Council of the
European Union

Brussels, 19 May 2017
(OR. fr)

7162/1/17
REV 1 DCL 1

GENVAL 22
CYBER 38

DECLASSIFICATION

of document:	7162/1/17 REV 1 RESTREINT UE/EU RESTRICTED
dated:	2 May 2017
new status:	Public
Subject:	7th round of Mutual Evaluations The practical implementation and operation of European policies on prevention and combating cybercrime - Report on Luxembourg

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, 2 May 2017
(OR. fr)

7162/1/17
REV 1

RESTREINT UE/EU RESTRICTED

GENVAL 22
CYBER 38

DECLASSIFIED

REPORT

Subject:	7th round of Mutual Evaluations The practical implementation and operation of European policies on prevention and combating cybercrime - Report on Luxembourg

ANNEX

CONTENTS

DECLASSIFIED

DECLASSIFIED

DECLASSIFIED

DECLASSIFIED

1 EXECUTIVE SUMMARY

- The evaluation visit to Luxembourg took place in a positive atmosphere. The Luxembourg authorities had taken great care in preparing both the programme and the evaluation team's interviews with representatives from the institutions and ministries involved.

- Luxembourg has implemented the main pieces of European and international legislation on combating cybercrime in its national law, and continues to explore what legislation it could adopt to improve its substantive law.

- Given the close relationship between its institutions and external partners when it comes to cybersecurity, Luxembourg can serve as an example for public-private partnerships, particularly on training, awareness-raising and prevention, and for the sharing of know-how, internationally as well as nationally.

- Nevertheless, bearing in mind the large number of different approaches, there is room for improvement in capacity to react operationally, including at the international level. That improvement could involve an increase in the human and financial resources allocated to the various entities involved, mainly at the Interior Ministry.

DECLASSIFIED

2 INTRODUCTION

Following the adoption of Joint Action 97/827/JHA of 5 December 1997[1], 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 of the Joint Action, 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[2] (transposition date 18 December 2013) and Directive 2013/40/EU on attacks against information systems[3] (transposition date 4 September 2015) are particularly relevant in this context.

DECLASSIFIED

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

Moreover, the June 2013 Council conclusions on the EU Cybersecurity Strategy[4] reiterate the objective of ratification of the Council of Europe Convention on Cybercrime (the Budapest Convention)[5] 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 xenophobia and racism committed through computer systems[6].

Experience from past evaluations shows that Member States are in different positions regarding implementation of the relevant legal instruments, and the current process of evaluation may also provide useful input to Member States that may not have 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 relating to fighting cybercrime, but also on operational aspects in the Member States.

Therefore, apart from cooperation with prosecution services, this 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.

DECLASSIFIED

4 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.

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

6 ETS No. 189, which was opened for signature on 28 January 2003 and entered into force on 1 March 2004.

The sequence of visits to the Member States was adopted by the GENVAL Working Party on 1 April 2014. Luxembourg was the twenty-fifth Member State to be evaluated during this round of evaluations. In accordance with Article 3 of the abovementioned 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 consist 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 Luxembourg were Mr Yves Vandermeer and Mr Stephane Robinot, together with Ms Carmen Necula 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 Luxembourg between 6 and 9 June 2016, and on Luxembourg's detailed replies to the evaluation questionnaire together with its detailed answers to subsequent follow-up questions.

DECLASSIFIED

3 GENERAL MATTERS AND STRUCTURES

3.1 National cybersecurity strategy

Luxembourg has a cybersecurity strategy. The English version can be downloaded from the ENISA website: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Luxembourg_Cyber_Security_strategy.pdf

The strategy is also designed to combat cybercrime. It sets out action to be taken, both in overarching terms and specifically:

- Overarching measures: Luxembourg seeks to promote national and international cooperation. Cybersecurity is a challenge to be tackled not by individuals, but collectively. Luxembourg is fostering cooperation and exchanges of information by establishing a shared taxonomy following a risk-based approach. This coordinated approach reduces both the effort required on the part of each individual and the complexity faced by each entity, thus putting cybersecurity into the hands of the many.
- Specific measures: Luxembourg has also provided for specific measures to fight cybercrime more effectively. These include, in particular, groups for coordination and information exchange between the public prosecutor's office, police services and the CERT, cooperation with Europol, EUCTF, Interpol and the FBI, ICCAM as a platform for exchange with Interpol and the INHOPE hotlines.

DECLASSIFIED

3.2 National priorities with regard to cybercrime

- Prevention

Luxembourg is aware that prevention plays a fundamental role in the fight against cybercrime. It therefore invests considerable effort in raising awareness among all those who may be affected (young people, adults, the elderly, private-sector employees and public-sector staff). There are several large-scale 'programmes' by means of which Luxembourg reaches out to these various target groups: BEE SECURE is for individuals (children, young people, parents and supervisors, adults in general and senior citizens), while CASES is for the public sector and private companies. Luxembourg also provides means of improving organisational security to anyone who requests them; notable examples include tools such as MONARC (an optimised methodology for CASES risk analysis) and a security check-up.

- Training

Awareness of the risks associated with digital society, and hence also cybercrime, forms a mandatory part of the curriculum in the first year of secondary education and is also compulsory for young public officials. Although mandatory measures for awareness-raising in primary education are still at the development stage, much is already being done in practice in this area. Courses for the private sector are on offer at attractive rates (EUR 25 per person). BEE SECURE offers information sessions and courses for parents, teachers and educators on demand. These awareness-raising and training activities provide a large amount of information on cybercrime-related threats.

DECLASSIFIED

- Detection

Luxembourg has recognised that it is essential to detect, as quickly as possible, any instances of information systems being compromised, and to react effectively. As a result, Luxembourg has four CERTs in the public sector and seven in the private sector. The CERTs use the MISP information-sharing platform to exchange information on indicators of a system being compromised. Many businesses (provided they meet a minimum size requirement) are also connected to this information-sharing platform.

- Response to incidents

Luxembourg has four public-sector CERTs that proactively manage incidents affecting Luxembourg. Luxembourg is highly aware of the importance of reacting quickly and effectively. Moreover, the BGP Ranking project documents the effectiveness of Luxembourg's CERTs in considerable detail.

- International cooperation

Luxembourg is very active at several levels:

- the CERTs from Luxembourg are closely interconnected
- Luxembourg is highly active in the ENISA context
- Kanner-Jugendtelefon operates the BEE SECURE Stopline and, in that capacity, is a member of INHOPE (the International Association of Internet Hotlines). Luxembourg is also a member of the Europe-wide Insafe network (of 'Safer Internet Centres') through the BEE SECURE initiative.

- BEE SECURE – initiative to raise awareness among the general public operated by the National Youth Service, securitymadein.lu and Kanner-Jugendtelefon (free telephone helpline for children and young people). BEE SECURE is a joint initiative of the Ministry of Economic Affairs, the Ministry of Family Affairs, Integration and the Greater Region, and the Ministry of National Education, Children and Young People.

DECLASSIFIED

3.3 Statistics on cybercrime

3.3.1 Overall trends in cybercrime

The first point to note is that Luxembourg's public prosecutor's office has had a special cybercrime department since 1 April 2011.

Initial statistics on cases filed with a 'cyber' reference between 1 April 2011 and 1 December 2012 record 385 such cases in a one-and-a-half-year period, and 228 in the second year. Between 2013 and 2014, the number of such 'cyber' cases increased by 50 % on the previous year (350 cases).

Between 1 January 2015 and 31 December 2015, 470 'cyber' cases were filed, which represents a further increase of almost 35 %.

There were more instances of fraud of any type (126) than of extortion and attempted extortion using compromising video footage recorded without the victims' knowledge (99).
The main ways of committing fraud included, in particular:

- rental of non-existent apartments (41)
- Microsoft scams (26)
- miscellaneous online selling of non-existent items (28)
- selling of non-existent dogs (9)
- selling of non-existent cars (8)
- non-existent holiday lettings (5)
- fake PayPal accounts (5)
- fake loans (2)
- 'Nigerian' scams (2)

DECLASSIFIED

The number of cases of phishing stabilised at 21 (compared to 17 in 2013 and 35 in 2014).

There was a marked increase (31 cases, up from 16 in 2014) in bank transfer scams, which involve criminals sending emails in the name of a bank customer and requesting a transfer to an account held by a third party (money mule) who has no right to receive the payment in question.

Another phenomenon that developed in 2014 (30 cases) and 2015 (35 cases) is CEO fraud. In this type of fraud, the perpetrator contacts the accounting department of a company claiming to be the CEO or a member of the board of directors. While insisting on the confidential nature of the exchange, he provides information about an important contract which needs to be concluded urgently. The perpetrator is generally very well informed about the structure of the company targeted and makes use of fictitious documents, prepared in advance, to demonstrate that the alleged operation is genuine. Using these details, he manages to convince the accountant to transfer funds to a foreign account (generally held by a money mule).

Of the 470 cases, 370 were classified as having an 'unknown perpetrator' while 27 files were closed without further action (in certain cases after a judicial inquiry or police investigation).

A police investigation was launched or continued in 42 cases, a judicial inquiry was opened in eleven cases, and in six cases a ‘mini-investigation' was requested. Possible convictions for these offences have not been identified, as the computer system does not allow them to be distinguished from other convictions. However, it is expected that a figure will be available for 2016.

The 470 cases represent a loss of at least EUR 3 052 315.37 (as against EUR 2 108 764.07 in 2014). This figure reflects only directly quantifiable financial losses. The new significant increase relates in particular to CEO fraud cases and to fake transfer orders.

DECLASSIFIED

As occurs every year, it should be noted that the large number (3 or 4 cases per day, over 900 a year) of cases of theft involving stolen credit card data, and the failure to identify the perpetrators, means that such cases are not included in these statistics, but are transmitted to the General Crime Section of the Criminal Investigation Department (SPJ) for centralisation and processing with information compiled by Europol, with a view to a major investigation in this field.

As regards cases of child pornography, 21 new cases involving possession of child pornography material (Article 384 of the Criminal Code) and transmission of child pornography material (Article 383 et seq. of the Criminal Code) were opened in 2013. Seven cases investigated during this period resulted in judgments/convictions, while two cases led to acquittals.

41 new cases involving possession of child pornography material (Article 384 of the Criminal Code) and transmission of child pornography material (Article 383 et seq. of the Criminal Code) were opened in 2014. Thirteen cases investigated during this period resulted in judgments/convictions.

Finally, 29 new cases involving possession of child pornography material (Article 384 of the Criminal Code) and transmission of child pornography material (Article 383 et seq. of the Criminal Code) were opened in 2015. Nineteen cases investigated during this period resulted in judgments/convictions.

It is difficult to determine the figure for cybercrime cases as a percentage of all cases. Overall, 52 959 cases were registered at the Luxembourg Public Prosecutor's Office in 2015.

DECLASSIFIED

3.3.2 Number of cybercrime cases recorded

The judicial statistics service is responsible for establishing all the statistics on Luxembourg courts.

The Grand Duchy Police do not access the statistics of external institutions and use only information derived from an internal database.

3.4 Amounts allocated under national budgets to prevent and combat cybercrime and the EU's financial contribution

As preventing cybercrime is one of GOVCERT's primary missions, the budget allocated to it by the State is fully invested in this domain. It should be noted, however, that the budget is divided into two parts: one is used for the acquisition of equipment (servers, PCs, etc. - EUR 60 000 in 2015), while the other budget item, used to ensure the efficient operation of GOVCERT (consultancy, studies, etc.) is limited to EUR 530 000.

GOVCERT has the two only budgetary items dedicated to cybercrime:
- 30.6.74.310 – Computer Emergency Response Team (GOVCERT): acquisition and installation of special equipment.
- 00.6.12.385 – Computer Emergency Response team (GOVCERT): operating costs.

GOVCERT does not receive funding from the EU to carry out its missions.
BEE Secure also has a budget under the European Commission's 'Connecting Europe Facility' programme.

DECLASSIFIED

3.5 Conclusions

The new national cybercrime strategy, which was adopted 27 March 2015, replaces and builds on the 2013 version.

After defining the different concepts relating to cybersecurity (an element that was lacking in the 2013 strategy), this new document lays down seven objectives, accompanied by their respective actions plans. The priorities as regards cybersecurity are: prevention, training, detection, response to incidents, international cooperation, raising public awareness, and raising the awareness of, and providing training for, public and private entities.

It should be noted that the key to this strategy is reinforcing cooperation. Whether at national or international level, or with the academic world, Luxembourg already has, for reasons relating to its traditions and culture, a solid basis for cooperation among the various domestic players.

It needs, however, to clearly develop its involvement in international cooperation, whether in the sphere of cybercrime or the broader field of cybersecurity.
Accordingly, while the creation of the national agency for the security of information systems is to be welcomed, it has not yet been provided with sufficient human and technical resources to carry out its tasks. As from 2017, and along with other entities, it should be possible to allocate a minimum level of human resources at the level of the central body, although this is a matter for a future collaboration.

DECLASSIFIED

As regards law enforcement, there is a cybercrime working group that brings together national authorities (Public Prosecutor's Office, police and CERT) for the purposes of exchanging information regularly. The subjects of discussion cover inter alia police and/or judicial cooperation with service providers and the procedure for cooperation and intervention between the police and the CERTs.

As regards the Ministry of Justice, the national priorities in relation to cybercrime appear to be well defined and to clearly identify the players, and the specialisation of the judicial authorities is a good practice..

The figures include computer-related offences as such, as well as other offences committed using a computer, all of which come under the 'cyber' heading. Like many other European countries, the national authorities acknowledge the existence of a ‘dark figure', i.e. cases in which the offence is not reported by the victim.

Of the 470 cyber cases reported in 2015, and despite the fact that the financial loss was very significant, a large number (370) of cases were classified as having been committed by an unknown perpetrator. The causes cited by the national authorities include the impossibility of identifying the perpetrators, the international nature of offences of this type, and difficulties as regards cooperation and mutual legal assistance. Another obstacle relates to the fact that the ISPs do not cooperate and that the data are not located in Luxembourg.

DECLASSIFIED

There are eleven CERTs in Luxembourg, of which four are financed by the Government. GOVCERT is responsible for critical infrastructure and works with the IT services of the entities concerned. It is the single point of contact for State entities. Its main task is to deal with incidents involving classified and non-classified infrastructure. The director of GOVCERT chairs the cyber-risk evaluation cell. Other services provided by GOVCERT are: incident handling, detection of compromised systems, black listing, analysis (automatic and manual) of malware, and security notices and recommendations.

Other CERTs focus on the private, health or research spheres. These CERTs hold meetings every three months to coordinate their cybercrime policies.

As regards prevention, in order to prepare for and manage possible crises effectively, the competent authorities organise exercises and draw up plans to ensure coordination.

DECLASSIFIED

4 NATIONAL STRUCTURES

4.1 Judicial system (prosecution and courts)

4.1.1 Internal structure

Public institutions responsible for preventing and combating cybercrime

- BEE SECURE – initiative to raise awareness among the general public, operated by the National Youth Service, securitymadein.lu and Kanner-Jugendtelefon (free telephone helpline for children and young people).
  - o Awareness-raising
  - o Assistance for citizens (BEE SECURE Helpline helpline.bee-secure.lu)
  - o Following up on anonymous reports (BEE SECURE Stopline stopline.bee-secure.lu) of child sexual abuse material or content that is of a racist, discriminatory or terrorist nature, or involves Holocaust revisionism
- Cyber Security Board - centralising body on combating and prevention of cybercrime
- CASES – raising awareness – training and organisational security for public and private bodies; run by securitymadein.lu
  - o Awareness-raising
  - o Training
  - o Preventive organisational measures
  - o Risk analysis methods
- CIRCL, GOVCERT – public CERTs
  - o Detection
  - o Response to incidents
- ANSSI (National Agency for the Security of Information Systems)
  - o Security policies for public-sector stakeholders and operators of critical infrastructure

DECLASSIFIED

Luxembourg's Public Prosecutor's Office has had a special cybercrime section since 1 April 2011.

At present, two magistrates from the Public Prosecutor's Office (a first assistant and an assistant) and a magistrate at the level of the Financial Intelligence Unit are responsible - amongst their other duties - for cybercrime cases.

This does not include child pornography cases, which are dealt with by three magistrates from the youth section (three first assistants), racism cases, which are dealt with by a magistrate (principal assistant), and terrorism cases, which are dealt with by another magistrate (deputy public prosecutor).

At the level of the office of the investigating judge, there is an investigating judge specifically responsible for cybercrime cases.

4.1.2 Capacities available and obstacles to the successful conclusion of investigations

With regard to the collection of computer data by the investigating authorities, Luxembourg has transposed the system established under the Budapest Convention, which provides for a two-stage procedure: the first stage involves storing the data for a certain period while the second allows data to be seized under ordinary law procedures.

To facilitate the comprehensibility of national texts, the Luxembourg legislator has defined a general procedure for storing data which applies to all these cases. Article 48-25 of the Code of Criminal Procedure (CIC) states as follows:

DECLASSIFIED

'Where there is reason to believe that the data stocked, processed or transmitted in, or through, a processing or automated transmission system, which would be useful in establishing the truth, are vulnerable to loss or modification, the Public Prosecutor or the investigating judge seised may order the rapid and immediate preservation of computer data for a period not exceeding 90 days'.

