/EU (trafficking in human beings) and 2002/90/EC and Council Framework Decision 2002/946/JHA (facilitation of unauthorised entry, transit and residence).

6 OPERATIONAL ASPECTS

6.1 Cyber attacks

6.1.1 Nature of cyber attacks

Number of cyber attacks recorded

Offence	Articles of Criminal Code	Number of cases recorded			
		2013	2014	2015	Quar 3 2016
Hacking	Art. 550 bis Criminal Code	1 745	2 054	2 159	1 682
Sabotage	Art. 550 ter Criminal Code	1 186	431	423	349
Telecommunications / interception	Art. 259 bis & Art. 314 bis CC	88	84	83	49
Total		**3 019**	**2 569**	**2 665**	**2 080**

Source: Police database, 20/01/2017

The numbers of cyberattacks have been rising for several years. In 2012, and less clearly in 2013, we have seen an atypical peak in the numbers — especially in the numbers of acts of sabotage— following the wave of the 'police ransomware' virus.

6.1.2 Mechanism for responding to cyber attacks

There is no legal obligation, but the government has set up a centre (the federal cyber emergency team) to centralise information and provide assistance to businesses (https://www.cert.be/fr).

On 28 April 2017, the Council of Ministers approved the national cyber emergency plan drawn up by the CCB in cooperation with all the entities concerned (FCCU/CCU/CERT/SGRS, etc.). This plan contains a procedure for the management of national cyber incidents and cyber crises, with a clear definition of the procedures to follow and the roles and responsibilities of each body.

When dealing with cyber attacks outside the Union, Belgium uses the mutual legal assistance instruments wherever they are essential. Direct information exchange is also used within the constraints imposed by national and foreign legislation, as well as information exchange between police forces.

6.2 Action against child pornography and online sexual abuse

6.2.1 Databases identifying victims and measures to avoid re-victimisation

The federal judicial police is connected to Interpol's ICSE (International Child Sexual Exploitation) database. Access is provided by the 'child pornography' section of the Directorate for the fight against serious and organised crime (DJSOC).

DJSOC handles reports until a final procedure has been established by the courts. Websites hosted abroad that contain child (sexual) abuse/exploitation material (CAM, CSAM or CSEM) are listed in a report which is sent to the relevant countries through SIENA (Europol) or Interpol channels.

Where such websites are hosted on Belgian territory, a report is drawn up to secure the magistrate's agreement to close the relevant website.

6.2.2 Measures to address sexual exploitation/abuse online, sexting and cyber bullying

Campaigns, posters and leaflets explaining the dangers facing children are distributed every year by Child Focus.

Communities and Regions (in charge of education, which is not a federal competence) are considering including awareness-raising in school curricula.

The website of Child Focus www.clicksafe.be informs children, young people, parents and practitioners about secure and responsible use of the internet. They can find related information, a helpline for problems, information about training courses and links to other interesting websites. 'Clicksafe' training courses are provided to professionals working with children and young people to help promote dialogue on 'secure and responsible' use of the internet.

6.2.3 Prevention of sex tourism, child pornographic performances and other phenomena

A number of preventive poster campaigns have been used in airports and travel agencies to attract the attention of travellers and front-line police by depicting the typical profile of a sex tourist.

The NGO ECPAT (End Child Prostitution, Child Pornography and Trafficking of Children for Sexual Purposes) has coordinated these campaigns. A national group was set up bringing together the Police, Foreign Affairs, Defence and Justice (Criminal Policy Service) ministries, the Federation of the Tourist Industry, the Royal Federation of Belgian Carriers and Logistic Service Providers, Plan Belgium, Child Focus, the Samilia Foundation and ECPAT Belgium. The group, named 'STOP', has been running for ten years and focuses on influencing the tourist industry, young people themselves, judicial bodies and the public authorities.

On 6 November 2014, STOP launched an awareness-raising campaign: 'I say STOP'. A website was set up (www.jedisstop.be) and a brochure was published as part of this third awareness-raising campaign. The aim of the campaign is to re-awaken public awareness of child victims of sexual abuse and to tell people who come across a suspicious situation that they can help the authorities by reporting it on the website www.jedisstop.be and filling in a special form, which contains the main information needed to launch an investigation. The Belgian police then pass on the information to colleagues in the relevant country and, where necessary, to Europol and Interpol. Regardless of the nationality of the reporting person or of the presumed perpetrator, a report may also be made on the new European online platform www.reportchildsextourism.eu which includes all the national alert lines in Europe.

In terms of preventive measures, the NGO Child Focus runs awareness-raising campaigns and, amongst other things, circulates brochures. A range of prevention tools have been developed:

- advertising slot warning against 'sexting'[16]: aimed at 13- to 16- year -olds, which encourages them to reflect on the impact of their online behaviour;
- personal test '*es-tu hot sur Internet?*'[17] ('are you hot on the internet?'): quiz for 12- to 17-year- olds on relationships, feelings and sexuality;
- online application '*Qui est-ce?*'[18] ('who's there?'): for 11- to 16 -year-olds concerning discussions and meetings with new people on the internet. Young people can learn about things that can happen on the web and how to have a totally safe online chat and recognise suspicious discussion partners;

[16] https://www.youtube.com/watch?v=LkJ5qcuebVA&list=UUeLTgN3i44Fcr6rERaN03fg.
[17] http://www.childfocus.be/clicksafe/clicksafetest/selftest.html.
[18] http://www.childfocus.be/clicksafe/chat/index.html.

- Appli Master F.I.N.D.[19]: application containing online games for young people on the media and privacy. By playing the games they find out how easy it is to discover the identity of, and intimate details about, people who say too much about themselves;
- contact point '*Charlie*'[20]: advertising slots aimed at 10- to 16- year- olds to draw their attention to the Child Focus contact point for safe and responsible use of the internet and to various problems (grooming, sexting, etc.);
- *irrespect* (disrespect) [21]: tool for teachers working with 10- to 14- year- olds. This comprises 10 lessons with animated videos on the theme of privacy on the internet;
- 'Surf Safe' campaign[22]: launched in August 2015 to draw very young children's attention to the contact point;
- The annual report for young people[23] between 12 and 18 was produced in 2015. It explains the work done by Child Focus in a concise and practical format.

For the Flemish Community: 'Now I'm talking about it' (http://kindinnood.be/nupraatikerover). If a child has questions concerning sexual abuse (What should you do if someone behaves inappropriately towards you? Is someone making you do things you don't want to do? Do you know someone this is happening to?), he can chat anonymously with a specialist worker at Vertrouwenscentra Kindermishandeling in Brussels.

For the Wallonia-Brussels Federation: maintentenantjenparle is run by Child Focus.

[19] http://www.childfocus.be/clicksafe/F.I.N.D/.
[20] https://www.youtube.com/watch?v=8B859LFJXUA.
[21] http://www.childfocus.be/sites/default/files/irespect_0.pdf.
[22] http://www.childfocus.be/fr/nouvelle/surf-safe-avec-child-focus.
[23] http://www.childfocus.be/sites/default/files/rapport_annuel_jeunes_2014.pdf.

In July 2015 the www.ecops.be website, which had enabled citizens to report to the authorities (federal police) any criminal offence linked to use of the internet (not only child pornography, but also robberies, illegal commercial practices, etc.), was limited to reports of child pornography images, owing to inadequate resources for handling the messages sent by citizens. The homepage has, however, been kept and provides links to Child Focus and other authorities. The web page and links help keep people informed and enable them to report suspicious websites.

6.2.4 Stakeholders active in combating websites containing or disseminating child pornography and measures taken

Belgium is able to block websites pursuant to section 3 of Article 39*bis* of the CIC. The problem does not arise for sites hosted in Belgium as the police can conduct a search and confiscate data. Since it cannot 'seize' digital data physically, the police are allowed to copy this data and make it inaccessible.

We would point out, however, that the police do not decide independently whether or not to block a website, since that is the task of the public prosecution service and/or the examining magistrate, who decides on a case-by-case basis.

At central level, the federal police have a four-person unit tasked with:

- managing the ICSE database;
- analysing seized material (assisting federal and local research units);
- processing of information; passing on police reports, where necessary, in order to identify suspects and/or victims;
- identification of victims, where necessary, based on images received via Interpol or else directly from police forces affiliated to Europol or Interpol;
- participating in Europol and Interpol experts' groups;
- representing the federal police in EMPACT Cybercrime/CSE;
- handling complaints.

6.3 Online payment card fraud

Online payment card fraud is not tackled at national level and cases are handled by the federal police responsible at district level.

Citizens and private companies almost always report payment card fraud to the (local) police because banks require a copy of the report/declaration made to the police in order to refund the amount involved in the fraud.

The federal police's FCCU is involved in the working group on 'Internet banking security', which focuses on weaknesses and threats concerning online bank fraud. As part of plans to improve the federal police, it was decided that there should be no national follow-up on other forms of payment card fraud; these cases are dealt with by the federal police services in the judicial district, which also have good contacts with the industry, but more on a case-by-case basis.

6.4 Conclusions

Combating cybercrime is a matter not just for the law enforcement bodies since the private security sector also contributes on awareness-raising and prevention.
Belgium has established a CERT to centralise information on cyber attacks.

The CCB has overall responsibility for the bodies involved in combating cyber incidents (FCCU, RCCU, CERT, SGRS). It is also important to have a platform for discussion and channelling of information.

Belgium is equipped to fight child pornography; the first steps in locating offences are taken centrally by the child abuse section of the DJSOC, after which the file is forwarded to the competent local services.

To ensure an effective fight against child pornography the internal operations of the police force need to be improved through strengthening both human and financial resources. Police officers also need to receive continuing training aimed at upgrading their skills, broadening their knowledge and promoting the sharing of experience.

Combating paedophilia comes under the remit of local units, supported by their regional counterparts since the child abuse section of the DJSOC is in charge, for instance, of handling the transmission of online paedophile images though it subsequently hands over the investigation to the competent local services.