Article 48-25 of the Code of Criminal Procedure provides for fast-track retention of data in the event of an offence in the process of being committed or of a preliminary investigation by the public prosecutor, and in the context of an investigation by an investigating judge. The procedure can be used at international as well as national level in the context of international letters rogatory.

In practice, the public prosecutor or the investigating judge requests, either directly or via the police, that the data custodian (specifically a host) retain the data for 90 days. Judges may make such requests in the context of national cases or at the request of a foreign competent authority.

It is only at the second stage, which commences only after a period of 90 days has elapsed since the filing of the data retention request, that the data are seized within the framework of a national or international procedure.

Moreover, the provisions on infiltration (Article 48-17 of the Code of Criminal Procedure) have also been supplemented with respect to computer-related offences along the lines of Article 509-1 to 509-7 of the Criminal Code. Pursuant to point 3 of Article 48-17, 'infiltration consists of conducting surveillance on persons, in respect of whom there are serious indications they are in the process of committing one or more of the acts referred to in the previous paragraph, by posing, with respect to those persons, as an accomplice, accessory or receiver of stolen goods'.

DECLASSIFIED

Luxembourg national legislation on infiltration is based on the French legislation in this field, as set out in Articles 706-81 to 706-87 of the Code of Criminal Procedure.

The public prosecutor or the investigating judge may henceforth, subject to the conditions established by law, order the deletion of data if the holding or use of that data is illegal or dangerous for the security of persons or property.

The main obstacles to the successful prosecution of cybercrime offences are the following:

- the international judicial assistance instruments operate too slowly and are insufficient to respond to the ephemeral nature of online evidence;
- the differences from State to State with respect to the length of time for which data can be held, or even the complete absence of data retention. In some cases, the communication data are the only data available to identity the suspect,
- encryption;
- strategies that prevent the identification of suspects, or make it more difficult (peer-to-peer networks, TOR, DARKNET);
- the new means of payment (bitcoin and derived systems) which make it easier for criminals to evade the authorities and conceal their transactions. These payment mechanisms are complex and thus not well understood;
- The mass of data to be analysed.

DECLASSIFIED

4.2 Law enforcement authorities

The law enforcement structure for preventing and combating cybercrime is as follows:

- Principal Public Prosecutor's Office (mutual legal assistance)
- Public Prosecutor (investigation and prosecution)
- Office of the Examining Magistrate (preparatory inquiries and enforcement action)
- Financial Intelligence Unit (financial crime using new technologies)
- Criminal courts

The judicial concept (guiding principle for all involved at judicial level, drafted in close consultation with the judicial authority) determines the division of powers and tasks between the various forces of the Grand-Ducal Police as regards criminal investigation.

When it comes to combating cybercrime, offences involving digital technologies (Articles 509-1 to 509-7 of the Criminal Code, hacking, intrusion, DDOS, etc.), are within the exclusive jurisdiction of the New Technologies Section of the Criminal Investigation Department (SPJ).
With all other offences committed using digital technologies (fraud, distribution of illegal content, counterfeiting) the principle of subsidiarity determines which unit is responsible. Technical support is provided by the specialists in the New Technologies Section.

DECLASSIFIED

Prevention is the only way to combat certain damaging activities (spamming, phishing, etc.) on the internet. It is not the main task of the New Technologies Section do deal with prevention and it does not have the resources to so. This does not entail consequences though, since that task is taken up by other structures such as BEE SECURE for individuals and CASES for the public sector and private companies, in close cooperation with the various stakeholders.

The New Technologies Section of the Criminal Investigation Department is responsible for cybercrime investigations, the exception being child pornography cases (SPJ, youth protection), terrorism (SPJ, counter-terrorism cell) and CEO fraud (SPJ, section dealing with general crime and money laundering, together with the Grevenmacher criminal investigation service).

There are no specialist officers: the investigators in the New Technologies Section possess expertise and specific IT knowledge.

When it comes to serious forms of cybercrime, the New Technologies Section has three investigators who specialise in this area. They can request assistance from one or more IT forensic specialists.

These IT specialists (computer, telecommunications and electronic engineers) have been recruited from civilian life since 2003. They receive training as law enforcement officers culminating in an examination.

DECLASSIFIED

Prosecutions brought in cases of cybercrime are long and usually require international cooperation and letters rogatory.

Luxembourg has set up a contact point that is available 24/7 which involves the SPJ's New Technologies Section providing operational standby.

4.3 Other services and public-private partnership

CERT.LU is an outstanding example of a CERT public-private partnership in Luxembourg. It consists of eleven entities, four from the public sector and seven from the private sector.

The BEE SECURE campaigns, which are held annually, are widely supported by the private sector as regards the circulation of messages.

DECLASSIFIED

4.4 Cooperation and coordination at national level

4.4.1 Legal and policy obligations

In the area of data protection, Article 3(3) of the amended law of 30 May 2005 concerning specific provisions on personal protection as regards personal data processing in the electronic communications sector lays down that 'in the event of personal data breaches, the supplier of electronic communications services accessible to the public shall notify the National Data Protection Authority (CNPD) of the breach without delay'.

In general, Article 23(2) of the Code of Criminal Procedure (CIC) obliges every official who becomes aware of facts likely to constitute a crime or an offence to inform the public prosecutor without delay.

Telecom operators must report offences to the regulator, ILR.

Luxembourg has a multidisciplinary coordination mechanism for responding to serious cyber-attacks. The High Commission for National Protection (Haut Commissariat à la Protection Nationale - HCPN) coordinates the response to such attacks. It also has a Cyber Risk Assessment Unit, known as CERC.

- http://www.infocrise.public.lu/fr/cyberattaque/index.html

DECLASSIFIED

The emergency intervention plan PIU Cyber, which was approved and brought into force by the Council of Government on 19 March 2014, lays down what action the government should take in the event of a technical failure or large-scale attack on public sector and/or private sector information systems.

The crisis management bodies are the Cyber Single Point of Contact (SPOC), the Cyber Risk Assessment Unit (CERC) and the Cyber Crisis Unit.

- the Cyber Single Point of Contact (SPOC) operates 24/7 to enable national and international actors to notify the national authorities of major cyber incidents.
- the Cyber Risk Assessment Unit (CERC), which is made up of experts, assesses how the situation evolves if there is a threat and introduces enhanced surveillance prior to the possible activation of the CC.
- the Cyber Crisis Unit (CC): it is activated by the Prime Minister, who is the Minister of State, if a crisis is imminent or unexpectedly occurs. The CC initiates, coordinates and ensures the implementation of all measures designed to deal with the crisis and its consequences, which includes advising a return to normal. It prepares the decisions that have to be taken and submits them to the government for approval. In the case of operational intervention in situ, its tasks also include coordinating and monitoring implementation.

DECLASSIFIED

The plan is activated when the Cyber SPOC is notified of a cyber incident or attack by national administrations or international actors. The Cyber SPOC immediately alerts the Cyber Risk Assessment Unit (CERC) which then evaluates the available information. If the incident is likely to have a significant impact, the High Commission for National Protection is alerted and informs the Prime Minister who is Minister of State and who decides whether the CC should be activated. The CC initiates, coordinates and ensures the implementation of all measures designed to deal with the crisis and its consequences, including advising a return to normal. The measures laid down involve assessment, enhanced surveillance, technical analysis, closing off, upgrading and protection of services and activation of the national cyber reserve and the restoration of services.

Banks and e-payment and e-money institutions must abide by the provisions laid down in the law of 12 November on combating money laundering and the financing of terrorism, which transposed Directive 2001/97/EC of the European Parliament and of the Council amending Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering (hereinafter the 'ML/FT law').

The Intelligence Unit is active at international level in exchanging information to ensure that the Member State concerned receives conclusive information as rapidly as possible.

- Increase the security of non-cash payment and minimise the vulnerability of magnetic strips

DECLASSIFIED

E-payment and e-money institutions must apply the due diligence measures imposed by the ML/FT law. The analysis of transactions carried out by the Financial Intelligence Unit has shown that in very many cases fraudulent transactions are blocked before the criminal receives the profit he or she expected.

- Strengthen the procedures for authorisation of on-line transactions and authentication of customers

Introduction of the '3D secure' system, also known commercially as 'Verified By Visa' and 'MasterCard SecureCode'.

Measures to make electronic data and on-line transactions secure have also been strengthened by the entry into force of the law on electronic commerce of 14 August 2000 and the Grand-Ducal Regulation on electronic signatures which lays down the features that such signatures have to incorporate to be recognised as legal (1 June 2001).

The setting up of LuxTrust S.A., two-thirds of whose capital is held by the State, produced a common electronic security solution which is used not only by the Luxembourg government but also by the most influential banks in Luxembourg.

This solution operates on the basis of personal authentication certificates issued by LuxTrust as the certifying authority. It is thanks to these certificates that LuxTrust can guarantee the identity of the person who uses one of its products to log on to an on-line application to carry out electronic operations.

DECLASSIFIED

Generally speaking, reciprocal cooperation between authorities and issuers is shown to be satisfactory.

As regards prevention, BEE SECURE (for young people and those around them) and CASES (for organisations and their employees) have been working intensively for over five years to raise awareness and provide training.

The exchange of compromise indicators and the proactive work of the CERTs (GovCERT and CIRCL) are important for operator-level prevention. The CERTs always suggest that the victim voluntarily submit evidence. They are also able to gather such evidence.

DECLASSIFIED

4.4.2 Resources allocated to improving cooperation

The Financial Intelligence Unit follows regular training courses to familiarise itself with the latest technological developments. It is inter alia a member of the Egmont information exchange working group - Stream 3 'Financial Technologies and Transaction Innovation'. It co-chairs, with the United-States, a working party on 'fake chairman' fraud (or 'business e-mail compromise', to use US terminology).

From a police viewpoint, it should be borne in mind that where a system has been penetrated it is generally already too late to prevent cloning of the data. It may still be possible to intercept the perpetrators, however, provided that the information reappears, for example if it is presented for sale on hackers' websites. Where it is possible to trace IP addresses, attempts are made to block access to the websites or to intercept the purchasers using the stolen references.

The state-of-the art technology associated with the payment card business (which will sooner or later be replaced by applications activated by mobile phones) is constantly changing, which means that the police need to keep tabs on innovations and operating methods. International experts' conferences allow for the exchange of know-how and facilitate contacts between the authorities in charge of combating this type of crime.

Bilateral meetings or talks dealing with IT security are held for that purpose. A GOVCERT member also performs the duties of National Liaison Officer at ENISA, which provides for links with the private sector. While it is difficult to give a numerical estimate of the resources invested, a constant effort is being made to strengthen or forge links with the private sector.

DECLASSIFIED

4.5 Conclusions

Responsibility for dealing with major crime and conducting technical investigations whenever these are required always lies with the Criminal Investigation Department (SPJ). The Crime Detection and Investigation Department (Service Régional d'Enquête Criminelle - SREC) has responsibility at regional level but jurisdiction over major investigations always lies with the SPJ. The decision is taken by the public prosecutor's office on a case-by-case basis. The SPJ has a technical and scientific department comprising two sections (New Technologies and Forensic Unit).

According to the national authorities, investigations dealing with offences connected with the sexual abuse of minors generate considerable work for the Forensic Unit (GSM, mobile phones, computers used to commit the offences). That is why the police believe a special unit focusing on child pornography should be set up.

At the same time, the New Technologies Section of the Grand-Ducal Police sets an example at European level in terms of its composition, its tasks and its positioning at international level.

The possibility of civilian IT specialists qualifying as law enforcement officers makes for a very attractive combination of skills that it would be advisable to develop at European level.

DECLASSIFIED

The IT legal service was set up in 2003 to offer special support for the analysis of digital evidence. In 2015 it analysed approximately 300 terabytes of data.

The Luxembourg Public Prosecutor's Office has prosecutors who specialise in cybercrime. As to investigative agencies, there is an investigating judge specifically assigned to cybercrime cases of a certain scale and technical complexity at the office of the investigating judge.

The obstacles encountered in the fight against cybercrime are the same as those in other European countries. It should be noted that certain practitioners see the lack of an agreed time limit for data storage as a hindrance.

The public-private partnership is the real cohesive force in the fight against cybercrime in Luxembourg. Management makes up for the structural and procedural shortcomings with know-how and personal networking.

Luxembourg clearly scores well in terms of both awareness-raising activities and tools for analysing risks and mitigating cyber-attacks.

DECLASSIFIED

5 LEGAL ASPECTS

5.1 Substantive criminal law on cybercrime

5.1.1 Council of Europe Convention on Cybercrime

Luxembourg ratified the Budapest Convention on Cybercrime and the related Protocol in 2014, through its Law of 18 July 2014, which

1) adopted the Council of Europe Convention on Cybercrime, which was opened for signature in Budapest on 23 November 2001,

2) adopted the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, established in Strasbourg on 28 January 2003,

3) amended the Criminal Code,

4) amended the Code of Criminal Procedure,

5) amended the amended Law of 30 May 2005 concerning the protection of privacy in the electronic communications sector.

DECLASSIFIED

5.1.2 Description of national legislation

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

Through its Law of 3 March 2010, Luxembourg established general rules covering the criminal liability of legal persons, which are specified in the following articles of the Criminal Code:

Chapter II-1. - Penalties applicable to legal persons
Article 34 (Law of 3 March 2010): Where a criminal offence or misdemeanour is committed in the name of and in the interests of a legal person by one of its legal bodies or by one or more of its de jure or de facto managers, the legal person may be held criminally liable and incur the penalties provided for in Articles 35 to 38. The criminal liability of legal persons shall not exclude that of the natural persons who perpetrate or are complicit in the same offences. The preceding clauses are not applicable to the State or communes.
Article 35 (Law of 3 March 2010) The criminal penalties or penalties for misdemeanour incurred by legal persons shall be:
1) a fine, under the conditions and provisions set out in Article 36;
2) special confiscation;
3) exclusion from participation in public procurement;
4) dissolution, under the conditions and provisions set out in Article 38.

DECLASSIFIED

Article 36 (Law of 3 March 2010) The fine for the purposes of criminal penalties and penalties for misdemeanour applicable to legal persons shall amount to at least EUR 500. In the case of crimes, the maximum fine applicable to legal persons shall be EUR 750 000. In the case of penalties for misdemeanour, the maximum fine applicable to legal persons shall be double the amount incurred by natural persons under the law punishing the offence. Where there is no fine for natural persons in the law punishing the offence, the maximum fine applicable to legal persons may not be more than double the amount obtained by multiplying the maximum prison sentence for the offence, in days, by the amount taken into account for imprisonment as a substitute for non-collectible fines.

Article 37 (Law of 3 March 2010) The maximum level of the fine incurred pursuant to the provisions in Article 36 shall be multiplied by five where the legal person is held criminally liable for one of the following offences:

- criminal offences and misdemeanours against state security
- acts of terrorism and financing of terrorism
- infringement of laws relating to banned weapons in conjunction with a criminal association or organisation
- human trafficking and pimping
- drug trafficking in conjunction with a criminal association or organisation
- money laundering and handling of stolen goods
- embezzlement, illegal interest charging, active and passive corruption, private corruption
- facilitation of unauthorised entry and residence in conjunction with a criminal association or organisation.
- (Law of 21 December 2012) illegal employment of illegally staying third-country nationals in conjunction with a criminal association or organisation.

DECLASSIFIED

Article 38 (Law of 3 March 2010) Dissolution may be ordered where a legal person has intentionally been established or, in the case of a crime or offence that is punishable for a natural person by a prison term of three years or more, where such legal person has been misused in order to commit the offences charged.

Dissolution shall not be applicable to any legal persons under public law who may be held liable. The decision ordering the dissolution of the legal person shall also include referral of that legal person to the court with responsibility for such dissolution.

Article 39 (Law of 3 March 2010) Where the legal person incurs a misdemeanour penalty other than a fine, that penalty may be imposed on its own and constitute the principal penalty.

Article 40 (Law of 3 March 2010) Where a misdemeanour is punishable by the imprisonment of natural persons under the law punishing the offence, the special confiscation defined under Article 31 may serve as the principal penalty against the legal person, even where there is no provision to that effect in the specific law invoked.
The provisions in the previous paragraph are not applicable to press misdemeanours.

Luxembourgs legislation does not include any specific criteria for classifying particular cyber crimes as more or less serious and which might trigger a faster reaction and 'stronger measures.

DECLASSIFIED

However, a number of aggravating circumstances are provided for in such cases.
Articles 509-1 of the Criminal Code (Law of 14 August 2000) covers one aggravating circumstance and, accordingly, increased penalties in cases where access to or fraudulent maintenance of all or part of a data processing or transmission system has led either to the removal or modification of data contained in that system or to an alteration in its functioning.

Furthermore, Article 509-4 of the Criminal Code (Law of 10 November 2006) provides for an additional increase in prison sentences and fines 'where, in the cases referred to in Articles 509-1 to 509-3, cash or a sum of money has been transferred, leading to loss of property for a third party, in order to confer a financial benefit to the person committing the offence or to a third party.'

Moreover, offences committed by several persons may be treated as crimes relating to a criminal association or organisation.

Minor offences are filed as not incurring criminal proceedings, or a warning is sent drawing the perpetrator's attention to the law, or else the pre-trial chamber at the relevant district court requests a referral to the police court on the grounds of mitigating circumstances (minors, little harm, no criminal record, first court case, etc.).

DECLASSIFIED

Almost all cybercrime acts precede, and constitute acts preparatory to fraud or attempted fraud (such as CEO fraud) or to extortion or attempted extortion (supported, for instance, by compromising videos recorded on social networks without the victims' knowledge).

The offence of connection with a criminal association or organisation may also be added to such offences where they are committed by several people.

It should also be noted that cyber offences constitute predicate offences to money laundering (Article 506-1 of the Criminal Code).

Besides that, Article 57 of the Criminal Code covers all comments and messages on social networks liable to incite hatred and violence against a specific group of non-Luxembourgish nationals.

No changes to the currents laws on cybercrime are currently planned.
The documents with a significant bearing on cybercrime are:

- The Criminal Code
- The Code of Criminal Procedure
- The Law of 15 July 1993 aimed at reinforcing the fight against economic crime and computer fraud

DECLASSIFIED

- The Law of 18 July 2014 adopting the Council of Europe Convention on Cybercrime opened for signature in Budapest, which was transposed through the creation of Articles 509-1 to 509-6 of the Criminal Code
- The Law of 14 August 2000 on electronic commerce
- The amended Law of 2 August 2002 on protection of individuals with regard to the processing of personal data
- The amended Law of 30 May 2005 establishing specific rules for the protection of privacy in the electronic communications sector
- The Law of 11 August 1982 on the protection of the right to privacy
- The Law of 18 April 2001 on copyright, neighbouring rights and databases.

A legal 'technical report' was produced in connection with CIRCL activities, which comprises a short summary of important legal articles including titles, references, the scope, examples and related sanctions:

- https://circl.lu/pub/tr-44/

Directive 2013/40/EU[7] on attacks against information systems was transposed into national law by the Law of 18 July 2014 adopting the Council of Europe Convention on Cybercrime opened for signature in Budapest on 23 November 2001.

The relevant texts are included in Annex D to this report.

DECLASSIFIED

[7] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (OJ L 218, 14.8.2013, p. 8).

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

The Law of 21 February 2013 on combating sexual abuse and sexual exploitation of children and amending several provisions in the Criminal Code transposed into national law Directive 2011/93/EU, which replaced Framework Decision 2004/68/JHA and is intended to approximate the laws of EU Member States in this area, so as to combat as effectively as possible sexual abuse and sexual exploitation of children, and child pornography, and ensure the effective punishment of the offences committed, the protection of the rights of victims, the prevention of sexual exploitation and abuse of children and the establishment of effective monitoring systems.

Insofar as the provisions in the aforementioned Directive are closely based on the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, which had been transposed through the adoption of the Law of 16 July 2011 modifying several aspects of the Luxembourg Criminal Code, most of the forms of conduct covered by the Directive had already been punishable under Luxembourg law since the adoption of the Lanzarote Convention.

DECLASSIFIED

C/ Online card fraud

As a general rule, credit card companies (Six Payment, formerly Cetrel) 'require' their customers to lodge complaints with the police in order to obtain reimbursement of misappropriated sums of money, so there is a large number of complaints.

Apart from that, many companies providing payment systems (such as PayPal) or online purchasing and sales (like Amazon), as well as banks, declare suspected instances of money laundering to the Financial Intelligence Unit, which in turn sends reports to the public prosecutor's office.

Luxembourg is actively involved in exchange projects supported by the European Commission aimed at ensuring the fastest possible communication of data relating to e-commerce to the Member States involved. One such project, 'FIU.net Crossborder Reporting', has been operating since January 2015.

The main participants working out of Luxembourg were responsible for more than 7 500 exchanges between 1 January and 30 April 2016 (statistics established by Europol, the manager of FIU.net) with the following countries: Germany 2 929, United Kingdom 2 863, Italy 462, France 368, Spain 185, The Netherlands 125, Belgium 99, Austria 96, Poland 90, Ireland 52, Lithuania 43, Romania 38, Portugal 35, Bulgaria 34, Sweden 30, Denmark 29, Estonia 20, Croatia 16, Latvia 16, Cyprus 13, Hungary 10, Finland 9, Greece 9, Czech Republic 7, Slovakia 6, Slovenia 5 and Malta 3.

DECLASSIFIED

Most of the declarations in question concerned online fraud.

In theory many cases of online fraud are officially notified to the competent authorities. However, payment card companies (or companies processing the transactions made by payment cards) only issue such notifications based on the following criteria:

i. if specific clues arise that may lead to the source of the problem (and will help identify the perpetrators) or prove relevant when the fraudsters try to activate encoded cards by using stolen references;

ii. if the financial damage is above a certain amount;

iii. if there are suspicious operating methods.

That restriction is due to the considerable volume of fraud committed using payment card references, which have (as is common knowledge) reached a peak, so as to create synergies and channel/optimise efforts.

D/ Other forms of cybercrime

From a police viewpoint, it should be borne in mind that where an encryption system has been penetrated it is generally already too late to prevent cloning of the data. It may still be possible to intercept the perpetrators, however, provided that the information reappears, for example if it is presented for sale on hackers' websites. Where it is possible to trace IP addresses, attempts may be made to block access to the websites or to intercept the purchasers using the stolen references.

DECLASSIFIED

The advanced technology associated with the payment card business (which will sooner or later be replaced by applications activated by smart phones) is constantly changing, which means that the police need to keep up with innovations and operating methods. International experts' conferences allow for the exchange of know-how and facilitate contacts between the authorities in charge of combating this type of crime.

5.2 Procedures

5.2.1 Investigation techniques

- Searches and seizure of IT information/data systems

These measures are provided for under Articles 31, 33 and 66 of the CIC.

As explained above, removal of data ordered by a public prosecutor or investigating judge, on the basis of Articles 33 and 66 of the CIC, is subject to the following conditions:

- a copy of the data has been made beforehand,
- the hardware containing the data has not been seized,
- holding or use of the data is illegal or harmful to the safety of people or goods,
- the physical device (for example the computer or server) hosting the data is located in the Grand Duchy of Luxembourg.

DECLASSIFIED

- Real-time interception/collection of traffic/content data

Article 88-1 of the Code of Criminal Procedure (Law of 26 November 1982) provides that an investigating judge may exceptionally, by specially reasoned decision and in accordance with the conditions set out therein, order the use of technical methods of surveillance and monitoring on all forms of communication.

- Retention of computer data

Retention of traffic data:

In Luxembourg, the collection and retention of traffic data are regulated by the Law of 30 May 2005 establishing specific provisions for the protection of privacy in relation to the processing of personal data in the electronic communications sector.

A Grand-Ducal Regulation of 24 July 2010 setting out the categories of personal data generated or processed in the context of providing electronic communications services or public communications networks clarified the concept of 'traffic data'.

Fast-track retention of data:

Article 48-25 of the Code of Criminal Procedure permits the fast-track retention of data where an offence is in the process of being committed or of a preliminary investigation by the public prosecutor, and in the context of an investigation by an investigating judge. The procedure can be used at international as well as national level in the context of international letters rogatory.

DECLASSIFIED

In practice, the public prosecutor or the investigating judge requests, either directly or via the police, that the data custodian (specifically a host) retain the data for 90 days. Judges may make such requests in the context of national cases or at the request of a foreign competent authority.

- orders to produce stored traffic/content data

Only investigating judges may order the seizure of traffic data (Article 67-1 of the Code of Criminal Procedure). This measure must be necessary to establish the truth, and the actions under investigation must be such as to give rise to a criminal penalty or a penalty for misdemeanour, the maximum term of which is equal to or greater than one year in prison. If a judicial investigation has not (yet) been opened the public prosecutor may request that the investigating judge make an order to that effect, in accordance with the conditions set out in Article 24-1 of the Code of Criminal Procedure ('mini investigation').

Seizures of content are subject to the general law on seizures. In practice, these seizures are nonetheless ordered by an investigating judge and are generally made in the context of seizures of traffic data.

- orders to communicate data on users

DECLASSIFIED

National legislators have not established the conditions in which service providers must make on-the-spot disclosures of traffic data. Consequently, this measure requires an order in due and proper form issued by an investigating judge.

Cybercrime concepts are not specifically defined in the legislation of Luxembourg. In practice, the courts refer to the definitions contained in international texts, including the Budapest Convention and its explanatory report.

Traffic data are defined in the Grand-Ducal Regulation of 24 July 2010 setting out the categories of personal data generated or processed in the context of providing electronic communications services or public communications networks.
The definitions of search and seizure are the same as those used in the general legal context.

In the interests of good practice in this area, it should be highlighted that cybercrime investigations often take place outside of Luxembourg. The results/success of investigations in this area depend on the speed with which requests for international legal assistance are processed.

DECLASSIFIED

5.2.2 Forensic examinations and encryption

As a general rule, forensic examinations are only carried out electronically or remotely in the following specific cases:

- the suspect consents to the copying of the data (for example, a social network account, email accounts);
- If, during the search, the criminal investigation officer (OPJ) discovers an open connection to the 'cloud' on the suspect's computer and the latter does not agree to allow access to their data, the OPJ must seek authorisation from the investigating judge before copying the data.

In all other cases an order or an international letter rogatory, if the data are located outside the territory of Luxembourg, is required to seize the data.

IT-Forensic examinations are carried out by the SPJ's New Technologies Section. For examining malware found, the NT Section has access to CIRCL specialists, to the resources made available by Europol-EC3 or to the automated services offered by private companies, depending on the situation. Under ordinary criminal law procedure, use of an external judicial expert may be required as needed.

o Encryption techniques are now easy to install and use. Terrorists, paedophiles and other types of criminal use them, and without a password it is almost impossible for the experts at PGD (Police Grand-Ducale) to access the content on a hard disk. Moreover, if the password is well chosen, attacks using brute force are doomed to failure.

o Messaging services now encrypt all conversations. Messages and calls are now protected with end-to-end encryption and are indecipherable by law enforcement authorities.

o All of the latest-generation smartphones have access denial and content encryption capabilities. These capabilities are increasingly being used by criminals. As long as the suspect does not divulge the access code, the smartphone is impregnable.

DECLASSIFIED

o The most widely-used sites and search engines use the HTTPS Protocol to encrypt traffic so that it is non-decodable in the event of interception.
This is an issue in all areas, principally terrorism, child pornography and drug trafficking. The only way to access the data is to capture them before encryption. The fitting of devices in order to capture data on suspects' equipment is not allowed. Draft legislation to allow the authorities to use such devices in terrorism cases is being developed.

In the event that an operator or any company notified pursuant to the Law of 27 February 2011 on electronic communications networks and services uses data encoding, compression or encryption procedures, the information intercepted must be communicated to the legal authorities uncoded.

We do not have specialist centres, and there is no cooperation on decryption with private companies.

This is still a problem in the aforementioned, crucial areas, and in cases involving life-threatening situations.

Draft legislation to allow law enforcement authorities to use technical devices to capture data remotely before encryption is being discussed.

DECLASSIFIED

5.2.3 E - e v i d e n c e (electronic evidence)

It is possible to seize computer equipment hosting data that is the subject of an inquiry or judicial investigation using a criminal seizure in the conventional sense of the term, i.e. by legal sequestration of the property. However, there are essentially two problems with this pragmatic solution:

- the contentious data could be stored on a server hosting data owned by people other than the subject of the inquiry or investigation. This is the case of shared web-hosting services, involving a server that hosts the internet sites of many clients. Seizures affect not just the subject of the inquiry or investigation but also the host and any other people legitimately storing their sites on the server in question;
- seizures of computer equipment result in all content stored thereon being completely blocked. As the measure is not targeted, perfectly lawful content put online by the subject of the inquiry or investigation is also blocked.

Physical seizures of computer equipment can be a solution in cases involving the exchange of child pornography content by peer-to-peer connections initiated by individuals[8].

DECLASSIFIED

[8] See, inter alia, Luxembourg Administrative Court 23.03.2011, No 1059/2011; Luxembourg Administrative Court 07.10.2008, No 2822/2008; Luxembourg Administrative Court 24.06.2008, No 2126/2008; Luxembourg Administrative Court 06.11.2008, No 3150/2008.

With the Law of 18 July 2014[9], legislators defined seizures of '*data stored, processed or transmitted in an automated data processing or transmission system*' more specifically[10]. Articles 31, 33 (crimes and offences in the process of being committed) and 66 (seizures ordered by an investigating judge) now expressly provide for the seizure of computer data '*by the seizure of either the physical device on which the data are located, or a copy*'.

If a copy is made, the data used as evidence are saved onto a CD, DVD or hard disk, depending on the volume of data to be seized. In this sense, there are no specific restrictions on electronic evidence under Luxembourg law.

The criminal law rules on evidence are contained in the Code of Criminal Procedure. There are no specific admissibility conditions for electronic evidence.

5.3 Protection of human rights / fundamental freedoms

The fundamental rights deriving from, in particular, the ECHR and the EU Charter on Fundamental Rights are protected by the fact that the court system in Luxembourg guarantees effective recourse for any citizen whose fundamental rights have been infringed.

DECLASSIFIED

9 Law of 18 July 2014 1) approving the Council of Europe Convention on Cybercrime opened for signature in Budapest on 23 November 2001, 2) approving the Additional Protocol to the Convention on Cybercrime concerning the criminalisation of racist and xenophobic acts committed using computer systems, signed in Strasbourg on 28 January 2003, 3) amending the Criminal Code, 4) amending the Code of Criminal Procedure, 5) amending the amended Law of 30 May 2005 on the protection of privacy in the electronic communications sector.

10 Since the Law of 15 July 1993 to combat economic crime and computer fraud that inserted computer-related offences into the Criminal Code, legislators have used the term 'automated data processing or transmission system' to denote ‘computer systems' (the terminology used in the Budapest Convention) in the various criminal law texts.

More specifically, in relation to data protection the National Data Protection Authority (CNPD) must:

o monitor and check the legality of the collection and use of the data subject to processing and inform those responsible for processing it of their obligations;

o ensure respect for fundamental freedoms and rights, particularly privacy, and inform the public of the rights of those affected;

o receive and examine complaints and requests to check the lawfulness of processing;

o ensure the application of the amended Law of 30 May 2005 concerning the protection of privacy in the electronic communications sector and its implementing rules.

Articles 33 and 66 of the Code of Criminal Procedure allow the principal public prosecutor, in the case of on-the-spot investigations, and the investigating judge, in the case of judicial investigations, to delete data stored, processed or transmitted using an automated data processing or transmission system, provided that:

- a copy of the data is made beforehand,
- the physical device used to store, process or transmit the data is not seized,
- possession or use of the data is illegal or poses a threat to the security of people or property,
- the physical device (for example the computer or server) hosting the data is located in the Grand Duchy of Luxembourg.

DECLASSIFIED

In parallel to the evidential requirements, the requirement that a copy of the data be made before deletion allows those data to be retrieved in the event that the decision to delete is annulled by the 'Chambre du Conseil' or the trial court, that there is no case to answer, or that the suspect is acquitted by the trial court. As explained by legislators: 'the decision to delete data cannot be interpreted as a pre-emptive confiscation measure. It is a measure used either to protect people and property against further offences (particularly in cases involving malware), or to prevent the diffusion of illegal material (such as child pornography). In the event of an acquittal or a case that does not proceed to judgment, the (copy of the) data seized could be recovered. However, in the event of a successful prosecution, the data would be confiscated'.

Examination of the parliamentary proceedings shows that the intention of legislators was to make unlawful or dangerous data inaccessible pending a substantive judgment. Content that can be blocked includes 'child pornography, malware or incitement of hatred or terrorism'.

It is possible to appeal against all of these measures.

DECLASSIFIED

5.4 Jurisdiction

5.4.1 Principles applicable to investigations of cybercrime

Article 7-2 of the Code of Criminal Procedure provides that 'any offence, one of the acts corresponding to a constituent element of which was carried out in the Grand Duchy of Luxembourg, shall be considered to have been committed in the Grand Duchy of Luxembourg'.

The terms of this article have been clarified by case law as follows: 'the element to be taken into account as the localisation criterion is the material element. This element can be considered equally with respect to the tortious conduct and to the damage arising from the act' For the Luxembourg courts to have jurisdiction, 'it is sufficient, therefore, that an act corresponding to one of the elements of the offence occurred on national territory (...). It is therefore necessary to establish the place the offence was committed, that is to say to geographically locate the elements constituting the offence, keeping in mind that it is sufficient that either the act or the resulting damage occurred on Luxembourg territory for jurisdiction to be awarded to the Luxembourg courts'. It should also be noted that in the Court of Appeal judgment of 11 March 2008 it was held that the act corresponding to a constituent element must have been committed 'in its entirety' on Luxembourg territory for jurisdiction to be awarded to the Luxembourg courts.

It is clear from the case law on the application of this text that it is sufficient that the damage arising from the offence was suffered in Luxembourg for jurisdiction of the national courts to be established.