The Public Prosecution Service is also involved and assigns a coordination role to the Liège principal public prosecutor.

A central unit is in charge of analysing paedophile images on the internet. Where an offence is observed, the report is sent to the public prosecutor's office, which transfers the case to the local police for investigation. Urgent cases, however, are often handled by the child abuse section of the DJSOC.

There are plans to purchase specialised software for detecting paedophile images. However, there is currently a shortage of equipment and of trained staff in the central units.

The evaluation team welcomes Belgium's initiatives on working with the private sector on prevention campaigns. It should also be stressed that there are many campaigns aimed at young people that focus on preventing, and raising awareness of sex tourism.

Another positive aspect is the establishment of the legislation needed to block access to websites with child pornography content.

The evaluation team is taking a keen interest in the draft law on strengthening the role of Child Focus in combating child pornography.

With regard to online payment card fraud, the evaluation team noted a lack of information concerning the results of investigations carried out by the local police.

7. INTERNATIONAL COOPERATION

7.1 Cooperation with EU agencies

7.1.1 Formal requirements for cooperation with Europol/EC3, Eurojust, ENISA

There are no specific procedures for cooperation on cybercrime matters.

7.1.2 Evaluation of the cooperation with Europol/EC3, Eurojust, ENISA

The cooperation is working well.

Cooperation takes place mainly through the involvement of Europol/EC3 in joint operations. The 2014 iOCTA consolidated the structural approach within the federal police.

The 'cyber bit' notes drafted and circulated by Europol/EC3 are useful, but it is still necessary to translate them into Belgium's official languages in order for them to be as useful as possible amongst the local police forces.

Operation Mozart

In August 2010 a Belgian bank was informed by several customers that their online banking sessions had been infected with malware. Hackers had attempted to make international transfers to bank accounts in Spain and Portugal. A complaint was lodged with the public prosecutor's office in Brussels.

Subsequently, five other Belgian banks were also hit by similar viruses and lodged complaints with the public prosecutor's office in Brussels in 2011. The investigation was handled by the federal police's central services.

The public prosecutor's office organised the legal action at national level, and brought the case before Brussels examining magistrate Michel Claise on 7 December 2011, citing the offences of computer forgery, computer fraud, hacking and money laundering committed by criminal organisations.

Initially, the hackers collect confidential data from online banking users whose computers have been infected with a virus. The perpetrators can then use the collected data to fraudulently open an online banking session without the customer knowing, and transfer money from the victim's account to their accomplices' bank accounts.

In the second stage, the 'money mule' accomplices (recruited by the criminal organisation by email) receive instructions on how to recover this money and transfer it to accounts held by third parties in other countries ('second-tier mules').

The police work coordinated by the Belgian federal police led to the arrest of 57 first-tier mules on Belgian soil. In separate cases, two convictions for money laundering have already been given, and one mule was given a fine.

Investigators carried out investigations in several countries (Germany, France, Poland, Latvia, Estonia, Ukraine, Russia, etc.).

A large-scale police operation run by Europol led to the arrest of seven suspects in Ukraine. Among these suspects were the two presumed main recruiters of Belgian mules.

Using the expertise gained over the past few years from similar computer fraud cases, the Belgian federal police has set up a new technology team composed of IT investigators specialising in cybercrime (the Federal Computer Crime Unit (FCCU)) working alongside the financial investigators experienced in money laundering techniques (OCEDEFO).

On 7 March 2013 five European countries (Austria, Belgium, UK, Finland and Norway), later joined by the Netherlands and with support from Eurojust and Europol, signed a memorandum of understanding on the creation of an international team of magistrates and police officers working to identify the organisations behind the hacking of European banks.

As regards cooperation with Europol/EC3, the approach is strongly influenced by a common law culture in which the role of the public prosecution service does not reflect reality in cases with repercussions for Belgium. Cooperation with Eurojust is working well.

7.1.3 Operational results of the JITs and cyber patrols

Belgium has already participated in JITs in the fight against cybercrime. This has proved to be a positive experience. Belgium has applied for EU funding under the national envelope of the internal security fund (ISF), for IT projects on forensics for the police and the 'Union Action' joint initiative with France. These applications are currently awaiting approval by the European Commission.
Belgium has no experience of participation in cyber patrols.

Belgium suggests that JITs be put into action more quickly, and considers that EU funding must continue. Belgium regrets that there is no EU funding for translation, despite it often being essential for good cooperation.

7.2 Cooperation between the Belgian authorities and INTERPOL

The federal judicial police has had links with the ISCE since 2011. Access is managed by a specialised department of the DJSOC. Specialist training has been organised in cooperation with INTERPOL.

7.3 Cooperation with third countries

Belgian experts put their know-how at the disposal of TAIEX: Belgian experts are made available to TAIEX for training or in order to increase expertise.

The same is true for the Council of Europe, where Belgian experts are involved in CoE projects, mainly those relating to the Balkans.

Regarding cooperation at European level, Belgium is part of the Global Alliance against Child Sexual Abuse Online, which was launched on 5 December 2012 and currently has 53 member countries. This initiative aims to bring together global decision makers in order to better identify and help victims, and to prosecute those who commit this abuse. Belgium has also been connected to the ECRIS (European Criminal Records Information System) since 2 July 2012.

Eurojust involvement has certainly brought added value to certain cases relating to third countries, but in our view Europol/EC3 has not yet provided any added value.

7.4 Cooperation with the private sector

There is ongoing cooperation with the private sector. Various initiatives have been launched, the most important being the following:

- cooperation with universities, which started with the creation of the B-CCENTRE centre of excellence, which is unfortunately no longer active;
- cooperation with the Federation of Belgian Enterprises;
- participation in international training initiatives (ECTEG);
- cooperation with the various cybersecurity companies;
- cooperation with the financial sector following attacks on online banking systems.

7.5 Instruments of international cooperation

7.5.1. Mutual legal assistance

There are no specific procedures for cooperation on cybercrime matters. The Code of Criminal Procedure provisions on mutual assistance in criminal matters apply.
Ordinary law procedure applies to the communication of requests for mutual legal assistance.

The Budapest Convention on Cybercrime includes in Chapter III, Section 1, Title 3 provisions covering mutual legal assistance within the framework of the Council of Europe relating specifically to IT offences in the broad sense, as defined in the Convention. The Convention provides for an urgent procedure and several grounds for refusal to cooperate.

There is no specific legal basis for mutual legal assistance on cybercrime matters. Article 3 of the Belgian Law of 9 December 2004 on international legal assistance in criminal matters amending Article 90b of the Code of Criminal Procedure (Official Journal of 24 December 2004) provides that the Belgian judicial authorities should grant the maximum degree of mutual legal assistance in accordance with that law and the applicable rules of international law.

We can refer to the rules of ordinary law on this matter. In principle, there are three possibilities, depending on the legal basis:

- the traditional approach, by which the requests sent by the requesting Member State are transferred to the Member State to which they are addressed, with the Federal Public Service Justice acting as intermediary;
- cooperation within the Schengen area and the Convention of 29 May 2000 within the European Union, which provides for direct contact between judicial authorities (although each Member State maintains its jurisdiction). These requests are communicated directly between the judicial authorities with territorial jurisdiction for issuing and executing them;
- cooperation according to the principle of mutual recognition within the European Union, which means that decisions issued in one Member State of the European Union are executed and recognised in another Member State as though they were decisions taken by that State's own national authorities.

In accordance with the Law of 9 December 2004, a distinction must be made between Member States of the EU and third countries.

Article 5 - The execution in Belgium of requests for mutual legal assistance in criminal matters communicated by a competent authority of a Member State of the European Union shall not require prior authorisation from the Ministry of Justice.

Nevertheless, if the execution of a request for mutual assistance from a foreign authority referred to in the first paragraph is likely to be refused on one of the grounds referred to in the first subsection, or subsection 1 or 2 of Article 4(2), the judicial authority which receives the request forwards it to the Justice Ministry. If the request was addressed to a public prosecutor or examining magistrate, it is forwarded to the Justice Ministry via the Prosecutor-General.

If necessary, the Justice Ministry informs the requesting authority that it cannot proceed with some or all of its request. The judicial authority concerned is informed of this, and ensures that the request for assistance is not executed nor case papers returned.

Article 7. *'1. Requests for mutual legal assistance in criminal matters issued by Belgian judicial authorities and addressed to foreign competent authorities shall be sent via the Justice Federal Public Service using diplomatic channels. Case papers shall be returned through the same channels.*

Requests for mutual legal assistance in criminal matters issued by foreign competent authorities and addressed to Belgian judicial authorities shall be sent through diplomatic channels.

Case papers shall be returned through the same channels.

(2) However, if provided for by an international instrument binding the requesting country and Belgium, the sending of requests for mutual legal assistance in criminal matters and return of case papers shall take place either directly between the Belgian judicial authorities and foreign authorities competent to issue and execute them, or between the justice departments concerned.

(3) A copy of any request for mutual legal assistance sent or received by a Belgian judicial authority shall be sent to the Federal Public Service Justice.

(4) If the request for mutual legal assistance in criminal matters sent or received by a Belgian judicial authority relates to a case liable to seriously disturb public order or undermine Belgium's vital interests, a report shall be sent immediately to the Ministry of Justice by the federal prosecutor or, if an examining magistrate or public prosecutor is in charge of the request, via the Prosecutor-General.
This requirement is without prejudice to the application of Article 5.

The central authority for international cooperation in criminal matters only has statistics and information available on requests for international legal assistance involving countries outside the EU. Since 2004, requests for international legal assistance in criminal matters involving EU Member States have been communicated directly between the judicial authorities without the involvement of the Justice Ministry. The principle is that we are sent a copy of these requests for mutual legal assistance. The only record kept of these copies is a list of offences, with no other details. We do not have any other information on developments in the cases concerned.

The table below shows the statistics with regard to cybercrime and child pornography, in relation to EU Member States.

(Only these two offences are recorded):

Year	Offence	From Belgium	To Belgium
2015	Cyber crime	23	38
	Child pornography	1	3
2014	Cyber crime	61	39
	Child pornography	2	7

The table below shows the statistics with regard to cybercrime and child pornography, in relation to third countries.
(Only these two offences are recorded):

Year	Offence	From Belgium	To Belgium
2015	Cyber crime	8	3
	Child pornography	2	1
2014	Cyber crime	21	3
	Child pornography	0	1

There are no specific procedures to follow or conditions to fulfil. The only thing to note is that requests for legal assistance involving the USA can now only be sent by email.

In principle, requests for legal assistance must be sent in their original format. In extremely urgent cases, a copy may be provided to the central authority, provided that the original follows. The average response time is six months.

7.5.2 Instruments of mutual recognition

The following should be noted with regard to instruments of mutual recognition:

- European protection decision: this directive has not yet been implemented. A draft law has already been prepared and will be submitted to Parliament later this year;
- mutual recognition of control measures: no known cases in 2014 or 2015;
- mutual recognition of prison sentences and detention orders: two known cases in 2014. One case related to child pornography and the other to cybercrime;
- recognition and execution of confiscation decisions: these cases are not recorded separately;
- mutual recognition of financial penalties: two known cases in 2014, both related to child pornography; execution of decisions to freeze assets or data: these cases are not recorded separately.

7.5.3 Surrender/Extradition

(a) Pursuant to Article 3 of the Law of 19 December 2003 on the European arrest warrant[24], a European arrest warrant may be issued for acts punishable under the issuing Member State's law by a custodial sentence or a detention order of a maximum of at least 12 months or, when a sentence has been passed or a detention order imposed, if the duration of these measures is at least four months.

Regarding the execution of a European arrest warrant issued by another Member State, Article 5 of the same law provides that in principle execution is refused if the act on which the warrant is based does not constitute an offence under Belgian law. However, this rule does not apply if the act constitutes one of the following offences, as long as it is punishable in the issuing Member State by a custodial sentence of a maximum of at least three years, including for cybercrime:

(b) Under Article 1 of the Law of 15 March 1874 on extraditions[25], in the implementation of treaties agreed with foreign countries on a reciprocal basis, the government may allow the extradition of any foreign national who is being prosecuted for breaking criminal law, as the perpetrator, co-perpetrator or accomplice, or is sought so that the judicial authorities of the foreign country can enforce a sentence or detention order.

Within the meaning of this law, detention order refers to any custodial measure imposed by a criminal court in addition to or instead of a sentence.

[24] Belgian Official Gazette, 22 December 2003.
[25] Belgian Official Gazette, 17 March 1874.

However, only acts punishable under Belgian law and under the law of the foreign country by a custodial sentence of a maximum duration of more than one year can be grounds for extradition. When the extradition is requested in order for a sentence to be enforced, the duration of the sentence must be at least one year's imprisonment. When the extradition relates to the enforcement of a detention order, the detention must be for an indeterminate period or for at least four months. If the offence for which the extradition is requested is punishable in the requesting country by the death penalty, the government does not grant the extradition unless the requesting country gives formal assurances that the death penalty will not be imposed.

If the extradition request covers a number of different offences each of which is punishable by a sentence of imprisonment, under Belgian law and the law of the other state, but some of which do not fulfil the condition concerning the severity of the sentence, extradition may also be granted for these offences even if they have only been punished by fines.

Under Article 2 of the law of 19 December 2003 on the European arrest warrant[26], the arrest and surrender are carried out on the basis of a European arrest warrant. The European arrest warrant is a judicial decision issued by the competent judicial authority of a Member State of the European Union - the 'issuing judicial authority' - with a view to the arrest and surrender by the competent judicial authority of another Member State - the 'executing judicial authority' - of a requested person, for the purposes of conducting a criminal prosecution or enforcing a custodial sentence or detention order.

[26] Belgian Official Gazette, 22 December 2003.

As regards communication channels, Articles 9 and 10 of the same law stipulate that an alert issued in accordance with Article 95 of the Convention of 19 June 1990 implementing the Schengen Agreement of 14 June 1985 on the gradual abolition of checks at common borders is equivalent to a European arrest warrant. If the alert does not contain all the information required by the European arrest warrant, the alert must be followed by transmission of the original, or a certified true copy, of that arrest warrant. The requested person may be arrested, on the basis of the alert referred to in Article 9 or on submission of a European arrest warrant.

In accordance with the law on extraditions, the Government may grant extradition on submission of either the original, or a true copy, of: a judgment; an order issued by the pre-trial chamber; an order issued by the indictments chamber; or a criminal procedural document issued by the competent judge, formally ordering, with immediate effect, the referral of the suspect or accused person to the criminal court.

Extradition will also be granted on submission of the arrest warrant, or any other document having equivalent effect, issued by the competent foreign authority, provided that these documents include a precise indication of the offence in respect of which they have been issued and are made enforceable by the pre-trial chamber at the court of first instance which has jurisdiction over the foreign national's place of residence in Belgium or the place where he may be found.

The documents referred to in the first and second paragraph may be submitted by fax in cases where an international convention explicitly so provides, subject to the conditions of authentication laid down in the convention.

The table below shows the statistics with regard to cybercrime and child pornography, in relation to EU Member States.

Year	Offence	From Belgium	To Belgium
2015	Cyber crime	2	1
	Child pornography	/	/
2014	Cyber crime	20	/
	Child pornography	/	/

The table below shows the statistics with regard to cybercrime and child pornography, in relation to third countries.

Year	Offence	From Belgium	To Belgium
2015	Cyber crime	7	3
	Child pornography	/	1
2014	Cyber crime	8	11
	Child pornography	0	1

Procedures or conditions always have to be complied with, both for surrender and for extradition. In this regard, we refer to the law of 19 December 2003 on the European arrest warrant (Belgian Official Gazette, 22 December 2003) and the Law of 15 March 1874 on Extradition (Belgian Official Gazette, 17 March 1874).

With respect to surrender, under Article 10 of the law of 19 December 2003 on the European arrest warrant (Official Gazette, 22 December 2003), arrest is possible once the person requested is the subject of an alert as referred to in Article 9 of the same law.

Article 5 of the law of 15 March 1874 on extradition (Belgian Official Gazette of 17 March 1874) provides that in urgent cases the foreign national may be arrested provisionally in Belgium, for one of the offences referred to in Article 1 of the same law, on presentation of an arrest warrant issued by the examining magistrate with jurisdiction over the foreign national's place of residence or the place where he may be found, and justified by an official notification given to the Belgian authorities by the authorities of the country in which the foreign national has been sentenced or prosecuted. However, in that case, he will be released if, within forty days of his arrest, the arrest warrant issued by the competent foreign authority has not been served on him.

After the arrest has been ordered, the examining magistrate is authorised to proceed following the rules laid down in Articles 87 to 90 of the Code of Criminal Procedure. The foreign national can request provisional release in cases where a Belgian is able to do so, subject to the same conditions. The request will be submitted to the pre-trial chamber. The pre-trial chamber will also decide, after hearing the foreign national, whether or not all or part of the documents and other objects seized should be sent to the foreign government which is requesting extradition. It will order documents and other objects not directly linked to the offence with which the suspect is charged to be returned and, if applicable, will rule on claims by third-party holders or rights-holders.

7.6 Conclusions

Belgium did not report any major difficulties with regard to international cooperation. Participation in joint investigation teams is assessed positively. They have no experience of cyber patrols.

The national authorities cooperate closely with Europol/EC3. Belgium is closely involved in the operation of the European system.

A specialised police unit has been set up to work with the ICSE database.
The national authorities did not provide any information concerning cooperation with third countries.

Cooperation with the private sector, and especially with universities and the Federation of Belgian Enterprises, is assessed positively.

However, the slowness of international judicial assistance procedures (6 months, on average) was criticised by the police authorities. This situation could be significantly improved, especially at European level, by simplified procedures for key information, such as IP addresses.

8 TRAINING, AWARENESS-RAISING AND PREVENTION

8.1 Specific training

The Belgian legal training institute - *Institut de formation judiciaire/(IFJ)/Instituut voor Gerechtelijke Opleiding (IGO)*[27] - offers various modules/courses on cybercrime:

A ***basic course on cybercrime*** which aims to raise awareness of computer crime (in the strict sense and in the broad sense) among the judges. Firstly, it equips participants with the technical knowledge required to understand the legal provisions on computer crime and the options available when carrying out investigations on computer systems. Secondly, it gives them a clear picture of the options and the legal restrictions when combating computer crime, so that they can apply them effectively in practice.

The course is intended for:

- judges who regularly come into contact with certain aspects of cyber research;
- appeal court and first-instance court judges hearing criminal cases, as well as investigating judges and public prosecutors;
- second-year judicial trainees, for whom the course is obligatory;
- prosecution service lawyers;
- public prosecutors appointed recently (since 1 January 2014) as a result of passing the professional competence examination or an oral assessment examination, for whom participation is obligatory as part of their initial training.

[27] http://www.igo-ifj.be/fr

- Since 2015, the IFJ/IGO has developed a ***specialised cybercrime course*** intended particularly for judges, judicial trainees and prosecution service lawyers who have already passed the ***basic cybercrime course***, as well as federal judges. The 2-day specialised course builds on the basic knowledge acquired in the initial cybercrime course. It enables participants to gain in-depth expertise in the use of social media in proactive and reactive criminal investigations, on special investigation methods in a virtual environment, international cooperation in criminal matters (particularly with the USA), especially as regards digital traces and evidence, and on territorial powers and jurisdictions in cyberspace.