DECLASSIFIED

In relation to fraud, it was held that 'the national courts have jurisdiction in cases involving defendants of Luxembourg or foreign nationality who have committed fraudulent acts in the Grand Duchy that facilitate the commission of fraud abroad, or who have placed funds resulting from fraud committed abroad in Luxembourg'. The Luxembourg courts also have jurisdiction if 'the acts preparatory to the fraudulent act, or the receipt of the funds by the perpetrator, occurred in the Grand Duchy of Luxembourg (...), even if the contract was signed or the funds were fraudulently acquired abroad'. However, acts classified as preparatory to the fraudulent act such as its setting up, or the acts following restitution, are not acts corresponding to a constituent element of the offence as defined in Article 7-2 of the Code of Criminal Procedure.

The same rules apply to embezzlement, extortion, forgery and the use of forged documents and involvement with a criminal gang.

Since computer crime now constitutes an offence predicate to the offence of money laundering, Article 506-3 of the Criminal Code confers jurisdiction on the Luxembourg courts even if the predicate offence was committed abroad.

Moreover, the Budapest Convention provides that jurisdiction is also conferred if one of the offences it defines is committed by a Luxembourg national, provided either that the offence is also punishable in the place in which it was committed or that it does not fall under the jurisdiction of any state. This extension of the national courts' jurisdiction over offences committed abroad by Luxembourg nationals is governed by Article 5 of the Code of Criminal Procedure.

DECLASSIFIED

Legislators supplemented Article 7-4 of the Code of Criminal Procedure by providing that computer-related offences committed abroad can be prosecuted in Luxembourg provided that the suspect is not extradited by the relevant country. Luxembourg has thus raised computer crime to the level of areas subject to the 'aut dedere aut judicare' obligation (extradite or prosecute).

In parallel to the legal texts defining the jurisdiction of the Luxembourg authorities responsible for prosecutions, it is appropriate to mention the case law origins of the grounds of jurisdiction.
Firstly, cases of extension of jurisdiction occur 'where there is a link between offences committed in different jurisdictions that is so close that it is in the interests of the proper administration of justice that those offences be judged by the same judge (Encyclopédie Dalloz, Pénal, V compétence, No 254).

Those cases involving the extension of jurisdiction of national courts to offences committed abroad involve connexity and indivisibility, in respect of which a logical, more or less close link between several offences means that the court with jurisdiction to hear one also has jurisdiction to hear the others, even though that might not have been the case had the offences been considered individually (Roger Thiry, Précis d'instruction criminelle en droit luxembourgeois, T. I, No 375)'.

Extension of jurisdiction also occurs in cases involving an offence committed abroad during the same period of time, involving the same motive and with the same legal basis as the offences committed in Luxembourg. This is the case if there is a logical connection between an offence committed abroad and offences committed in the Grand Duchy of Luxembourg, to the extent that the latter would not exist were it not for the former.

DECLASSIFIED

Another ground for jurisdiction is collective offences, which feature 'a number of facts, each of which constitutes an offence, but which may form a single criminal activity because they are interlinked by virtue of their unified planning and a unified purpose'. In the case of a collective offence, 'a sufficient condition for Luxembourg's criminal courts to have jurisdiction is that any of the acts reflecting one of the constituent elements of the offence occurred in the Grand Duchy of Luxembourg, irrespective of whether the acts making up such constituent elements were committed by one person or several people.

5.4.2 Rules for conflicts of jurisdiction and referring matters to Eurojust

As part of the proper administration of justice, it is of course helpful to have the cases involving one suspect managed centrally by a single State, provided that is compatible with national legislation (territorial jurisdiction, extension of jurisdiction by consent and criminalisation).

The result could otherwise be contradictory judgments or, if it emerges that a person has been prosecuted simultaneously in several States for the same act, the *ne bis in idem* principle might apply.

In practice, States come to an agreement among themselves and use the central authorities (in Luxembourg, the Principal Public Prosecutor's Office) as a channel to report the facts in accordance with the proper procedure. Luxembourg also cooperates with Eurojust very frequently and is a member of Eurojust's Cybercrime Network.

DECLASSIFIED

The public prosecutor's office takes several factors into account when assessing whether it should report a case: the perpetrator's nationality and location, the victim's nationality, the seriousness of the harm suffered, the stage reached in the inquiry, the need to uphold the rights of the defence, etc.

Luxembourg has not implemented any cybercrime-related provisions in connection with Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings.

5.4.3 Jurisdiction for cybercrime offences committed 'in the cloud'

Article 33(5) and Article 66(3) of the Code of Criminal Procedure provide that 'seizure of data stored, processed or transmitted in an automated data processing or transmission system may be effected either by seizing the physical medium on which the data are stored, or by making a copy of the data'. Since the wording makes no distinction as to whether the data are located in Luxembourg or abroad, any data accessible from Luxembourg may be seized in the form of a copy.

However, the data may be deleted only if they are stored in Luxembourg.

The police have not come up against any specific problems in their cybercrime investigations.

DECLASSIFIED

5.4.4 Luxembourg's view on the legal framework for fighting cybercrime

According to the police, the tools available for international mutual legal assistance are too slow and are insufficient to combat cybercrime effectively. The ephemeral nature of online evidence and the variation in data retention periods from one State to another make the ability to react swiftly and flexible tools a must.

5.5 Conclusions

Luxembourg ratified the Council of Europe Convention on Cybercrime and the Additional Protocol thereto in 2014.

Luxembourg has also transposed Directive 2013/40/EU on attacks against information systems and Directive 2011/39/EU on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA.

The provisions on identity theft also apply to identity theft on social networks (there is already one piece of case-law in this area, with two convictions – one criminal and the other administrative).

DECLASSIFIED

Jurisdiction in such cases is established if any of the acts constitutive of the offence has been committed in Luxembourg. There is no requirement for the act to be criminalised in both States, nor for the victim to report it, nor for it to be officially reported.

The investigating judge may authorise the use of investigative techniques such as telephone tapping, undercover operations, special computing techniques, tracking of telecommunications or seizure of computer data. Rapid retention of data can be authorised by the police, the public prosecutor or the investigating judge. Content stored in the 'cloud' can be seized if the data are accessible from Luxembourg.

Practitioners consider that the legislation on child pornography is a satisfactory tool for their work.

A considerable number of legislative developments are currently under way (remote data capture, investigations under a pseudonym, reform of the intelligence service, etc.). It must be stressed that the reform of the intelligence service was completed after the evaluation visit. Otherwise, no changes to cybercrime legislation are in the offing at the moment.

DECLASSIFIED

6 OPERATIONAL ASPECTS

6.1 Cyber attacks

6.1.1 Nature of cyber attacks

The police base their cybercrime statistics on all incidents recorded on their computer system in the 'cybercrime' category. This category covers a range of offences: illegal interference with a computer system, online bank fraud, online scams, etc. Owing to the variety of activities included, it is impossible to provide exact figures for different types of cybercrime, such as 'cyber attacks'.
A total of 715 cases were recorded in the 'cybercrime' category in 2014 and 1 190 cases in 2015.

6.1.2 Mechanism for responding to cyber attacks

The High Commission for National Protection (Haut Commissariat à la Protection Nationale - HCPN) coordinates the response to cyber attacks. It also has a Cyber Risk Assessment Unit, known as CERC. Additionally, there are crisis management bodies: the Cyber Single Point of Contact (SPOC), the Cyber Risk Assessment Unit (CERC) and the Cyber Crisis Unit.

The police rely on mutual legal assistance instruments, direct exchanges of information within the limits imposed by national and international legislation, exchanges via Europol and Interpol, exchanges of personal contacts (between police services) and the voluntary provision of information by communications service providers.

DECLASSIFIED

6.2 Action to combat child pornography and sexual abuse online

6.2.1 Databases identifying victims and measures to avoid re-victimisation

Luxembourg does not have a database identifying victims.
As yet, no record has been kept of cases of victims in Luxembourg who appear in child pornography disseminated via the internet.

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

Luxembourg has adopted an article of legislation specifically to counter the phenomenon of 'grooming'.

Article 385-2 of the Criminal Code (Law of 16 July 2011) provides that the act of an adult making sexual propositions via an electronic means of communication to a minor aged under 16, or to a person claiming to be such, is punishable by between one month and three years imprisonment and a fine of between EUR 251 and EUR 50 000.

The same Article provides for more severe penalties, namely imprisonment of between one and five years and a fine of between EUR 251 and EUR 75 000, in cases where those propositions have been followed by a meeting.
The topic of grooming forms an integral part of the BEE SECURE awareness-raising sessions. A campaign dealing specifically with cyber-bullying took place in 2011 and another is planned for the 2016-17 school year, with fighting internet hate speech as its main theme.

DECLASSIFIED

6.2.3 Prevention of sex tourism, child pornographic performance etc.

The association ECPAT Luxembourg should be mentioned here. Its mission is to use all available legal means to combat the sexual exploitation of children for commercial ends, and to inform the public and raise their awareness about children's rights in this area. The association helps to identify vulnerable children and/or victims of sexual exploitation for commercial ends, along with their families; it is also involved in running programmes to support them.

Also worthy of mention is BEE SECURE, a joint initiative of the Ministry for Economic Affairs, the Ministry for Family Affairs and Integration and for the Greater Region, and the Ministry for National Education, Children and Young People. BEE SECURE is run by three partners: the National Youth Service, KannerJugendTelefon and securitymadein.lu.

The BEE SECURE initiative encompasses awareness-raising measures to encourage people to use information and communication technologies more safely.

BEE SECURE is a project part-funded by the European Commission, which serves as Luxembourg's Safer Internet Centre in the Europe-wide Insafe network. The national BEE SECURE Stopline help line, run by KannerJugendTelefon, is a member of the international INHOPE (International Association of Internet Hotlines) network.

The site childprotection.lu has been set up to raise public awareness of various forms of child sexual abuse and exploitation and to enable children to report suspected cases.

DECLASSIFIED

Kanner-Jugendtelefon (which operates the BEE SECURE Stopline) and the Grand Ducal Police cooperated with ECPAT Luxembourg (which launched the project) on a campaign to raise awareness about child sex tourism (via childprotection.lu and printed leaflets and posters).

The campaign included information for the general public about the legal framework and ways of reporting incidents. It also launched measures to cooperate with Luxembourg tour operators.

No cases of 'pornographic performances' have been uncovered by the judicial authorities in Luxembourg to date.

The BEE SECURE Stopline would be responsible for sending out alerts to enable the authorities to act as swiftly as possible.

The Financial Intelligence Unit works closely with payment and e-money institutions to detect transactions connected with this type of crime. Half a dozen suspicious transaction reports were received in relation to this subject in 2015. These were analysed in cooperation with the intelligence units in the countries concerned.

DECLASSIFIED

Steps are currently being taken to cooperate more closely with Europol in this area.

- Setting up hotlines and providing specific information on the procedure for lodging a complaint.

Persons wishing to provide information on or lodge a complaint concerning child sexual abuse on the internet can access a virtual police station via the site www.police.lu where they can file the complaint, which will be processed by specialist investigators as quickly as possible. The BEE SECURE Stopline site (stopline.bee-secure.lu) allows any citizen to report child sexual abuse content anonymously via an interactive form. These reports are then dealt with according to the operational procedures of the BEE SECURE Stopline and forwarded to the Grand-Ducal Police.

- Developing sources of information for children to help them use the internet safely.

Luxembourg's BEE SECURE organisation, operated by the National Youth Service, KannerJugendTelefon et securitymadein.lu, regularly organises information sessions for young people to raise their awareness of the risks they may face when using the internet.

- Developing tools for flagging harmful/illegal behaviour on the internet.

The BEE SECURE initiative has a platform, BEE SECURE Stopline at stopline.bee-secure.lu, for anonymously reporting illegal content on the internet such as child sexual abuse content, racist, revisionist and discriminatory content and terrorist content. For other illegal content, users can anonymously and confidentially contact the BEE SECURE Helpline on the free number 80021234.

DECLASSIFIED

6.2.4 Combating sites containing or disseminating child pornography: who does what

Article 33(5) and Article 66(3) of the Code of Criminal Procedure allow the deletion and hence the blocking of data the possession or use of which is illegal or endangers the safety of people or assets.

Content that can be blocked includes 'child pornography, malware or incitement of hate or terrorism'.

There are significant safeguards attached to that measure, in that it requires an order from the public prosecutor if the offence in question is in the process of being committed, and from an investigating judge in any other circumstances. Actions for annulment and restitution may be brought against such orders.

Kanner-Jugendtelefon operates the BEE SECURE Stopline and, in that capacity, is a member of INHOPE (the International Association of Internet Hotlines). The association's goal is to support and improve cooperation between different hotlines so that reports of child sexual abuse content are acted on quickly and effectively.

The BEE SECURE Stopline transfers child sexual abuse content notifications to the national authorities if the content is hosted in Luxembourg and to the international network INHOPE if the content is hosted in a country with an INHOPE network partner hotline. Notifications on racist, revisionist and discriminatory content and terrorist content are sent to national authorities.

DECLASSIFIED

The limited liability granted to hosts, as provided for by Article 62 of the law on electronic commerce, entails an obligation on them to act swiftly to remove or bar access to any illegal content stored on their infrastructure as soon as they become aware of it.

Generally speaking, hosts in Luxembourg block content which is manifestly illegal in the countries of the European Union. This includes child pornography and material which clearly incites hatred (particularly racial hatred) or acts of terrorism.

To ensure greater legal certainty, many hosts define illegal content in their general terms and conditions. This legal framework, established under private law, enables them to block artistic works placed on-line in breach of copyright or malware disseminated via their computer systems.

In the context of managing the reporting of illegal content, BEE SECURE Stopline and the service providers are regarded as reporting intermediaries between the public and the competent authorities. Thus as soon as illegal content is forwarded to the competent police service by BEE SECURE Stopline, the police take care of blocking or removing that content.

The private sector is cooperative when notified of illegal content, and as a rule that content is rapidly removed.

DECLASSIFIED

Hosts may become aware of illegal content by carrying out spot checks or through reports from interested parties. Mention should be made in this respect of BEE SECURE Stopline, to which anyone can report content related to child pornography, racism, revisionism, other forms of discrimination and terrorism. In the context of managing the reporting of illegal content, BEE SECURE Stopline has a collaboration agreement with the Criminal Investigation Department of the police which enables it to act as an intermediary and expert for the reception, analysis and transmission of information to the appropriate police services. The final decision on the legality or illegality of content reported to BEE SECURE Stopline and the decision to inform the host, if it is located in Luxembourg, is taken by the prosecution authorities (the Grand-Ducal Police or the public prosecutor's office). As a rule, BEE SECURE Stopline does not contact the host directly when illegal content is removed unless the Grand-Ducal Police asks it to do so.

Content is blocked as a result of the cooperation between the police authorities and the private sector, generally under the host's terms and conditions, which expressly reserve the right to remove illegal content from its systems.

If necessary, the public prosecutor can order content to be blocked on the basis of Article 33(5) and Article 66(3) of the Code of Criminal Procedure.

Article 62 of the law on electronic commerce obliges the host to remove or bar access to the information. On the basis of this Article, the provider could therefore decide to permanently remove the contentious data. In practice, the provider removes the data from the infrastructure accessible from the internet but keeps a backup copy. The data is thus blocked.

DECLASSIFIED

A collaboration agreement concerning the BEE SECURE Stopline service, which is part of the BEE SECURE initiative, exists between the Grand-Ducal Police, Luxembourg's National Youth Service (SNJ), and the Kanner-Jugendtelefon (KJT). Whenever this service discovers an illegal site or is informed of the existence of such a site by its international counterparts, it informs the competent police services. The police services undertake to remove or block the site in question within a fairly short period of time (ideally within 48 hours if possible from the standpoint of the investigation).

In the case of child sexual abuse material on hosts in other countries, BEE SECURE Stopline's operational procedures require that the Grand-Ducal Police be informed and that the links concerned be forwarded to a partner hotline within the INHOPE network (International Association of Internet Hotlines). In this context it should be noted that INHOPE shuns the term 'child pornography' and prefers the expression 'child sexual abuse material' (or 'content pertaining to sexual violence against children').

The aim of the work of the BEE SECURE Stopline and the INHOPE network is to remove child sexual abuse content as fast as possible in order to avoid the re-victimisation of the children and adolescents shown in the pictures and videos ('notice and take down').

In cases where the server is located outside Luxembourg and in a state with an INHOPE (International Association of Internet hotlines) partner hotline, the BEE SECURE Stopline agency forwards the data to its relevant international counterparts and to the Grand-Ducal Police. If the server is outside Luxembourg and in a state with no INHOPE partner hotline, the BEE SECURE Stopline sends the data to the Grand-Ducal Police and to the INHOPE ICCAM database. In an emergency or in the case of a major or unique event, the police authorities inform their European counterparts via the Interpol/Europol systems of the illegal content that has been found.

DECLASSIFIED

The BEE SECURE Stopline transfers child sexual abuse content notifications to the national authorities (content hosted in Luxembourg) if the content is hosted in Luxembourg and to the international network INHOPE (content hosted abroad) if the content is hosted in a country with an INHOPE network partner hotline. Notifications on racist, revisionist and discriminatory content and terrorist content are sent to national authorities.

Luxembourg's public prosecutor's office has three judges who, in addition to dealing with youth cases, have particular responsibility for child pornography cases.
Within the police, the SPJ's youth protection unit also has special responsibility for these cases.

ECPAT and BEE SECURE are responsible for detecting such content, informing the general public and reporting the facts to the judicial authorities.

6.3 On-line card fraud

As a general rule, credit card companies (Six Payment, formerly Cetrel) 'require' their customers to lodge complaints with the police in order to obtain reimbursement of misappropriated sums of money, so there is a large number of complaints.

Apart from that, many companies providing payment systems (such as PayPal) or online purchasing and sales (like Amazon), as well as banks, declare suspected instances of money laundering to the Financial Intelligence Unit, which in turn sends reports to the public prosecutor's office.

DECLASSIFIED

Luxembourg is actively involved in exchange projects supported by the European Commission aimed at ensuring the fastest possible communication of data relating to e-commerce to the Member States involved. One such project, 'FIU.net Crossborder Reporting', has been operating since January 2015.

The main participants working out of Luxembourg were responsible for more than 7 500 exchanges between 1 January and 30 April 2016 with other countries (statistics established by Europol, the manager of FIU.net).

Banks and e-payment and e-money institutions must abide by the provisions laid down in the law of 12 November on combating money laundering and the financing of terrorism, which transposed Directive 2001/97/EC of the European Parliament and of the Council amending Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering (hereinafter the 'ML/FT law').

The Intelligence Unit is active at international level in exchanging information to ensure that the Member State concerned receives conclusive information as rapidly as possible.

- Increase the security of non-cash payment and minimise the vulnerability of magnetic strips

E-payment and e-money institutions must apply the due diligence measures imposed by the ML/FT law. The analysis of transactions carried out by the Financial Intelligence Unit has shown that in very many cases fraudulent transactions are blocked before the criminal receives the profit he or she expected.

- Strengthen the procedures for authorisation of on-line transactions and authentication of customers

DECLASSIFIED

Introduction of the '3D secure' system, also known commercially as 'Verified By Visa' and 'MasterCard SecureCode'.

Measures to make electronic data and on-line transactions secure have also been strengthened by the entry into force of the law on electronic commerce of 14 August 2000 and the Grand-Ducal Regulation on electronic signatures which lays down the features that such signatures have to incorporate to be recognised as legal (1 June 2001).

The setting up of LuxTrust S.A., two-thirds of whose capital is held by the State, produced a common electronic security solution which is used not only by the Luxembourg government but also by the most influential banks in Luxembourg.

This solution operates on the basis of personal authentication certificates issued by LuxTrust as the certifying authority. It is thanks to these certificates that LuxTrust can guarantee the identity of the person who uses one of its products to log on to an on-line application to carry out electronic operations.

Generally speaking, reciprocal cooperation between authorities and issuers is shown to be satisfactory.

DECLASSIFIED

6.4 Conclusions

While responding to the sexual exploitation of children is straightforward, via BEE SECURE and its partnership with the hosts, discussions with the hosts on other topics, such as cyberattacks and bank card fraud, are less productive.

The youth prosecutor's office has jurisdiction over all child pornography offences. It consists of five investigating judges who are specialists in this type of offence. Reports and complaints come from third parties, parents or teachers. In 90 % of cases, the offenders are convicted. Current legislation does not allow investigators to act in place of the victim, but a draft law will allow a pseudonym to be used in proceedings in the future.

Although it is needed, no psychological monitoring of the investigators involved in the protection of children is provided.

In the fight against the sexual exploitation of children, Luxembourg is an interesting example, both from the point of view of the criminal justice response and because it also takes account of representations of children (images and virtual representations).

However, the absence, due to the legal framework in place, of monitoring by the relevant police services prevents proactive detection. In addition, the lack of cross-checking tools and databases designed to avoid re-victimisation could undermine the operational efforts undertaken in this regard.

DECLASSIFIED

The fight against on-line card fraud suffers from the same structural problems relating to the lack of specialist investigators.

There is no monitoring system (such as peer-to-peer mapping or cyber patrols) within the police to detect on-line offences.

According to police authorities, the most frequent bank card offences are fraud, forged cheques and fake bank transfer orders. Mutual legal assistance is considered to be too slow and inadequate, whereas Europol's communication platform is highly valued.

DECLASSIFIED

7. INTERNATIONAL COOPERATION

7.1 Cooperation with EU Agencies

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

There are no particular formalities to be complied with for cooperation between Luxembourg's national authorities and Europol/EC3, Eurojust and ENISA regarding cybercrime. However, these authorities must always comply with Luxembourg national law.

Cooperation generally takes place via an investigating judge.

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

- SECURITYMADEIN.LU is collaborating with Europol on a project dedicated to fighting phishing attacks: EU-PI - https://phishing-initiative.eu/
- At ENISA, as part of the CERT support programme, regular exchanges take place with CIRCL, GOVCERT and the other CERT teams in Luxembourg.

Luxembourg is a member of Eurojust's Cybercrime Network.

The police cooperate on an ongoing basis with Europol/EC3, exchanging as much information as possible. This is exemplified by two cases; the first is an older case, while the second is more recent and is part of an ongoing investigation.

DECLASSIFIED

1. Citadel botnet

In 2013, information from Europol led to the seizure of C2 servers used by the Citadel botnet. Moreover, operation of the seized equipment was facilitated by the technical details supplied by Europol.

2. Currently, the Grand Duchy, like many other countries, is affected by the Dridex banking Trojan. Constant exchange of material brought to light by the analyses undertaken has helped to establish several links to cases in other countries.

The various meetings organised at Eurojust facilitate the exchanging of good practice in investigating cybercrime. The personal knowledge of the actors in the field helps to identify the correct procedures and to address requests directly to the right person.

Cybercrime is an international phenomenon and the fight against this type of crime can only be won by means of a constant and smooth exchange of information. The Grand Duchy, which has a sizeable banking sector and a growing IT sector, can only benefit from the opportunities for cooperation provided by institutions such as Europol.

Luxembourg does not participate in the European Union Strategic Group of the Heads of National High-Tech Crime Units at Europol or in other forms of practical cooperation (including 'cyber patrols').

DECLASSIFIED

7.1.3 Operational results of the JITs and cyber patrols

The law enforcement authorities exchange information. In 2014 and 2015 the Grand Duchy actively took part, with France and Belgium, in a mixed investigation group under the aegis of a 'joint investigation team'. This operation led to the arrest of the members of a criminal network engaged in large-scale fuel diversion operations.

7.2 Cooperation between the Luxembourg authorities and Interpol

At this point in time, Luxembourg, i.e. the SPJ's youth protection unit, has competence in the matter and does not use Interpol's ICSE (International Child Sexual Exploitation) database for national investigations. The unit has access to the ICSE and is therefore obliged, in principle, not only to consult the database regularly, but also to transmit illegal material (e.g. child pornography and hash values) obtained during court proceedings, so that attempts can be made to identify the victims and the potential perpetrators by way of international cooperation.

7.3 Cooperation with third countries

As far as policy regarding third countries on prevention of cybercrime and investigations is concerned, the public prosecutor's office forwards the cases in which an account held by a third party has been revealed, but where the perpetrator is not known and cannot be identified, to the Financial Intelligence Unit, which notifies its counterpart in the country concerned so that measures can be taken to block or close the account in question.

DECLASSIFIED

Furthermore, cases of online credit card fraud are generally forwarded to the General Crime Section of the SPJ for centralisation and processing of the information compiled within Eurojust/Europol, with a view to a major investigation in this area.

Provision is also made for forwarding to Interpol cases of 'Nigerian' scams ('sexting' or 'sextape'), in which an IP address in a third country has been identified, so as to alert the third country concerned to the offence and to highlight any overlaps at international level.

Europol/EC3/Eurojust represent an important added value with regard to coordination between the different institutions of third countries in major cases and for the exchange of information.

7.4 Cooperation with the private sector

The local branches of private companies cooperate on a voluntary basis with regard to BSI (basic subscriber information). However, they do not communicate information if they consider that it has no link to Luxembourg. When applicable, in order to seize such BSI data and the content, or in the event of failure to cooperate, the PGD is obliged to ask the investigating judge to issue international letters rogatory, which considerably slows down the results.

In particular, Luxembourg takes part in the FIU.net Cross-border system. It is also represented in Eurojust and Europol.

DECLASSIFIED

7.5 Instruments of international cooperation

7.5.1. Mutual legal assistance

(a) Insofar as mutual legal assistance with cybercrime most often entails the communication of data held by third parties (for example, banking data, data regarding the identification of the holder of an internet account or of an IP address) and requires coercive acts to be implemented, it is the amended Law of 8 August 2000 on international legal assistance in criminal matters which applies. This law is applicable to any request for mutual legal assistance in criminal matters intended to enforce in the Grand Duchy a seizure of items, documents, funds or goods of any kind, a search or any other investigation presenting a similar level of constraint.

The Law of 8 August 2000 applies with regard to:

– the judicial authorities of requesting States which are not linked to the Grand Duchy of Luxembourg by an international agreement on mutual legal assistance;

– the judicial authorities of requesting States which are linked to the Grand Duchy of Luxembourg by an international agreement on mutual legal assistance, unless the provisions of this Law are inconsistent with those of the international agreement; and

– an international judicial authority recognised by the Grand Duchy of Luxembourg.

(b) If the request for mutual legal assistance does not entail, for its implementation, any coercive acts (for example, hearing of a person, communication of police reports, communication of data appearing in the databases of police or judicial authorities, communication of public data), it is implemented on the sole basis of the international conventions and, in their absence, on a reciprocal basis.

DECLASSIFIED

For requests from abroad for mutual legal assistance in criminal matters, the procedure to be followed varies according to whether or not the request for mutual legal assistance entails the implementation of coercive measures.

(a) In the first case, the Law of 8 August 2000 on international legal assistance in criminal matters is applicable, and the request for mutual legal assistance must be addressed to the Principal Public Prosecutor's Office at the Supreme Court of Justice, which is the central authority in Luxembourg responsible for receiving requests for mutual legal assistance the execution of which entails coercive acts.

The Principal Public Prosecutor's Office forwards the request for mutual legal assistance, accompanied by its opinion based on the Law of 8 August 2000, to the public prosecutor's office at the district court with territorial jurisdiction for the place in which the request for mutual legal assistance must be enforced (Luxembourg or Diekirch district court). The public prosecutor's office then brings the matter before the investigating judge for the purpose of executing the request for assistance.

For the purpose of transmission to the requesting authority of the documents seized in executing the request for assistance, the public prosecutor's office must notify the pre-trial chamber of the district court of requisitions to that effect. The pre-trial chamber rules on the lawfulness of the procedure and the transmission to the requesting authority of papers and documents seized. This decision cannot be appealed.

(b) In the second case, the request for mutual assistance is executed directly by the public prosecutor's office of the district court with territorial jurisdiction, which forwards the case to the police for execution of the requested duties, without going through the central authority.

As for requests sent abroad for mutual legal assistance in domestic criminal matters, these are drawn up either by the public prosecutor's offices, in the case of a preliminary investigation, or by the investigating judge, in the case of a preparatory inquiry.

DECLASSIFIED

Such requests are most often sent directly to the judicial authority of the requested State (where international conventions provide for this communication channel); otherwise they are forwarded to the requesting judicial authority through official channels, via the Principal Public Prosecutor's Office, with, if necessary, the assistance of the Ministry of Justice and the Ministry of Foreign Affairs.

The requests for mutual legal assistance are received and sent by post, by email or by fax.

It should also be noted that Luxembourg has an Asset Recovery Office (ARO) which is responsible for receiving, via the SIENA program (installed by Europol), the requests for information prior to sending off a request for mutual legal assistance.

The conditions differ according to whether or not the request for mutual legal assistance entails the implementation of coercive measures.

If the execution of a request for mutual assistance does not entail any coercive obligations, it is effected without any further conditions.

If the execution of a request for mutual assistance entails coercive obligations, the Law of 8 August 2000 on international legal assistance in criminal matters is applicable, and the request for mutual assistance must, unless more favourable provisions are laid down in the international conventions, satisfy the following conditions (Article 5 of the Law of 8 August 2000):

- it must be from a judicial authority competent under the law of the requesting State;
- it must be possible to categorise the act on which the request is based as a crime or offence punishable by a prison term of at least one year maximum under Luxembourg law and the law of the requesting State;

DECLASSIFIED

- the subject of the request must not have been tried in the Grand Duchy of Luxembourg for the same offence;
- it must be possible for the Luxembourg judicial authorities to take the requested measure pursuant to Luxembourg law, for the purpose of investigation or prosecution, as if it were a similar domestic case;
- the statutory time limitation must not have expired, under either Luxembourg law or the law of the requesting State.

From a formal perspective, the request for mutual assistance must contain the following information (Article 4 of the Law of 8 August 2000):

- the authority making the request;
- the subject and reason for the request;
- the date and the place where the offences were committed, a summary of the facts and the link between those facts and the subject of the investigation requested;
- as far as possible, the identity and nationality of the person concerned;
- the name and address of the addressee, if applicable;
- the text of the charge and of the associated penalties;
- a translation into French or German of the request for mutual assistance and of the documents to be submitted.

DECLASSIFIED

The request for mutual assistance may, in addition, be refused on the decision of the Principal Public Prosecutor's Office in the following cases (Article 3 of the Law of 8 August 2000):

- if the request for mutual assistance is likely to undermine sovereignty, security, law and order or other vital interests of the Grand Duchy of Luxembourg;
- if the request for mutual assistance relates to offences which may be categorised by Luxembourg law either as political offences or as offences linked to political offences;
- If the request for mutual assistance relates to offences in connection with taxes or duties, customs and exchange, pursuant to Luxembourg law.

The request for mutual assistance may also be refused (Article 4 of the Law of 8 August 2000, condition of proportionality) if, without having to carry out a thorough examination, it can be anticipated that the means to be implemented are not suited to achieving the objective referred to in the request for mutual assistance or go beyond what is necessary to achieve it.

It should be noted that several international conventions to which Luxembourg is party provide for more flexible conditions of application:

For instance, pursuant to the Schengen Convention,

- the offence on which the request is based must be punishable by imprisonment for a maximum term of only six months at least, pursuant to Luxembourg law, instead of one year laid down by the above Law,
- the condition of proportionality laid down in Article 4 of the Law of 8 August 2000 and that of the statutory time limitation laid down in Article 5 are not applicable.

DECLASSIFIED

The transmission to the requesting authority of the seized documents and items requires the agreement of the pre-trial chamber of the district court, which at the same time rules on the lawfulness of the procedure by an order which is not subject to appeal. It rules within a period of 20 days of referral.

Article 8 of the Law of 8 August 2000 stipulates that requests for mutual legal assistance should be given priority as matters of urgency.

Article 2 of the Law of 8 August 2000 states that, if the case appears serious and there is urgency owing to the danger of loss of validity of evidence, the judicial authority may proceed to carry out the investigation requested without first forwarding the request to the Principal Public Prosecutor.

Requests for mutual assistance entailing coercive measures are generally executed within a few months.

For very urgent requests (immediate risk of damage to life or physical integrity), there have been cases whereby the procedure has been executed and the case papers have been communicated to the requesting authority (electronically) within 24 hours.

The most frequent kinds of action are requests for identification of holders of electronic accounts or of IP addresses.

DECLASSIFIED

The most frequent cybercrime offences forming the basis for the mutual assistance are the following:

- abuse of payment cards or of electronic accounts in connection with online payments,
- online scams,
- online consultation of child pornography,
- extortion (threat to reveal compromising video recordings made by webcam).

To ensure that their request for mutual assistance satisfies the conditions required by Luxembourg legislation, certain countries (Japan, for example) systematically send the central authority a draft request for mutual assistance, informally and electronically, to obtain its advice.

Informal consultations with the competent authorities of another Member State sometimes take place during major investigations. In this case, the channels used are either personal contacts or channels made available by Europol/Interpol.

At an informal level, the European (TF-CSIRT - https://www.terena.org/activities/tf-csirt/) and international networks of CERTs (FIRST - https://www.first.org/) constitute an efficient and useful tool in terms of mutual assistance, detection and prevention of cyber attacks.

DECLASSIFIED

Mutual assistance with cybercrime is granted particularly on the basis of the following treaties:

Multilateral conventions:

- Budapest Convention on Cybercrime of 23 November 2001,
- European Convention on Mutual Assistance in Criminal Matters of 20 April 1959,
- Schengen Convention of 14 June 1985,
- Mutual Legal Assistance Convention.

Bilateral conventions:

- Treaty between the Government of the Grand Duchy of Luxembourg and the Government of the United States of America on Mutual Legal Assistance in Criminal Matters of 13 March 1997,
- Treaty between the Grand Duchy of Luxembourg and Australia on Mutual Assistance in Criminal Matters of 24 October 1988.

In the absence of treaties, mutual assistance is granted on the basis of reciprocity and subject to the conditions laid down in the Law of 8 August 2000.

The police rely on mutual legal assistance instruments, direct exchanges of information within the limits imposed by national and international legislation, exchanges via Europol and Interpol, exchanges of personal contacts (between police services) and the voluntary provision of information by communications service providers.

DECLASSIFIED

7.5.2 Instruments of mutual recognition

Luxembourg has not used the EU's mutual recognition instruments in relation to prevention, investigation and prosecution of cybercrimes.