- A half-day specialised ***course on international cooperation with the United States to obtain communication data from American suppliers*** has also been run for judges (federal judges or judges specialising in terrorism), judicial trainees and legal experts from the public prosecutors' offices since 2015. It takes the form of a round table focusing on obtaining international judicial assistance from the USA and American service providers; obtaining data (content, traffic data, subscriber details) from online communication services based in the USA (WhatsApp, Skype, Facebook, Google, YouTube, Yahoo, etc.) and an open discussion of particular dossiers, together with specialists from the US Department of Justice.

Various training courses are also run for the police:

- 'First responder' training for local police forces is being developed in the form of online learning, which will result in a reference guide being made available for identifying and seizing objects which may contain digital traces and for interviewing victims of non-specific crime committed using new technologies.
- The training for investigators from the local and federal police forces includes 12 hours on new forms of crime and the options available for conducting investigations.
- The specialised investigators of the RCCUs and the FCCU follow a 120-hour course of training, of which 90 hours are devoted to computer forensics and 30 hours to the legal framework and international cooperation. After this basic course, which is normally run each year, they follow intermediate and advanced courses, run in-house or as part of projects financed by EU subsidies (OLAF, ECTEG pilot courses, etc.). There is no budget line specifically allocated to cyber training, and the existing courses which require a financial contribution are run as budget resources are made available, on a case-by-case basis, with a focus on training the trainers.

Courses on IT security auditing, including how to respond in the event of an incident, are also offered by institutions such as the Solvay Brussels School, and ICHEC as well as various tertiary-level training institutions such as HOWEST and ESI, and universities such as Namur (FUNDP), Leuven (KU Leuven) and Gent.

At present, certification is not required for judicial experts - they need only be designated as such by a judge.

The FCCU coordinates training courses and organises them based on the needs expressed by practitioners and taking account of the expertise indicated by partner institutions in the university sector, Europol, Interpol and counterparts in the EU, for instance within the ECTEG.

The basic computer forensics and cyber courses are based on the materials available from the ECTEG; some members of the FCCU/RCCUs also contribute to updates as experts.

The basic course run by EC3/Europol provides a basic training which complements the existing courses and is an excellent opportunity for networking among practitioners.

When places are available on courses run in Belgium by the FCCU, in-house or in collaboration with the B-CCENTRE, they are opened up to third countries, taking account of the language of the course and its subject.

For the federal police, the main cost is the employment of specialised staff who contribute to the design and distribution of the courses. There is no specific budgetary allocation, in the federal judicial police, for training run by external cybercrime specialists. The average annual cost is EUR 22 000. In 2015, a specific 'one- shot' budget for counter-terrorism was partially devoted to training, especially in forensic analysis of mobile devices (smartphones, tablets), with EUR 20 000 spent on training 4 persons responsible for rolling out this training nationally.

Training courses were run by the Belgian centre of excellence, the B-CCENTRE, for specialised investigators in the RCCUs and the FCCU.

When the EU-funded B-CCENTRE project ended, the partnership could not be continued for lack of any structural national funding, for instance from the ISF fund.

There is a variety of training provision available in the university sector, in the form of years of specialisation in cybersecurity, incorporated into bachelor's degree and master's degree courses.

In these courses, lecturers from the FCCU teach the key points of how to respond in the event of an incident and preserve digital traces.

8.2 Awareness-raising

A number of initiatives, by both state and private-sector bodies, aim to raise awareness of the problem of cybercrime.

8.3 Prevention

Although a number of initiatives exist, contacts stressed that the resources are not sufficient to provide an appropriate response to the phenomenon of cybercrime. To avoid overlap between the different players, prevention should be centrally organised - a task which could be entrusted to the new CCB.

8.3.1 National legislation/policy and other measures

CERT.be has an important role to play in prevention. As an expert on Internet and network security, CERT.be aims to help companies and other organisations to coordinate on, resolve and prevent security problems. It must however be noted that the focus of the CERT's specific interventions in the event of cyber incidents is on critical infrastructures. There is thus very limited help to enterprises and it is provided only if the resources are available.

The low level of awareness among end users increases the risks. Staff regularly compromise the security of IT systems without realising, for instance by working on an unprotected device, by sharing a password in good faith, by re-using weak passwords or by clicking on a link in a phishing email. Users who work without antivirus software, or with an out-of-date version of it, can also cause problems for the company. For that reason, CERT.be also focuses on individual users, for whom it runs awareness-raising campaigns.

The malware used by criminals is becoming more and more difficult to neutralise; in some cases, it even includes its own defence mechanism. CERT.be automatically collects information on threats and incidents via sensors, honeypots and other systems. CERT'S pro-active services aim at preventing cyber incidents and limiting their impact when they do occur. In the medium and long term, CERT is seeking to improve the protection of IT infrastructure by:

- publishing information and advice on protection;
- monitoring and evaluating trends and technologies;
- raising awareness among IT specialists and system users;
- sharing knowledge and information;
- organising conferences and specialist workshops.

Most recently, in October 2015, an awareness-raising campaign, resulting from collaboration between CERT and the cyber-security coalition, was launched in Belgium to promote the use of sentences, rather than words, as a password (see www.safeonweb.be). The cyber-security coalition also aims at awareness raising.

8.3.2 Public/private partnership (PPP)

In 2014, on the initiative of private-sector actors (the traditional telecommunications operator, audit firms, etc.) and partners in the university and government sector (B-CCENTRE, CERT, FCCU, etc.), the establishment of the Cyber Security Coalition initiated projects on awareness-raising, good practice and training (for managers).

Cooperation with Child Focus is currently under discussion. The parties around the table (the Ministry of Justice, the judicial authorities and the police) are currently examining how to develop the role of Child Focus, without going beyond the private sector's area of activity.

8.4 Conclusions

The evaluation team noted, with regard to the police, that some police areas are also establishing their own "Local CCU", either by poaching members of the RCCU, or by having this role filled by volunteers who have practical skills.

In the absence of any specific training, the staff who fulfil this role carry out analyses without complying with good practice, which can undermine the validity of the evidence in court. The evaluation team suggests that training should be centralised and coordinated by the FCCU.

The training offered by private companies is very expensive and unaffordable with the external training budget of EUR 3 000 per year available for the FCCU and all the RCCUs.

As regards prevention and awareness raising, the resources employed are not sufficient to permit an adequate response.

Specialised training for judges started in 2004 and became obligatory, but only for newly-appointed judges, from 2013.

In 2015, 55 judges took the course on cybercrime and 33 judges followed the course on cooperation with the United States. The main problem, however, continues to be the lack of training for judges recruited before 2013, partly because of a certain reluctance on the part of judges to devote time to training (it was stated that judges cannot leave the courts for two or three days to go to the legal training institute (IFJ/IGO) in Brussels).

In 2015, a new cybercrime course was designed (which is very well-structured, over two days) and a new course on cooperation with the United States.

It should be suggested to Belgium that it reinforce training for judges on cybercrime.

9 FINAL REMARKS AND RECOMMENDATIONS

9.1 Suggestions by Belgium

- An EU-level reference model should be drawn up, with standards for the structure and operation of cybercrime investigation units; laying down minimum standards would improve operations at national level and make it easier to involve the relevant bodies when there is an international dimension to a phenomenon.

- Standards should be made available, such as the Council of Europe's Electronic Evidence Guide, combined with the EVIDENCE project, to support efforts to improve the quality of evidence collection and management.

- If all countries used a common classification (ENISA project), combined with a similar statistical tool, it would be possible to gain a better overview of how phenomena were developing in real time and thus provide policy makers with a useful assessment criterion.

- The guidelines for ISF fund allocation no longer cover tasks previously supported by EU funds. These tasks are still necessary, especially as regards the creation and operation of public/private partnerships with industry, but also with academia. The importance of these partnerships for awareness, training and R&D is widely recognised.

- An approach whereby analytical bodies were subject to certification, covering both procedures and practitioners, and based on validation of the software tools used, would improve the quality of forensic evidence in the field of new technologies. In the absence of global standards, laying down standards at European level would simplify judicial cooperation on cases with an international dimension and make it easier for practitioners to share knowledge and methodologies.

9.2 Recommendations

Belgium should conduct a follow-up on the recommendations given in this report 18 months after the evaluation and report on progress to the Working Party on General Affairs including Evaluation (GENVAL).

The evaluation team saw fit to make a number of suggestions to the Belgian authorities. It also put forward recommendations to the EU, its institutions and agencies, particularly Europol, based on various examples of good practice.

9.2.1 Recommendations to Belgium

Belgium should:

1. continue efforts to unify the system for gathering statistics and have everyone use a common classification;

2. finalise establishment of the CCB by appropriate staff recruitment, and give the body a greater role in coordinating cyber security;

3. increase the budget earmarked for anti-cybercrime bodies (human resources, equipment and training);

4. further clarify the responsibilities of the various police bodies with an anti-cybercrime remit;

5. tighten up legislative and procedural rules on open-source investigations;

6. increase cybercrime training for judges.

9.2.2 Recommendations to the European Union and its institutions and to other Member States

At EU level, the evaluation team thinks it would be useful to consider:

- simplifying procedures for mutual legal assistance between Member States to make information sharing quicker and easier;

- put forward a new draft directive on data storage;

- standardise procedural rules on digital evidence and develop immediate mutual recognition;

- adopt rules requiring undertakings to communicate data to the judicial authorities if they provide services in Europe (Yahoo doctrine).

The Member States should carefully study the good practice identified in Belgium, viz:

1. specialisation within the prosecution service through the creation of an expert network for cybercrime coordinated by the Antwerp principal public prosecutor's office;

2. the structure and quality of the cybercrime training provided by the Belgian legal training institute;

3. the activities of civil society (Child Focus) in the field of prevention and its involvement in combating paedophilia.