7.5.3 Surrender/Extradition

Under Luxembourg law, the European arrest warrant is governed by the Law of 17 March 2004 on the European arrest warrant and the surrender procedures between Member States of the European Union.
It must be pointed out that there are no specific arrangements for cybercrime offences, which, furthermore, may in general form the basis for a European arrest warrant on condition that they are punishable with a maximum period of at least 12 months' imprisonment where the warrant is issued for prosecution and, where a sentence has been passed or a detention order has been made, for sentences of at least four months.

Furthermore, it should be noted that cybercrime is among the offences allowing for the execution of a European arrest warrant without verification of double criminality.

Articles 4 and 5 of the Law of 17 March 2004 stipulate the cases in which execution of the warrant may be refused.

The execution of the European arrest warrant falls within the jurisdiction of the public prosecutor's office which forwards it to the police for notification and execution.

DECLASSIFIED

Within 24 hours of notification, the person must be brought before the investigating judge, who, following a brief interrogation, issues a warrant for ‘retention in custody'.

The procedure then differs according to whether or not the person concerned is in agreement with his or her surrender.
If the person is in agreement, he or she must be surrendered to the requesting authority within ten days.

If he or she is not in agreement, the public prosecutor's office must refer the matter by way of requisition to the pre-trial chamber of the district court, which must then decide on the surrender within 20 days.

Exchanges between the requesting and requested authorities issuing the warrants (investigating judge, public prosecutor's office and police as executing department) are direct (by telephone, email, post).

There is no provision for any specific procedure with regard to requests linked to cybercrime.
Article 6 of the Law of 17 March 2004 stipulates 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.

The wanted person may then be arrested provisionally on the basis of the alert referred to in the previous paragraph without the arrest warrant having been issued.

However, the person will have to be brought before the investigating judge within 24 hours, failing which he or she must be released.

In theory, the person could also be held in police custody for four hours.

The response time depends on whether or not the person has been brought before the authorities and whether the file is complete.

DECLASSIFIED

7.6 Conclusions

With regard to cooperation with third countries, the national authorities reported that it has been attempted with certain African countries but has proven unsuccessful.

With regard to cooperation with the private sector, other problems were raised in relation to cooperation with certain major ISPs. The United States of America is often unwilling to provide data on hate crimes, invoking the right to freedom of expression.

Given that the majority of requests from abroad require judicial authorisation to obtain information for the reply, international letters rogatory are considered quicker and more efficient than requests for mutual assistance.

The police authorities also made the suggestion that it would be useful to establish an EU contact point for relations with big multinationals. Although Europol already provides this service, it should be promoted more effectively.

Despite the size of the country, and in proportion to the resources available, police involvement in international collaboration with Europol via the EMPACT, EUCTF and ECTEG groups could be stepped up.

DECLASSIFIED

8 TRAINING, AWARENESS-RAISING AND PREVENTION

8.1 Specific training

The Academy of European Law (ERA) offers training on this subject. The New Technologies Section of the SPJ provides training for judges, especially presentations on new tools used by cyber criminals (Darknet, bitcoin, etc.).

Microsoft has also already organised training for judges from the public prosecutor's office.

The Intelligence Unit actively participates in Egmont working groups to learn about the risks associated with the use of new technologies in the financial sector (bitcoin, online payment, mobile payment, etc.).

At the police college, cybercrime is covered during basic training and professional development for police officers and investigators.

There are no special training courses for IT forensic experts or investigators working on cybercrime cases.

DECLASSIFIED

Because it requires special courses, the New Technologies Section arranges and coordinates its own technical training. This is mainly training provided free of charge or at a reduced cost by Europol, Interpol or neighbouring police agencies, which is attended by members of the NT Section. Since specialist training offered by the private sector is usually expensive, as far as possible only one member of the NT section will attend and then pass on the knowledge to others. Internal training sessions are therefore organised four or five times a year to share what has been learned.

For judges, professional development is offered under the framework contracts concluded between the National School for the Judiciary (France) and Luxembourg. Training is also offered by the ERA in Trier. The Principal Public Prosecutor's Office acts as a coordinating authority as regards training for judges. Luxembourg also participates in the EJTN (European Judicial Training Network).

The annual cost of training the Grand Ducal Police on cybercrime is approximately EUR 15 000.

The University of Luxembourg does not offer specific courses on cybercrime. However, it does organise conferences on the subject.

In addition, the University of Luxembourg offers a professional Master's in information systems security management and the vocational high school offers cybersecurity programmes as part of its Advanced Technician's Certificate in IT.

DECLASSIFIED

8.2 Awareness-raising

Every year the BEE SECURE initiative raises awareness among 10 000 primary and secondary school pupils, as well as parents, teachers and youth workers, through information sessions and targeted training. The annual BEE SECURE campaigns also help to raise awareness among the general public about a specific subject.

An awareness-raising programme for older people was launched in 2014 under the name Silver Surfer, in cooperation with the Ministry of Family Affairs.

The BEE SECURE initiative is designed for youngsters, as well as trainers/teachers, people working with this age group and, of course, parents. Launched in 2013, the illustrated 'Bibi and friends' stories are aimed at children aged five to eight. The project also won the 2015 European Crime Prevention Award from the European Crime Prevention Network.

DECLASSIFIED

8.3 Prevention

8.3.1 National legislation/policy and other measures

GOVCERT is not responsible for prevention. The state has entrusted this responsibility to the National Agency for Information Systems Security (ANSSI), which is supported in its efforts by CASES.

Since CASES was set up in 2003 as part of the strategic plan for communication and information systems security, a policy of prevention, awareness-raising and security training has been pursued.

This resulted in the BEE SECURE initiative, which raises awareness among 10 000 primary and secondary school pupils every year as well as parents, teachers and educators, with targeted information and training sessions. BEE SECURE's yearly campaigns also raise awareness among the general public on a specific theme.

An awareness-raising programme for older people was launched in 2014 under the name Silver Surfer, in cooperation with the Ministry of Family Affairs.

CASES focuses on initial and continuing training for state officials and offers its services to the private sector, in partnership with training centres (e.g. House of Training).

CIRCL supports and trains operational teams in incident response and intrusion detection techniques.

DECLASSIFIED

8.3.2 Public-private partnership (PPP)

CERT.LU is a shining example of a CERT public-private partnership in Luxembourg. It consists of 11 entities, four from the public sector and seven from the private sector.

The BEE SECURE campaigns, which are organised annually, are widely supported by the private sector in terms of message delivery.

DECLASSIFIED

8.4 Conclusions

Luxembourg has a wealth of experience that it would be useful to share more widely with the other Member States and the institutions.

BEE SECURE, which is part of INHOPE, is a joint project between a number of ministries, led by a an interministerial committee. BEE SECURE organises awareness-raising sessions for children, parents and adults, at the request of communes or schools. These campaigns focus on a different theme every year. In 2015-2016, the topic chosen was called 'Clever cloud user'. A workshop for children also aims to teach them safe online behaviour.

The BEE SECURE helpline provides internet services and actively participates in ICCAM within the framework of information exchange between different helplines focusing on child sexual abuse content. The BEE SECURE helpline also has an operational agreement with the Luxembourg police to filter websites.

A phone line – KJT – is available to children and young people seeking assistance. KJT also has a website on which illegal online content (child sexual abuse, racism, discrimination, terrorism) can be anonymously reported.

DECLASSIFIED

SecurityMadein.lu is another website dedicated to awareness-raising and prevention activities. Its three areas of activity are Aware, CASES and CIRCL.

As an example, on the day of the visit, six sessions for older people had already been organised (with a total of 100 participants) as part of the Silver Surfer project, as well as 11 events for children (with over 500 participants).

DFIR, a CERT focusing on companies, organises monthly breakfasts for around 50 participants.

Besides the MONARC project, CASES also organises prevention and support activities for companies, including training for the public sector. Ad-hoc activities are organised for the municipal administrations (risk analysis, implementation of the security charter and training).

CIRCL, which was established in 2007 and focuses on the communes and the private sector, takes a pragmatic, open and innovative approach to prevention. In addition to the above projects, BGP Ranking, MISP and others, CIRCL has led 1 400 technical investigations on the basis of incident reports it has received.

DECLASSIFIED

9 FINAL REMARKS AND RECOMMENDATIONS

9.1 Suggestions from Luxembourg

Luxembourg recognises the importance of the internet for the economy and has equipped itself with numerous means of prevention, detection and response. Cooperation and coordination function thanks to the tools, services and methods made available to the relevant people, but also thanks to the events organised to consolidate cooperation in this area.

Examples of good practice include:

- MONARC, a risk analysis method that promotes collaboration, thereby reducing individual efforts expended on risk analysis by 80 %;
- BGP Ranking (a tool for compiling blacklists and evaluating the malicious potential of autonomous systems), the HCPN and the emergency intervention plan;
- MISP, a platform for exchanging compromise indicators;
- the large-scale awareness-raising campaigns carried out by CASES and BEE SECURE (over 60 % of the population are familiar with BEE SECURE);
- compulsory and optional awareness-raising sessions in schools;
- the CERTs.

The following are a number of suggestions made by Luxembourg to strengthen the fight against cybercrime:

- create a European contact point, and establish common rules and procedures for exchanging data with the major communications service providers outside the EU;
- facilitate and accelerate the execution of international letters rogatory;
- create a common, uniform taxonomy for cybercrime classification and statistics;
- reinforce cooperation with the private sector and academia;
- create a reference model by defining minimum standards for the structure and functioning of the investigative units working on cybercrime, cyber-patrols and cyber-prevention.

DECLASSIFIED

9.2 Recommendations

Luxembourg should follow up on the recommendations in this report 18 months after the evaluation and report on the progress made to the Working Party on General Matters including Evaluation (GENVAL).

The evaluation team deems it appropriate to make a number of suggestions to the Luxembourg authorities. It also puts forward recommendations based on the various good practices to the EU, its institutions and agencies, and especially Europol.

9.2.1 Recommendations to Luxembourg

Luxembourg should:

1. create and build up more consolidated statistics that would provide a better understanding of cybercrime;
2. further develop the operational part of the national cybersecurity strategy;
3. equip itself with the legal and technical tools to carry out infiltration operations and undercover investigations in cyberspace;
4. establish the legal basis to enable sites with illegal content to be blocked;
5. increase staff numbers at the Criminal Investigation Department to allow for cross-cutting approaches and specialisations;
6. contribute to international databases on victims of child pornography;

DECLASSIFIED

7. continue and reinforce international judicial and police cooperation, especially with respect to information exchange;
8. continue to deliver training to investigators and public prosecutors on aspects of crime relating to IT techniques, including by contributing to the synergies provided by ECTEG, CEPOL and Interpol;
9. offer structured psychological support to police officers dealing with child pornography cases.

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

The Member States should take inspiration from the good practices identified by the evaluation team in Luxembourg, i.e.:

- the excellent collaboration between the public sector and private sector;
- the existence of public prosecutors specialising in cybercrime;
- the recruitment of and career path for specialists in new technologies;
- the dynamism in research and development and the sharing of results with the various stakeholders;
- the law enforcement policy on child pornography;
- the holistic approach to awareness-raising;
- the role of the institutions in finding data leaks (especially CIRCL).

9.2.3 Recommendations to Eurojust/Europol/ENISA

Europol should:

- promote the services available to Member States better.

DECLASSIFIED

ANNEX A: PROGRAMME FOR THE ON-SITE VISIT

Programme for the on-site- visit carried out in Luxembourg on 7 to 9 June 2016

Monday 6 June 2016

Arrival of experts in Luxembourg

Tuesday 7 June 2016

8.30 Departure of experts from hotel (transported by Grand-Ducal Police)

9.00-12.00 Meeting room of the Principal Public Prosecutor's Office (judicial precinct)

- 9.00-9.10 Experts welcomed by the Principal Public Prosecutor
- 9.10-10.30 General introduction on the evaluation and explanation of Luxembourg's measures on cybercrime and cybersecurity (round table discussion with representatives of all the bodies involved in the evaluation)
- 10.30-10.45 Coffee break
- 10.45-11.15 Presentation of Luxembourg's measures on cybersecurity (F. Thill)
- 11.15-12.00 Legal texts and implementation of the Budapest Convention

12.00-14.00 Lunch break

14.00 -18.00 Meeting room of the Principal Public Prosecutor's Office (judicial precinct)

- 14.00-14.30 Measures taken by the public prosecutor's office on cybercrime
- 14.30-15.30 Mutual legal assistance on cybercrime
- 15.30-15.45 Coffee break
- 15.45-16.30 Presentation on hate speech on the internet
- 16.30-17.00 Presentation on child pornography on the internet
- 17.00-18.00 The Financial Intelligence Unit (CRF) and cybercrime; training of magistrates

18.00 Return of experts to hotel

DECLASSIFIED

Wednesday 8 June 2016

8.30 Departure of experts from hotel

9.00-13.00 Meeting room of the Criminal Investigation Department, rue de Bitbourg, Hamm

- 9.00-9.15 Presentation of organisation chart
- 9.15-9.45 International cooperation
- 9.45-10.00 Coffee break
- 10h00-10h20 Bank card fraud
- 10.20-10.40 Online scams
- 10.40-10.55 Coffee break
- 10.55-12.00 Training
- 12.15-12.45 Cybercrime investigations: one example
- 12.45-13.00 Summary and question-and-answer session

13.00-14.30 Lunch break

14.30-18.00 Meeting room of the SNJ (National Youth Service), 138 bd. de la Pétrusse

- 14.30-14.50 Presentation of public awareness-raising activities (BEE SECURE)
- 14.50-15.20 Presentation of BEE SECURE Stopline: anonymous site for reporting illegal content found on the Internet
- 15.20-15.40 Presentation by SecurityMadein.lu
- 15.40-16.10 Presentation of prevention and support activities for companies (CASES)
- 16.10-16h.30 Coffee break
- 16.30-17.30 Presentation of the work and players involved in IT incident response activities – CERT.LU, CIRCL, GOVCERT and NCERT.
- 17.30-18.00 Presentation of ANSSI (National Agency for the Security of Information Systems)

18.00 Return of experts to hotel

DECLASSIFIED

Wednesday 09 June 2016

8.30 Departure of experts from hotel

9.00-12.00 Meeting room of the Ministry of Justice

- Closing session of the evaluation visit (with representatives of all the bodies involved in it)
- Opportunity for experts to discuss some matters in more detail

12.00 End of evaluation visit

ANNEX B: LIST OF PARTICIPANTS

Luxembourg experts

(a) Coordination

Mr Laurent THYES
Ministry of Justice

Ms Nina BURMEISTER
Media and Communications Unit

(b) Participants

. Prosecuting authorities

Ms Martine SOLOVIEFF, Principal Public Prosecutor's Office Mr Jeannot NIES, Principal Public Prosecutor's Office Mr Marc HARPES, Principal Public Prosecutor's Office Ms Dominique PETERS, Public Prosecutor's Office Mr Max BRAUN, Public Prosecutor's Office Mr Gabriel SEIXAS, Public Prosecutor's Office Mr Jim POLFER, Public Prosecutor's Office

. Police authorities

Mr Alain KLEULS
Mr Jeff MULLER
Mr Michel CONRAD
Mr Georges GESCHWINDT
Mr Guy VONCKEN
Mr Pascal ENZINGER
Mr Claude WEIS

DECLASSIFIED

. CASES (Cyberworld Awareness and Security Enhancement Services)

Mr François THILL

. ANSSI

Mr Gérard CAYE

. HCPN

Mr Paul RHEIN

. GOVCERT

Mr Laurent WEBER

. Security Made In Luxembourg (SMILE)

Mr Eric KRIER

Mr Pascal STEICHEN

Ms Judith SWIETLIK

Ms Barbara GORGES-WAGNER

Mr Georges KNELL

DECLASSIFIED

ANNEX C: LIST OF ABBREVIATIONS/GLOSSARY OF TERMS USED

LIST OF ACRONYMS, ABBREVIATIONS AND TERMS USED	ACRONYM IN FRENCH OR THE ORIGINAL LANGUAGE	FULL NAME IN FRENCH OR THE ORIGINAL LANGUAGE	ENGLISH VERSION
ANSSI		*Agence nationale de la sécurité des systèmes d'information*	National Agency for the Security of Information Systems
CIC	*CIC*	*Code d'instruction criminelle*	Code of Criminal Procedure
CP	*CP*	*Code pénal*	Criminal Code
CRF	*CRF*	*Cellule de renseignement financier*	Financial Intelligence Unit
CRI	*CRI*	*Commission rogatoire internationale*	International letter rogatory
ENISA	*ENISA*	*Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information*	European Union Agency for Network and Information Security
GENVAL	*GENVAL*	*Groupe "Questions générales, y compris l'évaluation"*	Working Party on 'General Questions including Evaluation'
IP	-	*Internet Protocol*	Internet Protocol
Law of 17 March 2014		*Loi modifiée du 17 mars 2004 relative au mandat d'arrêt européen et aux procédures de remise entre États membres de l'Union européenne*	Law of 17 March 2004 on the European arrest warrant and the surrender procedures between Member States of the European Union
PGD	*PGD*	*Police grand-ducale*	Grand-Ducal Police
SNT	*SNT*	*Section Nouvelles technologies*	New Technologies Section
SPJ	*SPJ*	*Service de police judiciaire*	Criminal Police Department
SREC	*SREC*	*Section de recherche et d'enquêtes criminelles*	Criminal investigation section