ANNEX A: PROGRAMME FOR ON-SITE VISITS

Seventh round of mutual evaluations of the GENVAL of the Council of the European Union

The practical implementation and operation of European policies on prevention and combating cybercrime

Programme for on-site visits in Belgium from 26 to 28 April 2016

Monday 25 April 2016

Arrival

Tuesday 26 April 2016

9.30:

Visit to the

FPS Justice (*Boulevard de Waterloo 115, 1000 Brussels)*

Subjects: welcoming address, legislative framework, political priorities, roles of the various bodies in combating cybercrime

Participants:

- Representatives of the FPS Justice
- Representatives of the Justice Minister's strategy unit
- Examining magistrate
- Federal public prosecutor's office
- Principal public prosecutor's office
- Federal police
- Belgian centre for cybersecurity (CCB)

12.30: Lunch

14.00-17.00:

Visit to the federal public prosecutor's office (*Rue aux Laines 66, 1000 Brussels)*

Subjects: Operation of the prosecution service in the context of combating cybercrime (including cyber attacks, on-line sexual abuse/pornography involving children, and cyber fraud involving credit cards)

Participants:

- Expert network of the College of Principal Public Prosecutors
- Federal public prosecutor's office
- Examining magistrate

Wednesday 27 April 2016

9.00: Visit to the federal police (RAC building, Rue Royale 202A, 1000 Brussels)

Subject: combating cybercrime

Participants:

- FGP [Federal CID] Antwerp RCCU
- FCCU

12.00: Lunch

13.00-17.00: Subjects: on-line sexual abuse/pornography involving children, internet searches and cyber security

Participants:

- Federal police;
- Belgian centre for cybersecurity (CCB)
- CERT
- CYBER SECURITY COALITION

Thursday 28 April 2016

9.30: Visit to the legal training institute (*Avenue Louise 54, 1000 Brussels)*

Subject: training

Participants:

- Federal public prosecutor's office
- Examining magistrate
- Federal police
- Legal training institute

12.30: Lunch

13.30-16.00: Subject: Europol/Eurojust relations

Subject: General discussion, question and answer session

ANNEX B: PERSONS INTERVIEWED/MET

Persons interviewed/met	Organisation
Daniel Flore	Director-general of the Department of Legislation, Fundamental Rights and Freedoms, Justice FPS
Stéphanie Bosly	Head of department of European criminal law, Justice FPS
Frederik Decruyenaere	Head of department of individual offences and procedures, Justice FPS
Claire Huberts	Attaché at department of principles of criminal law and criminal procedure, Justice FPS
Nathalie Cloosen	Attaché at department of European criminal law, Justice FPS
Serge De Biolley	Representatives of the Justice Minister's strategy unit
Geert Schoorens	Federal public prosecutor's office
Dirk Schoeters	Antwerp public prosecutor's office
Yves Vandermeer	Federal police

Wednesday 27 April 2016 – Visit to federal police

Persons interviewed/met	Organisation
Johan Van Den Berghe	Antwerp federal police – RCCU
Walter Coenraets	Federal police – DJSOC/FCCU
Yves Vandermeer	Federal police – DJSOC/FCCU
Marjolein Delplace	Federal police – DJSOC/Strategy & PNS
Christine Casteels	Federal police – DJSOC/Strategy & PNS
Yves Goethals	Federal police – DJSOC/Child abuse
Elrik Robbe	Federal police – DJSOC/Internet research
Didier Louis	Brussels federal police – DJSOC/Child abuse
Vanessa Hubert	Local police - Montgomery police zone - child abuse
Peter Gouwy	Europol
Phédra Clouner	Cyber Security Centre Belgium
Geert Schoorens	Federal public prosecutor's office
Nathalie Dewancker	Cyber Security Coalition
Nathalie Cloosen	Justice FPS

Thursday 28 April 2016 – Visit to legal training institute

Persons interviewed/met	Organisation
Jan Kerkhofs	Federal public prosecutor's office
Philippe Van Linthout	Malines examining magistrate
Dirk Schoeter	Antwerp public prosecutor's office
Jos De Vos	Legal training institute
Meta Lubambu	Legal training institute
Yves Vandermeer	Federal police
Nathalie Cloosen	Justice FPS

ANNEX C: LIST OF ABBREVIATIONS/GLOSSARY OF TERMS USED

LIST OF ACRONYMS, ABBREVIATIONS AND TERMS	FRENCH OR ACRONYM IN ORIGINAL LANGUAGE	FRENCH OR ACRONYM IN ORIGINAL LANGUAGE	ENGLISH
B-CCENTRE		Consultation platform on computer network security	Belgian Cybercrime Centre of Excellence for Training, Research & Education BelNIS
CCB	Belgian centre for cybersecurity (CCB)		
CCU			Computer Crime Unit
CERT			Federal Cyber Emergency Team
CIC	Code of Criminal Procedure:		
DJSOC	Federal judicial police - directorate for the fight against serious and organised crime		
JIT	Joint Investigation Teams		
FEB	Belgian federation of enterprises		
FEDICT	Federal Public Service for Information and Communication Technology		
FCCU			Federal Computer Crime Unit

LIST OF ACRONYMS, ABBREVIATIONS AND TERMS	FRENCH OR ACRONYM IN ORIGINAL LANGUAGE	FRENCH OR ACRONYM IN ORIGINAL LANGUAGE	ENGLISH
IBPT	Belgian institute of postal and telecommunications services		
IFJ	Legal training institute		
LCCU			Local Computer Crime Unit
RCCU	Regional CCU		
SGRS	General Intelligence and Security Service		
SPF	Federal Public Service		

ANNEX D: RELEVANT LEGISLATION

Article 550bis of the Criminal Code: '1. Anyone who, knowing that they are not authorised to do so, accesses a computer system or stays on that system, shall be liable to imprisonment for a term of between three months and one year and to a fine of between EUR 26 and EUR 25 000 or to one of these penalties. If the offence referred to in the first subsection is committed with fraudulent intent, the prison term shall be between six months and two years. 2. Anyone who, with fraudulent intent or intent to cause damage, exceeds their authority to access a computer system, shall be liable to imprisonment for a term of between six months and two years and to a fine of between EUR 26 and EUR 25 000 or to one of these penalties. 3. Anyone in one of the situations referred to in sections 1 and 2 who either: 1° accesses data stored, processed or transmitted by the computer system; or 2° uses a computer system belonging to a third party in any way whatever or uses the computer system to access the computer system of a third party; or 3° causes any damage, even if unintentionally, to the computer system or to the data stored, processed or transmitted by that system or to the computer system of a third party or to data stored, processed or transmitted by that system; shall be liable to imprisonment for a term of between one and three years and to a fine of between EUR 26 and EUR 50 000 or to one of these penalties. 4. An attempt to commit one of the offences referred to in sections 1 and 2 shall be liable to the same penalties. 5. (Anyone who, without authorisation, possesses, produces, sells, obtains with a view to using, imports, disseminates or makes available in any other form any device whatever, including computer data, principally designed or adapted to allow commission of the offences referred to in sections 1 to 4, shall be liable to imprisonment for a term of between six months and three years and to a fine of between EUR 26 and EUR 100 000 or to one of these penalties.). 6. Anyone who orders or incites the commission of one of the offences referred to in sections 1 to 5 shall be liable to imprisonment for a term of between six months and five years and to a fine of between EUR 100 and EUR

200 000 or to one of these penalties. 7. Anyone who, knowing that data have been obtained by commission of one of the offences referred to in sections 1 to 3, holds, reveals to another person or discloses or makes any use whatsoever of data so obtained, shall be liable to imprisonment for a term of between six months and three years and to a fine of between EUR 26 and EUR 100 000 or to one of these penalties. 8. The penalties provided for in sections 1 to 7 shall be doubled if any of these provisions is breached within five years of a conviction for one of these offences or for one of the offences referred to in Articles 210bis, 259bis, 314bis, 504quater or 550ter'.

Article 550ter of the Criminal Code: 1. (Anyone who, knowing that they are not authorised to do so, directly or indirectly enters into a computer system, modifies or deletes data, or modifies the normal use of data in a computer system by any technological means, shall be liable to imprisonment for a term of between six months and three years and to a fine of between EUR 26 and EUR 25 000 or to one of these penalties. If the offence referred to in the first subsection is committed with fraudulent intent or with intent to cause damage, the prison term shall be between six months and five years.) . 2. Anyone who, following commission of an offence as defined in section 1, causes damage to data in the computer system concerned or in any other computer system shall be liable to imprisonment for a term of between six months and five years and to a fine of between EUR 26 and EUR 75 000 or to one of these penalties. 3. Anyone who, following commission of an offence as defined in section 1, partially or completely prevents the computer system concerned or any other computer system from working properly shall be liable to imprisonment for a term of between one and five years and to a fine of between EUR 26 and EUR 100 000 or to one of these penalties. 4. (Anyone who, without authorisation, possesses, produces, sells, obtains with a view to using, imports, disseminates or makes available in any other form any device,

including computer data, principally designed or adapted to allow commission of the offences referred to in sections 1 to 3, although they know that these data can be used to cause damage to data or to partially or completely prevent a computer system from working properly, shall be liable to imprisonment for a term of between six months and three years and to a fine of between EUR 26 and EUR 100 000 or to one of these penalties.). 5. The penalties provided for in sections 1 to 4 shall be doubled if any of these provisions is breached within five years of a conviction for one of these offences or for one of the offences referred to in Articles 210bis, 259bis, 314bis, 504quater or 550ter. (6. An attempt to commit one of the offences referred to in section 1 shall be liable to the same penalties.)'.

Article 550ter of the Criminal Code: '1. (Anyone who, knowing that they are not authorised to do so, directly or indirectly accesses a computer system, changes or deletes data, or changes by any technological means the normal use of data in a computer system shall be liable to imprisonment for a term of between six months and three years and to a fine of between EUR 26 and EUR 25 000 or to one of these penalties.