DECLASSIFIED

ANNEX D: RELEVANT LEGISLATION

I. General provisions concerning criminal liability

Intention, negligence/carelessness	With the exception of minor offences and unintentional misdemeanours, fraudulent intent must always be present.
Aggravating/mitigating circumstances	General aggravating circumstance: **Criminal Code: Chapter V - Repeat offences** **'Article 54** Anyone who was previously sentenced to a criminal penalty and commits a criminal offence punishable by five to ten years' imprisonment may be sentenced to ten to fifteen years' imprisonment. Where the criminal offence is punishable by ten to fifteen years' imprisonment, the offender may be sentenced to fifteen to twenty years' imprisonment. Where the criminal offence is punishable by fifteen to twenty years' imprisonment, the offender shall serve at least seventeen years of that sentence. **Article 56** Anyone who was previously sentenced to a criminal penalty and commits a misdemeanour may be sentenced to a penalty corresponding to double the maximum incurred under the law punishing that misdemeanour. The same penalty may be handed down where the offender has incurred a previous sentence of at least one year's imprisonment and has committed the new misdemeanour within five years from the date on which he or she served the sentence or it was extinguished by limitation. **Article 57** The rules on repeat offences shall be applied, in accordance with the previous articles, in the event of prior conviction by a military tribunal in respect of an act defined as a criminal offence or misdemeanour under ordinary criminal laws, and shall incur a penalty corresponding to those laws. Where a penalty punishable by military laws has been imposed for that act, when assessing the repeat offence the courts and tribunals shall only take into account the minimum penalty punishable by the first judgment that could be imposed under ordinary criminal laws. **Article 57-1** (Law of 29 February 2008) Article 57-1 (Law of 29 February 2008) 1. Anyone who, having been sentenced to more than five years' imprisonment by a court in a Member State of the European Union for

DECLASSIFIED

	acts cited under articles 162, 168, 173, 176, 180 - indents 3 to 6, 186 - indents 3 to 6, 192-1 and 192-2, has committed such an act again, may be sentenced to ten to fifteen years' imprisonment, where the act is a criminal offence punishable by five to ten years' imprisonment. Where the criminal offence is punishable by ten to fifteen years' imprisonment, the offender may be sentenced to fifteen to twenty years' imprisonment. Where the act is a criminal offence punishable by fifteen to twenty years' imprisonment, the offender shall be sentenced to at least seventeen years' imprisonment. 2. Anyone who, having been sentenced to over five years' imprisonment by a court in a Member State of the European Union for acts cited under articles 162, 163, 168, 169, 170, 173, 176, 177, 180 - indents 3 to 6, 185, 186 - indents 3 to 6, 187-1, 192-1 and 192-2, has committed such an act again, may receive a penalty corresponding to double the maximum punishment for that act provided for in the law, where the act in question is a misdemeanour. 3. Anyone who, having been sentenced to at least one year's imprisonment by a court in a Member State of the European Union for acts cited under articles 162, 163, 168, 169, 170, 173, 176, 177, 180 - indents 3 to 6, 185, 186 - indents 3 to 6, 187-1, 192-1 and 192-2, has committed such an act again within five years from the date on which he or she served the sentence or it was extinguished by limitation, may receive a penalty corresponding to double the maximum punishment for that act provided for in the relevant law, where the act in question is a misdemeanour. **Article 57-2** (Law of 3 March 2010) Where a legal person, having received a criminal penalty pursuant to Article 36, incurs criminal liability by committing a new criminal offence, the maximum amount of the applicable fine shall be four times that imposed under Article 36. Where a legal person, having received a criminal penalty pursuant to Article 37, incurs criminal liability by committing a new criminal offence, the maximum amount of the applicable fine shall be four times that imposed under Article 37. **Article 57-3** (Law of 3 March 2010) Where a legal person, having received a criminal penalty, incurs criminal liability by committing a misdemeanour, the maximum applicable fine shall be four times that imposed under Article 36. The penalties set in the previous paragraph may be imposed where a legal person, who has previously

DECLASSIFIED

	received a fine for misdemeanour amounting to at least EUR 36 000, incurs criminal liability by committing a new misdemeanour within five years from the date on which it served the sentence or on which the sentence was extinguished by limitation.' **Criminal Code: Chapter IX - Mitigating circumstances** (Law of 13 June 1994) **'Article 73** (Law of 13 June 1994) Where there are mitigating circumstances, the criminal penalties shall be reduced or amended in accordance with the following provisions. **Article 74** (Law of 13 June 1994) Life imprisonment shall be replaced by a prison term of no less than fifteen years. Twenty to thirty years' imprisonment shall be replaced by no less than ten years' imprisonment. Fifteen to twenty years' imprisonment shall be replaced by no less than five years' imprisonment. Ten to fifteen years' imprisonment shall be replaced by five to ten years' imprisonment or even by a prison term of no less than three years. Five to ten years' imprisonment shall be replaced by a minimum of three months' imprisonment. **Article 75 (**Law of 13 June 1994) Where the law raises the minimum level of a criminal penalty, the ordinary minimum penalty shall be applied, or even the next lowest penalty, in accordance with the previous article. **Article 75-1** (Law of 3 March 2010) Assessment of mitigating circumstances applying to a legal person shall be based on the criminal penalties incurred by a natural person for the acts for which the legal person may incur criminal liability. **Article 76** (Law of 1 August 2001) The fine serving as a criminal penalty may be reduced but may in no event be less than EUR 251. Article 77 (Law of 1 August 2001) Convicted persons whose criminal penalty has been commuted to imprisonment may receive a fine of between EUR 251 and 10 000. (Law of 13 June 1994) They may be deprived of all or part of the rights mentioned in Article 11 for a period of at least five, but no more than ten years. Article 78 (Law of 1 August 2001) In the event of mitigating circumstances, it is possible not to impose the prison sentence and to reduce the fine to less than EUR 251 though not less than EUR 25. (Law of 13 June 1994) Where the deprivation of rights mentioned in Article 11 has been ordered and

DECLASSIFIED

	authorised, judges may impose those penalties for a period of between one and five years or may restore the rights in full. **Article 79** (Law of 13 June 1994) The assessment of mitigating circumstances shall be left to the courts and tribunals. Those circumstances shall be indicated in their decisions and judgments.'
Conditions for granting of a suspension	Code of Criminal Procedure: Section IV - Suspension of the enforcement of penalties '**Article 626** (Law of 26 July 1986) In the event of a sentencing, following a trial, to imprisonment and a fine, or just one of those penalties, courts and tribunals may order, in the same reasoned decision, a suspension of the enforcement of all or part of the penalty. (Law of 3 March 2010) Suspension shall not be possible for natural persons if, prior to the act giving rise to the prosecution, the offender had received a sentence that was rendered irrevocable, to a prison term for misdemeanour or to a more serious penalty for an ordinary law offence. Suspension shall not be possible for legal persons if, prior to the act giving rise to the prosecution, the offender had received a sentence that was rendered irrevocable, to a prison term for misdemeanour or to a more serious penalty for an ordinary law offence. … Section V – Probation **Article 629** (Law of 26 July 1986) In the event of sentencing to a prison term for an ordinary law offence, where the offender has not been sentenced, in respect of a criminal offence or an ordinary law misdemeanour, to a previous prison sentence, or has been sentenced only to a suspended prison term of one year or less, courts and tribunals may, by ordering that the execution of all or part of the principal penalty be suspended for a period of no less than three years and no more than five years, sentence the offender to a suspended prison term with probation. However, where the previous conviction already imposed a suspended prison sentence, the provisions in the first paragraph shall not apply. Where the previous conviction entailed an ordinary suspension, the first penalty shall, by derogation from the provisions of Article 627, only be enforced if the second one has been imposed under the conditions and within the deadlines provided for by Article 631 or Article 631-2. The first penalty shall be treated as null

DECLASSIFIED

	and void if the second penalty is considered null and void under the conditions and within the deadlines provided for by Article 631-3.'

DECLASSIFIED

Minimum/maximum penalty	Fine of EUR 25/life imprisonment
Alternative or cumulative penalties	**Article 17** (Law of 13 June 1994) of the Criminal Code: 'Where the perpetrator of a misdemeanour incurs a criminal penalty other than imprisonment or a fine, that penalty may be imposed on its own as the principal penalty. **Article 18** (Law of 13 June 1994) Where the perpetrator of a misdemeanour punishable by imprisonment has knowingly exploited opportunities arising through the conduct of a professional or social activity to prepare or commit that misdemeanour, the court may impose, as the principal penalty, a ban on carrying on that activity in any form or manner for a period not exceeding five years, unless the activity consists in working as a member of parliament or municipal councillor. The provisions of this Article are not applicable to press misdemeanours. **Article 19** (Law of 13 June 1994) Where a misdemeanour is punishable by imprisonment, special confiscation as defined in Article 31 may be imposed as the principal penalty, even where there is no provision to that effect in the specific law invoked. The provisions in the previous paragraph are not applicable to press misdemeanours. **Article 20** (Law of 13 June 1994) Where a misdemeanour is punishable by imprisonment and a fine, the court may elect to impose, as the principal penalty, only one or the other of those penalties. If the fine is imposed on its own, it may be increased to twice the maximum amount stipulated. If only imprisonment is provided for, the court may substitute for it a fine not exceeding the amount obtained by multiplying the maximum prison sentence provided for, expressed in days, by the amount taken into account for imprisonment as a substitute for a non-collectible fine. **Article 21** (Law of 13 June 1994) Where a misdemeanour is punishable by imprisonment, the court may elect to impose, as the principal penalty, one or more of the following penalties: 1) a ban on driving certain vehicles for a period not exceeding five years, or a restriction on the entitlement to drive for a maximum of the same duration; 2) confiscation of one or more vehicles owned by the defendant; 3) a ban, for a period not exceeding five years, on keeping or carrying a weapon requiring a licence;

DECLASSIFIED

	4) a ban on hunting for a period not exceeding five years; 5) confiscation of one or more weapons owned by the defendant. **Article 22** (Law of 13 June 1994) 1) If the court considers that the misdemeanour does not warrant a prison sentence of longer than six months, it may, as the principal penalty, sentence the convicted person to perform unpaid community service, the duration of which may not be less than forty hours nor greater than two hundred and forty hours, for a local authority, for a public establishment, or for a medical or philanthropic association or institute. 2) This Article may be invoked only if the defendant is present. Before the judgment is handed down, the president of the court shall inform the defendant of the right to refuse to perform community service and hear the defendant's response. 3) Performance of the community service must begin within eighteen months of the date on which the decision under criminal law has become irrevocable. 4) The principal public prosecutor shall decide on the arrangements for the performance of the community service. In particular, he or she may, for serious medical, family, professional or social reasons, temporarily suspend the period within which the service is to be performed. 5) Possible types of community service shall be laid down by Grand-Ducal Regulation. 6) Where the convicted person is an employee, the community service may be performed in addition to the maximum working time permitted by law. 7) Provisions laid down in statute and regulations on night work, hygiene, safety, and on work performed by women and young workers, are applicable to community service.'

DECLASSIFIED

Multiple offences and repeat offences	**Criminal Code: Chapter VI – Concurrent offences** **Article 58** Anyone convicted for several minor offences shall incur the penalty for each of them. **Article 59** In the event of one or more misdemeanours being concurrent with one or more minor offences, the minor-offence penalties shall be imposed cumulatively; the most severe penalty for a misdemeanour shall be imposed on its own and may even be increased to twice the maximum, provided it does not exceed the sum of the penalties for the various offences. **Article 60** In the event of concurrent misdemeanours, the most severe penalty shall be imposed on its own. That penalty may even be increased to twice the maximum, provided it does not exceed the sum of the penalties for the various misdemeanours. (Law of 13 June 1994) In any case, alternative penalties will be imposed cumulatively. **Article 61** (Law of 8 July 1996) (1) Where a criminal offence is concurrent either with one or more misdemeanours, or with one or more minor offences, the most severe penalty shall be imposed on its own. (2) The most severe penalty is that associated with the longest term of imprisonment. (3) If the terms of imprisonment are of equal duration, the most severe penalty is that associated with the highest mandatory fine. (4) If the terms of imprisonment are of equal duration and the mandatory fines are equal in amount, the most severe penalty is that for the criminal offence. (5) In all cases, the provisions on repeat offences, statutory time limitation, suspension of the execution of penalties and rehabilitation are those that apply to criminal penalties. **Article 62** In the event of concurrent crimes, the most severe penalty shall be imposed on its own. If that penalty consists of a prison term or imprisonment for five to ten years, it may even be increased by five years beyond the maximum. **Article 64** Special confiscation penalties shall always be cumulative when they are imposed for several criminal offences, misdemeanours or minor offences. **Article 65** If the same facts constitute more than one offence, the most severe penalty shall be imposed on its own.' Repeat offences: see aggravating circumstances.
Incitement, aiding and abetting	**Criminal Code: Chapter VII – involvement of**

DE-CLASSIFIED

and attempt	**several people in the same criminal offence or misdemeanour** '**Article 66** The following shall be punished as perpetrators of a criminal offence or misdemeanour: Those who committed it or cooperated directly in its commission; Those who, by some action, assisted in its commission such that, without their help, the criminal offence or misdemeanour could not have been committed; Those who, by means of gifts, promises, threats, abuse of authority or power, machinations or culpable deceit, gave direct encouragement to commit the criminal offence or misdemeanour; (Law of 8 June 2004) Those who, either by means of speeches held at meetings or in public places, or by means of posters or bills, or by means of writing, whether printed or otherwise and sold or distributed, gave direct encouragement to commit it, without prejudice to the last two provisions of Article 22 of the Law of 8 June 2004 on freedom of expression in the media. **Article 67** The following shall be punished as accessories to a criminal offence or misdemeanour: Those who gave instructions for it to be committed; Those who procured weapons, tools or any other instruments used for the criminal offence or misdemeanour, knowing they would be used for that purpose; Except in the cases provided for in the third paragraph of Article 66, those who knowingly aided or abetted the perpetrator or perpetrators of the criminal offence or misdemeanour, either in the act of preparing or facilitating it, or in the act of committing it. **Article 68** Those who, while aware of the criminal activities of offenders carrying out robberies or attacking State security, public order, persons or property, regularly provided them with accommodation, hiding places or meeting places, shall be punished as their accessories. **Article 69** Accessories to a criminal offence shall incur the penalty ranking immediately below that which they would have incurred as perpetrators of that offence, in accordance with the scale set out in Article 52 of this code. The penalty imposed on accessories to a misdemeanour may not exceed two thirds of that which would have applied to them as perpetrators of that misdemeanour.' **Criminal Code: Chapter IV – attempted criminal offences or misdemeanours**

DE-CLASSIFIED

	'**Article 51** A punishable attempt exists where the determination to commit a criminal offence or misdemeanour has been demonstrated by exterior actions which constitute the beginnings of carrying out the criminal offence or misdemeanour, and which were suspended or failed to be effective only because of circumstances beyond the perpetrator's control. **Article 52** (Law of 7 July 2003) The attempt to commit a criminal offence shall be punishable by the penalty ranking immediately below that for the criminal offence itself. Penalties considered as ranking immediately below others are as follows: a) imprisonment for twenty to thirty years ranks immediately below life imprisonment; b) imprisonment for fifteen to twenty years ranks immediately below imprisonment for twenty to thirty years; c) imprisonment for ten to fifteen years ranks immediately below imprisonment for fifteen to twenty years; d) imprisonment for five to ten years ranks immediately below imprisonment for ten to fifteen years; e) imprisonment for a minimum of three months ranks immediately below imprisonment for five to ten years. **Article 53** The instances in which attempted misdemeanours are punishable, and the applicable penalties, are determined by statute.'
Penalties in the event of a summary trial or judicial examination	No different penalties in the event of a penalty order being issued or a judgment upon consent (summary trial)
Other general provisions	/

II. Cybercrime offences and penalties

Budapest Convention Article 2 – Illegal access	Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.
Corresponding provision in domestic law	**Article 509-1** (Law of 14 August 2000) of the Criminal Code: 'Anyone who fraudulently accesses or maintains a connection to all or part of an automated data processing or transmission system shall be liable to

DECLASSIFIED

	imprisonment of between two months and two years or a fine of between EUR 500 and EUR 25 000, or both. Where this results in the deletion or modification of data in the system, or alters the functioning of the system, the term of the imprisonment shall be between four months and two years and the amount of the fine shall be between EUR 1 250 and EUR 25 000.'
Intention, negligence/carelessness	Fraudulent intent required.
Aggravating circumstances	If the fraudulent access resulted in deletion or modification of the data and **Article 509-4** (Law of 10 November 2006) of the Criminal Code: 'Where, in the cases referred to in Articles 509-1 to 509-3, money or monetary value has been transferred, leading to loss of property for a third party, in order to confer a financial benefit on the person committing the offence or on a third party, the penalty shall be imprisonment of between four months and five years and a fine of between EUR 1 250 and EUR 30 000.'
Minimum/maximum penalty	Imprisonment of between two months and five years or fine of between EUR 500 and EUR 30 000, or both.