If the offence referred to in the first subsection is committed with fraudulent intent or with intent to cause damage, the prison term shall be between six months and five years. 2. Anyone who, following commission of an offence as defined in section 1, causes damage to data in the computer system concerned or in any other computer system shall be liable to imprisonment for a term of between six months and five years and to a fine of between EUR 26 and EUR 75 000 or to one of these penalties. 3. Anyone who, following commission of an offence as defined in section 1, partially or completely prevents the computer system concerned or any other computer system from working properly shall be liable to imprisonment for a term of between one and five years and to a fine of between EUR 26 and EUR 100 000 or to one of these penalties.

4. (Anyone who, without authorisation, possesses, produces, sells, obtains with a view to use, imports, disseminates or makes available in any other form any device, including computer data, principally designed or adapted to allow the commission of the offences referred to in sections 1 to 3, although they know that these data can be used to cause damage to data or to partially or completely prevent a computer system from working properly, shall be liable to imprisonment for a term of between six months and three years and to a fine of between EUR 26 and EUR 100 000 or to one of these penalties.). 5. The penalties provided for in sections 1 to 4 shall be doubled if any of these provisions is breached within five years of a conviction for one of these offences or for one of the offences referred to in Articles 210bis, 259bis, 314bis, 504quater or 550ter. (6. An attempt to commit one of the offences referred to in section 1 shall be liable to the same penalties.)

Article 259bis of the Criminal Code: '1. Any public officer or official holding public authority or law enforcement powers who, in the course of their duties, in cases not provided for by law, or without observing the formalities prescribed by law: 1° either intentionally, with the aid of any device whatever, intercepts or causes to be intercepted, gains knowledge of or causes such knowledge to be gained, records or causes to be recorded, during transmission, private communications or telecommunications in which they are not taking part, without the consent of all of the participants in those communications or telecommunications; 2° or installs a device of any sort or causes such a device to be installed with the intention of committing one of the above offences; 3° or knowingly holds, reveals or discloses to another person the content of private communications or telecommunications which were illegally intercepted or recorded or of which they gained knowledge illegally, or who knowingly uses in any way whatsoever information so obtained, shall be liable to imprisonment for a term of between six months and two years and to a fine of between EUR 500 and EUR 20 000 or to one of these penalties.

2. Any public officer or official holding public authority or law enforcement powers who, in the course of their duties, in cases not provided for by law, or without observing the formalities prescribed by law, uses a legally made recording of private communications or telecommunications with fraudulent intent or intent to cause harm, shall be liable to imprisonment for a term of between six months and three years and to a fine of between EUR 500 and EUR 30 000 or to one of these penalties. [2bis Any public officer or official holding public authority or law enforcement powers who, in the course of their duties, in cases not provided for by law, or without observing the formalities prescribed by law, who, without authorisation, possesses, produces, sells, obtains with a view to using, imports, disseminates or makes available in any other form any device, including computer data, principally designed or adapted to allow commission of the offences referred to in section 1, shall be liable to imprisonment for a term of between six months and two years and to a fine of between EUR 500 and EUR 20 000 or to one of these penalties.] 3. An attempt to commit one of the offences referred to in sections 1 and 2 shall be liable to the same penalties. 4. The penalties [provided for in sections 1 to 3] shall be doubled if any of these provisions is breached within five years of a final conviction for one of these offences or for one of the offences referred to [in Article 314bis (1) to (3)]. 5. [The provisions of section 1(1) and (2) shall not apply to [1 research]1 capturing, intercepting, gaining knowledge of or recording by the General Intelligence and Security Service of the armed forces of any form of communication transmitted from abroad, both for military purposes during missions as described in section 2(1) and (2) of Article 11 of the organic law of 30 November 1998 on the intelligence and security services and for the security and protection of Belgian and allied troops during foreign missions and of Belgian citizens established abroad, as described in section 2(3) and (4) of that same Article 11.]'. '.

Article 314bis of the Criminal Code: '1. Anyone who: 1° either intentionally, with the aid of any device whatever, intercepts or causes to be intercepted, gains knowledge of or causes such knowledge to be gained, records or causes to be recorded, during transmission, private communications or telecommunications in which they are not taking part, without the consent of all of the participants in those communications or telecommunications; 2° or installs a device of any sort or causes such a device to be installed with the intention of committing one of the above offences, shall be liable to imprisonment for a term of between six months and one year and to a fine of between EUR 200 and EUR 10 000 or to one of these penalties.]. 2. Anyone who knowingly holds, reveals or discloses to another person the content of private communications or telecommunications which have been intercepted or recorded illegally, or of which they have illegally gained knowledge, or who knowingly makes any use whatsoever of information so obtained, shall be liable to imprisonment for a term of between six months and two years and to a fine of between EUR 500 and EUR 20 000 or to one of these penalties. Anyone who uses a legally made recording of private communications or telecommunications with fraudulent intent or intent to cause damage shall be liable to the same penalties. (2bis Anyone who, without authorisation, possesses, produces, sells, obtains with a view to using, imports, disseminates or makes available in any other form any device, including computer data, principally designed or adapted to allow commission of the offence referred to in section 1, shall be liable to imprisonment for a term of between six months and one year and to a fine of between EUR 200 and EUR 10 000 or to one of these penalties.] 3. An attempt to commit one of the offences referred to in (sections 1, 2 and 2bis) shall be punished in the same way as the offence itself. 4. The penalties (provided for in sections 1 to 3) shall be doubled if any of these provisions is breached within five years of a final conviction for one of these offences or for one of the offences referred to [in Article 259bis (1) to (3)].'

CHAPTER V. - INDECENT ASSAULT AND RAPE

Article 372 of the Criminal Code: 'Anyone who commits, without the use of violence or threats, an indecent assault against or with the assistance of a child of either sex under the age of 16 years, shall be liable to imprisonment (of between five and 10 years). (Any ascendant or adopter who commits, without the use of violence or threats, an indecent act against or with the assistance of a minor, including a minor who is at least 16 years of age but has not been emancipated by marriage, shall be liable to imprisonment of between 10 and 15 years. (The same penalty shall apply if the offender is the sibling of the minor victim or has a similar status in the family, i.e. any person who habitually or occasionally lives with and has authority over the minor victim.)'

Article 373 of the Criminal Code: 'Anyone who commits, with the use of violence or threats, an indecent assault against anyone of either sex, shall be liable to imprisonment of between six months and five years. If the assault is committed against a minor who is at least 16 years of age, the offender shall be liable to imprisonment (of between five and 10 years). The penalty shall be (imprisonment of) between 10 and 15 years if the minor was under the age of 16 years.'

Article 374 of the Criminal Code: 'An assault shall have been committed as soon as it begins to be carried out.'

Article 375 of the Criminal Code: '(Any act of sexual penetration, regardless of its nature and by whatever means, committed against a person who has not consented to it shall constitute the crime of rape. Consent is not obtained where the act is induced by means of violence, coercion or deception, or is made possible because the victim has a physical or mental disability.) (Anyone who commits the crime of rape shall be liable to imprisonment of between five and 10 years.) (If the crime is committed against a minor who is at least 16 years of age, the offender shall be liable to imprisonment of between 10 and 15 years.) (If the crime is committed against a minor who is at least 14 years of age and under 16 years of age, the offender shall be liable to imprisonment of between 15 and 20 years.) (Any act of sexual penetration, regardless of its nature and by whatever means, committed against a child under the age of 14 shall be considered rape with the use of violence. In such cases, the penalty shall be imprisonment of between 15 and 20 years.) (The penalty shall be imprisonment of between 20 and 30 years if the minor was under the age of 10 years.)'

Article 376 of the Criminal Code: 'If the rape or indecent assault causes the death of the person against whom it was committed, the offender shall be liable (to imprisonment of between 20 and 30 years). (If the rape or indecent assault is preceded or accompanied by the acts referred to in the first paragraph of Article 417ter, or by false imprisonment, the offender shall be liable to imprisonment of between 15 and 20 years.) If the rape or indecent assault is committed either against a person [1 who is particularly vulnerable as result of age, pregnancy, illness or physical or mental disability that is apparent or known to the perpetrator]1, or using a weapon or an object resembling a weapon as a threat, the offender shall be liable to (imprisonment of) between 10 and 15 years.'

Article 377 of the Criminal Code: '[1 The penalties shall be as laid down in paragraphs 2 to 6:
- if the offender is the ascendant or adopter of the victim, a direct descendent of the victim or a direct descendent of the victim's sibling; - if the offender is the sibling of the minor victim or has a similar status in the family, i.e. any person who habitually or occasionally lives with and has authority over the minor victim; - if the offender is in a position of authority over the victim; if the offender has abused the authority or powers afforded by his or her position; if the offender is a doctor, surgeon, midwife or health professional and the child or any other vulnerable person referred to in the third paragraph of Article 376 is under that person's care; - if in the cases of Articles 373, 375 and 376 the offender, whosoever it may be, is assisted in the commission of the crime by one or more people.]1 (In the cases provided for in the first paragraph of Article 372 and the second paragraph of Article 373, the penalty shall be imprisonment of between 10 and 15 years.) (In the case provided for in the first paragraph of Article 373, the minimum period of imprisonment shall be doubled. (In the cases provided for in the third paragraph of Article 373, the fourth paragraph of Article 375 and the third paragraph of Article 376, the penalty shall be imprisonment of at least 12 years;) In the case provided for in the first paragraph of Article 375, the period of imprisonment shall be at least seven years. (In the cases provided for in the fifth and sixth paragraphs of Article 375 and the second paragraph of Article 376, the penalty shall be imprisonment of at least seventeen years.)'

Article 377bis of the Criminal Code: 'In the cases provided for in this chapter, the minimum penalties imposed by these articles may be increased by two years if they concern imprisonment for a major criminal offence and doubled if they concern imprisonment for other offences, where one of the motives of the offence is hatred, contempt or hostility towards a person on the grounds of that person's presumed race, skin colour, ancestry, national or ethnic origin, sex, sexual orientation, civil status, birth, age, wealth, religious or philosophical beliefs, current or future state of health, disability, language, political beliefs, [1 membership of a trade union,]1 physical or genetic characteristics, or social origins.'

Article 377ter of the Criminal Code: 'In the cases provided for in this chapter or in Chapters VI and VII of this title, the minimum penalties imposed by the articles concerned may be increased by two years if they concern imprisonment for a major criminal offence and doubled if they concern imprisonment for other offences, where the crime or infraction was committed against a minor aged under 16 years and where, prior to the crime or offence, the perpetrator had groomed the minor with the intention of subsequently committing the acts referred to in this chapter or in Chapters VI and VII of this title. In the cases referred to in paragraphs 4 to 6 of Article 377, any increase to the minimum penalty laid down in the first paragraph must be such that, when combined with the increase to the penalties provided for in Article 377bis, it does not exceed the maximum penalty provided for.]1'

Article 377quater of the Criminal Code: '[1 Any adult who, using information and communication technology, proposes a meeting with a minor under the age of 16 years with the intention of committing an offence referred to in this chapter or in Chapters VI and VII of this title, shall be liable to imprisonment of between one and five years, if the proposal was followed by actual deeds leading to the meeting.]1'

Article 378 of the Criminal Code: 'In the cases provided for by this chapter, offenders shall be sentenced to revocation of the rights set out in [1 the first paragraph of Article 31]1.

[2 The courts may also temporarily or permanently ban the offender from directly or indirectly operating a rest home, care facility, retirement home or any other residential facility for the people referred to in the third paragraph of Article 376, or from being a volunteer, member of the permanent or contract staff, or member of the administrative or management bodies of any institution or association whose activities relate mainly to the vulnerable people referred to in the third paragraph of Article 376. This ban shall be implemented in accordance with Article 389.]'

Article 378bis of the Criminal Code: 'It is prohibited to publish or disseminate texts, drawings, photographs, images of any kind or audio messages revealing the identity of the victim of an offence referred to in this chapter, whether in a book, in the press, on film, on the radio, on television or by any other means, unless the victim gives written consent or the public prosecutor or examining magistrate gives permission for the purposes of information and instruction. The offences in this article shall be subject to imprisonment of between two months and two years and a fine of between [EUR] 300 and [EUR] 3 000, or to one of these penalties.'

CHAPTER VI - (CORRUPTION OF MINORS AND PROSTITUTION)

Article 379 of the Criminal Code: 'Anyone who contravenes public decency by provoking, encouraging or facilitating the debauchery, corruption or prostitution of a minor of either sex in order to satisfy the desires of another person, shall be liable to imprisonment (of between five and 10 years) and a fine of between [EUR] 500 and [EUR] 25 000. The penalty shall be (imprisonment of) between 10 years and 15 years and a fine of between [EUR] 500 and [EUR] 50 000 if the minor is under the age of 16 years. (The penalty shall be (imprisonment of) between 10 years and 15 years and a fine of between [EUR] 500 and [EUR] 50 000 if the minor is under the age of 16 years.)'

Article 380 of the Criminal Code: '1. A penalty of imprisonment of between one and five years and a fine of between [EUR] 500 and [EUR] 25 000 shall be applicable to: 1 anyone who, in order to satisfy the desires of another person, recruits, impels, entices or retains the services of an adult, even where the adult consents, for the purposes of debauchery or prostitution; 2 anyone who keeps a brothel or bawdy house; 3 anyone who sells, rents out or makes available rooms or any other premises for the purposes of prostitution, with the aim of obtaining an abnormal profit; 4 anyone who exploits, by whatever means, the debauchery or prostitution of another person. 2. Anyone who attempts to commit the offences referred to in paragraph 1 above shall be liable to imprisonment of between six months and three years and a fine of between EUR 100 and EUR 5 000. 3. The penalty for the offences referred to in paragraph 1 shall be (imprisonment of) between 10 and 15 years and a fine of between [EUR] 500 and [EUR] 50 000 where the offender: 1 uses deception, violence, threats or any other form of coercion, either directly or indirectly; 2 or abuses [1 the vulnerability resulting from a person's illegal or insecure administrative status, age, pregnancy, illness, infirmity or physical or mental disability].

4. A penalty of (imprisonment of) between 10 and 15 years and a fine of between [EUR] 1 000 and [EUR] 100 000 shall be applicable to: 1 anyone who, in order to satisfy the desires of another person, recruits, impels, entices or retains the services of a minor (...), either directly or through the use of an intermediary and even where the minor consents, for the purposes of debauchery or prostitution; 2 anyone who, either directly or through the use of an intermediary, keeps a brothel or bawdy house where minors engage in prostitution or debauchery;

3 anyone who sells, rents out or makes available to a minor rooms or any other premises for the purposes of debauchery or prostitution, with the aim of obtaining an abnormal profit; 4 anyone who exploits, by whatever means, the debauchery or prostitution of a minor (...).(5 anyone who procures the debauchery or prostitution of a minor by providing, offering or promising a material or financial reward.) 5. (Anyone who commits an offence referred to in paragraph 4 shall be liable to imprisonment of between 15 and 20 years and a fine of between [EUR] 1 000 and [EUR] 100 000 if the offence is committed against a minor under the age of 16 years.) (6. Anyone who assists in the debauchery or prostitution of a minor shall be liable to imprisonment of between one month and two years and a fine of between [EUR] 100 and [EUR] 2 000.) 7. The fine shall be applied as many times as there are victims.]'.

Article 380bis of the Criminal Code: 'Anyone who uses words, gestures or signs in a public place that cause a person to engage in debauchery shall be liable to imprisonment of between eight days and three months and a fine of between [EUR] 26 and [EUR] 500. The penalty shall be doubled if the offence is committed against a minor.'

Article 380ter of the Criminal Code: '1. Anyone who directly or indirectly publishes, distributes or disseminates advertising for services of a sexual nature or who directly or indirectly causes such advertising to be published, distributed or disseminated, by any means and even where the nature of the advertising is disguised through the manipulation of language, shall be liable to imprisonment of between two months and two years and a fine of between [EUR] 200 and [EUR] 2 000 where the advertising is specifically intended for minors or features services offered by minors or by people purporting to be minors. The penalty shall be imprisonment of between three months and three years and a fine of between [EUR] 300 and [EUR] 3 000 where the direct or indirect purpose or result of the advertising referred to in paragraph 1 is to facilitate the prostitution or debauchery of a minor or the sexual exploitation of a minor.

2. Anyone who directly or indirectly publishes, distributes or disseminates advertising for services of a sexual nature or who directly or indirectly causes such advertising to be published, distributed or disseminated, by any means and even where the nature of the advertising is disguised through the manipulation of language, shall be liable to imprisonment of between one month and one year and a fine of between [EUR] 100 and [EUR] 1 000 where the services are provided by a means of telecommunications. 3. In cases not covered by paragraphs 1 and 2, anyone who makes it known by any means of advertising that he or she engages in prostitution, facilitates the prostitution of another person, or wishes to enter into relations with a person who engages in debauchery, even where the nature of the offer or request is disguised through the manipulation of language, shall be liable to imprisonment of between one month and one year and a fine of between [EUR] 100 and [EUR] 1 000. Anyone who encourages, through references made in any means of advertising, the sexual exploitation of minors or adults or uses such advertising when offering services, shall be liable to the same penalties.'

Article 381 of the Criminal Code: 'The punishment shall be imprisonment of between 15 and 20 years and a fine of between EUR 1 000 and EUR 100 000 in the case of the offences referred to Articles 379 and 380(3) and (4), or imprisonment of between 17 and 20 years and a fine of between EUR 1 000 and EUR 100 000 in the case in the case of the offences referred to in Article 380(5), if the offences constitute participation in the main or secondary activity of an association, regardless of whether or not the offender is the leader of the association.'

Article 382 of the Criminal Code: '(1) 'In the cases referred to in Articles 379 and 380, offenders shall also be sentenced to revocation of the rights set out in [1 the first paragraph of Article 31]1. 2. The courts may also ban, for a period of between one and three years, individuals convicted of an offence provided for in Article 380(1) to (3) from operating, either themselves or through an intermediary, or from being employed in any capacity whatsoever by, licensed premises, an employment agency, a performance business, an agency that rents or sells visual media, a hotel, a furniture rental business, a travel agency, a marriage agency, an adoption institution, an establishment entrusted with the care of minors, a business transporting pupils and youth groups, a leisure or holiday establishment, or any other establishment offering physical or mental care.

In the event of a second conviction for an offence provided for in Article 380(1) to (3), the ban may be for a period of between one and 20 years. In the event of a conviction for an offence provided for in Articles 379 and 380(4) and (5), the ban may be for a period of between one and 20 years. 3. Regardless of whether the operator, owner, lessee or manager is a natural or legal person, the court may order the establishment in which the offences were committed to be closed for a period of between one month and three years.

If the offender is not the owner, operator, lessee or manager of the establishment, its closure may only be ordered if the severity of the practical circumstances requires, and may last a maximum of two years, following a summons requested by the public prosecution service, or the owner, operator, lessee or manager of the establishment. The summons before the court shall be recorded in the mortgage registry of property locations at the request of the bailiff serving the process. The summons must include the land registry identification of the building concerned and identify its owner in the form and subject to the penalty provided for in Article 12 of the Law of 10 October 1913 amending the law on mortgages and the law on forced expropriation and reorganisation of the mortgage registry. Any decision taken in the case shall be noted in the margins of the summons record in accordance with the procedure provided for in Article 84 of the law on mortgages. The registrar shall send the extracts and the declaration that no appeal has been lodged to the mortgage registrar. (4) Article 389 shall apply to this provision.'

Article 382bis of the Criminal Code: 'Without prejudice to the application of Article 382, any conviction for the acts referred to in Articles 372 to 377, [377quater,] 379 to 380ter, 381 and 383 to 387, committed against a minor or involving the participation of a minor, may entail, for a duration of between one and twenty years, a ban on the right: (1) to participate, in any capacity, in teaching given in a public or private establishment serving minors; (2) to be part, as a volunteer, permanent or contractual member of staff, or member of the management bodies of any legal person or unincorporated association whose activities relate mainly to minors;

(3) to be assigned to an activity which places the offender in a relationship of trust or authority with minors, as a volunteer, permanent or contractual member of staff, or member of the management bodies of any legal person or unincorporated association. [(4) to live, reside or be present in the area designated by the competent judge. Special justification must be given for imposing this measure, and the severity of the acts and offender's capacity for reintegration must be taken into account.] Article 389 shall apply to this provision.'

Article 382ter of the Criminal Code: '[The special confiscation referred to in Article 42(1) shall be applied even if the offender is not the owner of the items to which it applies, albeit without this confiscation being able to prejudice the rights of third parties to assets likely to be subject to confiscation. It must also be applied, under the same circumstances, to the movable property or part of it, to the immovable property, room or any other space. It may also be applied to the equivalent of the movable and immovable property alienated between the offence being committed and the final judicial decision being given. If immovable property is seized, the procedure to be followed shall be that set out in Article 35bis of the Code of Criminal Procedure.]'

Article 382quater of the Criminal Code: '[When an offender convicted of an act referred to in Articles 372 to 377, [377quater], 379 to 380ter and 381 is, due to their status or profession, in contact with minors and there is a known employer, legal person or authority with disciplinary power, the court can order the transfer of the criminal part of the sentence to this employer, legal person or disciplinary authority. This measure shall either be taken automatically, or at the request of the private party or the public prosecutor in a judicial decision specially justified by the severity of the acts, the capacity for reintegration or the risk of repeat offending.]'

CHAPTER VII - PUBLIC INDECENCY

Article 383 of the Criminal Code: 'Anyone who has displayed, sold or distributed songs, leaflets or other printed or non-printed material, models or images contravening public decency shall be liable to imprisonment for a term of between eight days and six months and to a fine of between EUR 26 and EUR 500. (Anyone who has sung, read, recited, played or uttered obscenities at the public meetings or in the public spaces referred to in Article 444(2) shall be liable to the same penalties.) (Anyone who has manufactured, held, imported or had imported, transported or had transported, handed over to a transport or distribution agent, or advertised by whatever means, with a view to sale or distribution, songs, leaflets, written material, models or images contravening public decency shall be liable to the same penalties;) (Anyone who has displayed, sold or distributed emblems or objects contravening public decency, or, with a view to sale or distribution, has manufactured or held, imported or had imported, transported or had transported, handed over to a transport or distribution agent, or advertised them by whatever means.) (Anyone who has, through display, sale or distribution of printed or non-printed written material, or by whatever means of advertising, advocated the use of any means of terminating a pregnancy, has provided instructions on how to obtain or use such means, or has made them known, with the aim of recommending them, people who apply such means. Anyone who has displayed, sold, distributed, manufactured or had manufactured, had imported, had transported, handed over to a transport or distribution agent, or advertised by whatever means drugs or devices specifically intended to terminate a pregnancy or which claim to do so.)'

Article 383bis of the Criminal Code: '(1) (Without prejudice to the application of Articles 379 and 380, anyone who has displayed, sold, rented out, distributed, broadcast or handed over emblems, objects, films, photos, slides or other visual media representing sexual positions or acts of a pornographic nature, involving or depicting minors, or, with a view to sale or distribution, has manufactured or held, imported or had imported, or handed these items over to a transport or distribution agent, shall be liable to imprisonment of between five and ten years and a fine of between EUR 500 and EUR 10 000.)

(2) Anyone who has knowingly possessed the emblems, objects, films, photos, slides or other visual media referred to in paragraph 1 [or knowingly access them through a computer system or other technological means] shall be liable to imprisonment of between one month and one year and a fine of between EUR 100 and EUR 1000. (3) If the offence referred to paragraph 1 constitutes participation in the main or secondary activity of an association, the punishment shall be imprisonment of between 10 and 15 years and a fine of between EUR 500 and EUR 50 000, regardless of whether or not the offender is the leader of the association. (4) The special confiscation provided for in Article 42(1) may be applied with regard to the offences referred to in (1) and (2) above, even if the offender is not the owner of the items to which it applies. (5) (Articles 382 are 389 shall apply) to the offences referred to in (1) and (3) above.'

Article 384 of the Criminal Code: '(In the cases referred to in Article 383), the creator of the written material, model, image or object shall be liable to imprisonment of between one month and one year and a fine of between EUR 50 and EUR 1000.

Article 385 of the Criminal Code: 'Anyone who causes an affront to public decency through indecent behaviour shall be liable to imprisonment of between eight days and one year and a fine of between EUR 26 and EUR 500. (If the affront was committed in the presence of a minor aged under 16 years, the punishment shall be imprisonment of between one month and three years and a fine of between EUR 100 and EUR 1000.)'

Article 386 of the Criminal Code: 'If the offences referred to in Article 383 were committed against minors, the punishment shall be imprisonment of between six months and two years and a fine of between EUR 1000 and EUR 5000. In the same cases and without prejudice to the application of Article 385(2), the punishments provided for in the first paragraph of this article may be doubled.'

Article 387 of the Criminal Code: 'Any who sells or distributes to minors or displays on or along a public highway indecent images, models or objects likely to disturb minors' imagination shall be liable to imprisonment of between six months and two years and a fine of between EUR 1000 and EUR 5000.'

Article 388 of the Criminal Code: 'In the cases provided for in this chapter, offenders may also be sentenced to revocation of the rights set out in [Article 31(1)]. In the case of conviction under Articles 386(1) or 387, if the offence was committed in the operation of a business selling books, second-hand books, photographic equipment or material necessary for the creation of any type of visual medium, or an entertainments business, the establishment in question may be ordered to close for a duration of between one month and three months. In the event of a second conviction for one of the acts referred to in paragraph (2), committed within three years of the first conviction, the closure may be ordered for a duration of between three months and six months. In the event of a third conviction for the same acts, committed within five years of the second conviction, permanent closure may be ordered.

In this last case, the court may also ban the offenders from operating, either themselves or through an intermediary, a business selling books, second-hand books, photographic equipment or material necessary for the creation of any type of visual medium, an entertainments business, or one or more of these businesses, or from being employed in any such business in any capacity. If the offender is not the owner, operator, lessee or manager of the establishment, its closure may only be ordered if the severity of the practical circumstances requires. In this cases, Article 382(3), subsections 2 to 5 shall apply. Article 389 shall apply to this provision.'

Article 389 of the Criminal Code: '(1) The duration of the ban imposed in application of Articles 378, 382(1), 382bis and 388(1), shall start from the day of the suspended sentence, or the day on which the offender served the (suspended) sentence or on which the (suspended) sentence was extinguished by limitation and, in the event of early release, from the day of release, provided that this is not revoked. However, the ban imposed in application of Article 382(2) shall be effective from the date on which the sentencing following trial or default sentencing becomes irrevocable. (2)

Any infringement of the sentence or judgment imposing a ban pursuant to the articles referred to in (1) above shall be punished by imprisonment of between one month and six months and by a fine of between EUR 100 and EUR 1 000 or by one of these penalties. (3) The closure ordered pursuant to Articles 382(3) and 388 shall be effective from the date on which the sentencing following trial or default sentencing becomes irrevocable. (4) Any infringement of the sentence or judgment ordering the closure of an establishment pursuant to the articles referred to in (3) above shall be punished by imprisonment of between three months and three years and by a fine of between EUR 1000 and EUR 5000 or by one of these penalties.

Article 433bis(1) '[Any adult shall be liable to imprisonment of between three months and five years for communicating using information and communication technology with a minor or presumed minor, with a view to facilitating the commission of a crime or offence against the minor: (1) if the adult has hidden or lied about their identity, age or position; (2) if the adult has insisted that the exchanges remain secret; (3) if the adult has given or alluded to a gift or other advantage; (4) if the adult has manipulated the minor in any other way.]'

Article 210bis of the Criminal Code: '(1) Anyone who commits forgery by entering data in a computer system, by modifying or deleting the data stored, processed or transmitted by a computer system, or by modifying through any technological means the possible use of data in a computer system and thus changes the legal significance of these data, shall be liable to imprisonment of between six months and five years and a fine of between EUR 26 and EUR 100 000 or one of these penalties. (2) Anyone who makes use of data obtained through these methods, knowing that they are false, shall be liable to punishment as if they were the perpetrator of the forgery. (3) An attempt to commit the offence referred to in (1) shall be punished by imprisonment of between six months and three years and a fine of between EUR 26 and EUR 50 000 or one of these penalties. (4) The penalties provided for in (1) to (3) shall be doubled if any of these provisions is breached within five years of a conviction for one of these offences or for one of the offences referred to in Articles 259bis, 314bis, 504quater or in Title IX bis.

Article 504quater of the Criminal Code: (1) (Anyone who attempts to obtain, for themselves or others, with a fraudulent intent, an illegal economic advantage) by entering data in a computer system, by modifying or deleting the data stored, processed or transmitted by a computer system, or by modifying through any technological means the (normal use of) data in a computer system, shall be liable to imprisonment of between six months and five years and a fine of between EUR 26 and EUR 100 000 or one of these penalties. (2) An attempt to commit the offence referred to in (1) shall be punished by imprisonment of between six months and three years and a fine of between EUR 26 and EUR 50 000 or one of these penalties. (3) The penalties provided for in sections (1) to (2) shall be doubled if any of these provisions is breached within five years of a conviction for one of these offences or for one of the offences referred to in Articles 210bis, 259bis, 314bis, or in Title IX bis.'