Attempt	**Article 509-6** (Law of 15 July 1993) of the Criminal Code: 'An attempt to commit the offences set out in Articles 509-1 to 509-5 shall be punishable by the same penalties as the offence itself.'
Penalties applicable to legal persons	**Criminal Code: Chapter II-1 - Penalties applicable to legal persons** (Law of 03 March 2010) '**Article 34** (Law of 3 March 2010) Where a criminal offence or misdemeanour is committed in the name of and in the interests of a legal person by one of its legal bodies or by one or more of its de jure or de facto managers, the legal person may be held criminally liable and incur the penalties provided for in Articles 35 to 38. The criminal liability of legal persons shall not exclude that of the natural persons who perpetrate or are complicit in the same offences. The preceding paragraphs are not applicable to the State or communes. **Article 35** (Law of 3 March 2010) The criminal penalties or penalties for misdemeanour incurred by legal persons are: 1) a fine, under the conditions and provisions set out in

DECLASSIFIED

	Article 36; 2) special confiscation; 3) exclusion from participation in public procurement; 4) dissolution, under the conditions and provisions set out in Article 38. **Article 36** (Law of 3 March 2010) The fine for the purposes of criminal penalties and penalties for misdemeanour applicable to legal persons shall amount to at least EUR 500. In the case of crimes, the maximum fine applicable to legal persons shall be EUR 750 000. In the case of penalties for misdemeanour, the maximum fine applicable to legal persons shall be double the amount incurred by natural persons under the law punishing the offence. Where there is no fine for natural persons in the law punishing the offence, the maximum fine applicable to legal persons may not be more than double the amount obtained by multiplying the maximum prison sentence for the offence, in days, by the amount taken into account for imprisonment as a substitute for non-collectible fines. **Article 37** (Law of 3 March 2010) The maximum level of the fine incurred pursuant to the provisions in Article 36 shall be multiplied by five where the legal person is held criminally liable for one of the following offences: - criminal offences and misdemeanours against state security - acts of terrorism and financing of terrorism - infringement of laws relating to banned weapons in conjunction with a criminal association or organisation - human trafficking and pimping - drug trafficking in conjunction with a criminal association or organisation - money laundering and handling of stolen goods - embezzlement, illegal interest charging, active and passive corruption, private corruption - facilitation of unauthorised entry and residence in conjunction with a criminal association or organisation. - (Law of 21 December 2012) illegal employment of illegally staying third-country nationals in conjunction with a criminal association or organisation. **Article 38** (Law of 3 March 2010) Dissolution may be ordered where a legal person has intentionally been established or, in the case of a crime or offence that is punishable for a natural person by a prison term of three years or more, where such legal person has been misused in order to commit the offences charged. Dissolution shall not be applicable to any legal persons under public law who may be held liable.

DECLASSIFIED

	The decision ordering the dissolution of the legal person shall also include referral of that legal person to the court with responsibility for such dissolution. **Article 39** (Law of 3 March 2010) Where the legal person incurs a misdemeanour penalty other than a fine, that penalty may be imposed on its own and constitute the principal penalty. **Article 40** (Law of 3 March 2010) Where a misdemeanour is punishable by the imprisonment of natural persons under the law punishing the offence, the special confiscation defined under Article 31 may serve as the principal penalty against the legal person, even where there is no provision to that effect in the specific law invoked. The provisions in the previous paragraph are not applicable to press misdemeanours.'

Additional notes	**Article 509-7** (Law of 15 July 1993) of the Criminal Code: 'Anyone who participates in an association or agreement formed or established with a view to the preparation, demonstrated by one or more material facts, of one of more of the offences set out in Articles 509-1 to 509-5 shall be subject to the same penalties laid down for the offence itself or for the offence carrying the most severe penalty.'

i. Penalties for illegal interception

Budapest Convention **Article 3 – Illegal interception**	Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.
Corresponding provision in domestic law	**Article 509-3** (Law of 14 August 2000) of the Criminal Code: '...punishable by imprisonment of between three months and three years or a fine of between EUR 1 250 and EUR 12 500, or both. (Law of 18 July 2014) Anyone who, intentionally and with contempt for the rights of others, intercepts non-public transmissions of computer data to, from or within an automated data processing or transmission system, will be subject to the same penalties.'

DECLASSIFIED

Intention, negligence/carelessness	Offence committed intentionally and with contempt for the rights of others.
Aggravating circumstances	**Article 509-4** (Law of 10 November 2006) of the Criminal Code: 'Where, in the cases referred to in Articles 509-1 to 509-3, money or monetary value has been transferred, leading to loss of property for a third party, in order to confer a financial benefit on the person committing the offence or on a third party, the penalty shall be imprisonment of between four months and five years and a fine of between EUR 1 250 and EUR 30 000.'

Minimum/maximum penalty	Imprisonment of between three months and five years or fine of between EUR 1 250 and EUR 30 000, or both.
Attempt	**Article 509-6** (Law of 15 July 1993) of the Criminal Code: 'An attempt to commit the offences set out in Articles 509-1 to 509-5 shall be punishable by the same penalties as the offence itself.'
Penalties applicable to legal persons	See above.
Additional notes	**Article 509-7** (Law of 15 July 1993) of the Criminal Code: 'Anyone who participates in an association or agreement formed or established with a view to the preparation, demonstrated by one or more material facts, of one of more of the offences set out in Articles 509-1 to 509-5 shall be subject to the same penalties laid down for the offence itself or for the offence carrying the most severe penalty.'

DECLASSIFIED

ii. Penalties for data interference

Budapest Convention Article 4 – Data interference	1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.
Corresponding provision in domestic law	**Article 509-1** (Law of 14 August 2000) of the Criminal Code: 'Anyone who fraudulently accesses or maintains a connection to all or part of an automated data processing or transmission system … Where this results in the suppression or modification of the data in the system, or alters the functioning of the system, the term of the imprisonment shall be between four months and two years and the amount of the fine shall be between EUR 1 250 and EUR 25 000.' **Article 509-3** (Law of 14 August 2000) of the Criminal Code: 'Anyone who, intentionally and with contempt for the rights of others, either directly or indirectly inputs data into an automated data processing or transmission system, or suppresses or modifies the data it contains or the means of processing or transmitting that data, shall be liable to imprisonment of between three months and three years or a fine of between EUR 1 250 and EUR 12 500, or both. … '
Intention, negligence/carelessness	Fraudulent intent/Offence committed intentionally and with contempt for the rights of others.
Aggravating circumstances	**Article 509-4** (Law of 10 November 2006) of the Criminal Code: 'Where, in the cases referred to in Articles 509-1 to 509-3, money or monetary value has been transferred, leading to loss of property for a third party, in order to confer a financial benefit on the person committing the offence or on a third party, the penalty shall be imprisonment of between four months and five years and a fine of between EUR 1 250 to EUR 30 000.'
Minimum/maximum penalty	Imprisonment of between three months and five years or fine of between EUR 1 250 and EUR 30 000, or both.

DECLASSIFIED

Attempt	**Article 509-6** (Law of 15 July 1993) of the Criminal Code: 'An attempt to commit the offences set out in Articles 509-1 to 509-5 shall be punishable by the same penalties as the offence itself.'
Penalties applicable to legal persons	See above.
Additional notes	**Article 509-7** (Law of 15 July 1993) of the Criminal Code: 'Anyone who participates in an association or agreement formed or established with a view to the preparation, demonstrated by one or more material facts, of one of more of the offences set out in Articles 509-1 to 509-5 shall be subject to the same penalties laid down for the offence itself or for the offence carrying the most severe penalty.'

iii. Penalties for system interference

Budapest Convention Article 5 – System interference	Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.
Corresponding provision in domestic law	**Article 509-2** (Law of 15 July 1993) of the Criminal Code: 'Anyone who, intentionally and with contempt for the rights of others, hinders or distorts the functioning of an automated data processing or transmission system shall be liable to imprisonment of between three months and three years or a fine of between EUR 1 250 and EUR 12 500, or both. **Art. 509-3** (L. 14 August 2000) 'Anyone who, intentionally and with contempt for the rights of others, either directly or indirectly inputs data into an automated data processing or transmission system, or suppresses or modifies the data it contains or the means or processing or transmitting that data, shall be liable to imprisonment of between three months and three years or a fine of between EUR 1 250 and EUR 12 500, or both.'

DECLASSIFIED

Intention, negligence/carelessness	Offence committed intentionally and with contempt for the rights of others.
Aggravating circumstances	**Article 509-4** (Law of 10 November 2006) of the Criminal Code: 'Where, in the cases referred to in Articles 509-1 to 509-3, money or monetary value has been transferred, leading to loss of property for a third party, in order to confer a financial benefit on the person committing the offence or on a third party, the penalty shall be imprisonment of between four months and five years and a fine of between EUR 1 250 and EUR 30 000.'
Minimum/maximum penalty	Imprisonment of between three months and five years and fine of between EUR 1 250 and EUR 30 000.
Attempt	**Article 509-6** (Law of 15 July 1993) of the Criminal Code: 'An attempt to commit the offences set out in Articles 509-1 to 509-5 shall be punishable by the same penalties as the offence itself.'
Penalties applicable to legal persons	See above.
Additional notes	**Article 509-7** (Law of 15 July 1993) of the Criminal Code: 'Anyone who participates in an association or agreement formed or established with a view to the preparation, demonstrated by one or more material facts, of one of more of the offences set out in Articles 509-1 to 509-5 shall be subject to the same penalties laid down for the offence itself or for the offence carrying the most severe penalty.'

DECLASSIFIED

iv. Penalties for misuse of devices

Budapest Convention Article 6 – Misuse of devices	See Annex.
Corresponding provision in domestic law	**Article 509-5** (Law of 18 July 2014) of the Criminal Code: 'It shall be punishable by imprisonment of between four months and five years and a fine of between EUR 1 250 and EUR 30 000 for any person, with fraudulent intent, to produce, sell, procure, import, distribute or make available: – a computer device intended for the purpose of committing any of the offences referred to in Articles 509-1 to 509-4; or – any electronic key allowing access, with contempt for the rights of others, to all or part of an automated data processing or transmission system.'
Intention, negligence/carelessness	Fraudulent intent required.
Aggravating circumstances	No.
Minimum/maximum penalty	Imprisonment of between four months and five years and fine of between EUR 1 250 and EUR 30 000.
Attempt	**Article 509-6** (Law of 15 July 1993) of the Criminal Code: 'An attempt to commit the offences set out in Articles 509-1 to 509-5 shall be punishable by the same penalties as the offence itself.'
Penalties applicable to legal persons	See above.
Additional notes	**Article 509-7** (Law of 15 July 1993) of the Criminal Code: 'Anyone who participates in an association or agreement formed or established with a view to the preparation, demonstrated by one or more material facts, of one of more of the offences set out in Articles 509-1 to 509-5 shall be subject to the same penalties laid down for the offence itself or for the offence carrying the most severe penalty.'

v. Penalties for computer-related forgery

Budapest Convention Article 7 – Computer-related forgery	Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal

DE-CLASSIFIED

	liability attaches.
Corresponding provision in domestic law	**Article 196** (Law of 14 August 2000) of the Criminal Code: 'It shall be punishable by imprisonment of between five and 10 years to forge official public documents, or to forge commercial, banking or private documents, including electronic private deeds, by forging signatures, by counterfeiting or altering documents or signatures, by fabricating agreements, provisions, obligations or discharges, or by introducing them into documents after the fact, by adding or altering clauses, statements or facts which these acts were intended to include and record. **Art. 197** (L. 14 August 2000) In all of the cases referred to in this section, a person who makes use of the forgery shall be subject to the same penalties as the perpetrator of the forgery. **Art. 488** (L. 14 August 2000) Anyone who fraudulently counterfeits or alters keys, including electronic keys, shall be sentenced to imprisonment of between four months and five years and a fine of between EUR 1 250 and EUR 30 000. (Law of 18 July 2014)'
Intention, negligence/carelessness	Fraudulent intent required.
Aggravating circumstances	No.
Minimum/maximum penalty	Article 488: imprisonment of between four months and five years and fine of between EUR 1 250 and EUR 30 000, Art. 196 and 197; imprisonment of between five and 10 years.
Attempt	Article 488: no. Articles 196 and 197: imprisonment of at least three months.
Penalties applicable to legal persons	See above.

vi. Penalties for computer-related fraud

Budapest Convention Article 8 – Computer-related fraud	Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: (a) any input, alteration, deletion or suppression of computer data; (b) any interference with the functioning of a computer system,

DECLASSIFIED

	with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.
Corresponding provision in domestic law	**Article 509-4** (Law of 10 November 2006) of the Criminal Code: 'Where, in the cases referred to in Articles 509-1 to 509-3, money or monetary value has been transferred, leading to loss of property for a third party, in order to confer a financial benefit on the person committing the offence or on a third party, the penalty shall be imprisonment of between four months and five years and a fine of between EUR 1 250 and EUR 30 000.'
Intention, negligence/carelessness	Fraudulent intent required.
Aggravating circumstances	No.
Minimum/maximum penalty	Imprisonment of between four months and five years and fine of between EUR 1 250 and EUR 30 000.
Attempt	**Article 509-6** (Law of 15 July 1993) of the Criminal Code: 'An attempt to commit the offences set out in Articles 509-1 to 509-5 shall be punishable by the same penalties as the offence itself.'
Penalties applicable to legal persons	See above.
Additional notes	**Article 509-7** (Law of 15 July 1993) of the Criminal Code: 'Anyone who participates in an association or agreement formed or established with a view to the preparation, demonstrated by one or more material facts, of one of more of the offences set out in Articles 509-1 to 509-5 shall be subject to the same penalties laid down for the offence itself or for the offence carrying the most severe penalty.'

vii. Penalties for offences related to child pornography

Budapest Convention Article 9 – Offences related to child pornography	1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a producing child pornography for the purpose of its distribution through a computer system; b offering or making available child pornography through a computer system; c distributing or transmitting child pornography through a computer system; d procuring child pornography through a computer system for oneself or for another person; e possessing child pornography in a computer system or on a computer-data storage medium.

DECLASSIFIED

	2 For the purpose of paragraph 1 above, the term 'child pornography' shall include pornographic material that visually depicts: a minor engaged in sexually explicit conduct; b a person appearing to be minor engaged in sexually explicit conduct; c realistic images representing a minor engaged in sexually explicit conduct. 3 For the purpose of paragraph 2 above, the term 'minor' shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall not be less than 16 years. 4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.
Corresponding provision in domestic law	**Criminal Code Chapter VII – Affront to public decency and specific provisions for the protection of children** (Law of 16 July 2011) **"Art. 383** (L. 16 July 2011) Producing, transporting or distributing, by whatever means and regardless of the medium, a message which is violent or pornographic in nature or which presents a serious affront to human dignity, or trading in such a message, shall be punishable by imprisonment of between one month and three years and a fine of between EUR 251 and EUR 50 000 where that message is likely to be watched or seen by a minor. **Art. 383a** (L. 16 July 2011) The offences referred to in Article 383 shall be punishable by imprisonment of between one and five years and a fine of between EUR 251 and EUR 75 000 where they involve or depict minors or persons who are particularly vulnerable as a result of their illegal or insecure administrative situation, pregnancy, illness, infirmity or physical or mental disability. In the event of conviction, confiscation of the items set out in Article 383 shall always be ordered, even if the property does not belong to the convicted person or the conviction is handed down by the police court following the admission of mitigating circumstances. **Art. 383b** (L. 16 July 2011) Fixing, recording or transmitting the image or representation of a minor for the purpose of its distribution, where that image or that representation is of a pornographic nature, shall be punishable by imprisonment of between one month and three years and a fine of between EUR 251 and EUR 50 000. Offering, making available or distributing such an image or representation by whatever means, importing it or exporting it, or having it imported or exported, shall be subject to the same penalties.

DECLASSIFIED

	The offences are punishable by imprisonment of between one and five years and a fine of between EUR 251 and EUR 100 000 where an electronic communications network has been used to distribute the image or representation of the minor to an unknown audience. An attempt to commit the offences set out in the preceding paragraphs shall be subject to the same penalties. **Art. 384** (L. 21 February 2013) It shall be punishable by imprisonment of between one month and three years and a fine of between EUR 251 and EUR 50 000 to knowingly acquire, hold or consult written or printed material, images, photographs, films or other items of a pornographic nature involving or depicting minors. (L. 16 July 2011) In the event of conviction, confiscation of these items shall always be ordered, even if the property does not belong to the convicted person or the conviction is handed down by the police court following the admission of mitigating circumstances. **Art. 385** (L. 31 May 1999) Anyone who causes an affront to public decency through indecent behaviour shall be liable to imprisonment of between eight days and three years and a fine of between EUR 251 and EUR 25 000. **Art. 385-1** (L. 8 June 2004) Anyone who causes an affront to public decency by means of songs, pamphlets, figures, written or printed material, drawings, engravings, paintings, emblems, images or any other type of writing, sound, words or images communicated to the public using media, shall be liable to imprisonment of between eight days and one year and a fine of between EUR 251 and EUR 12 500. **Art. 385-2** (L. 16 July 2011) An adult who makes sexual propositions via an electronic means of communication to a minor aged under 16, or to a person claiming to be such, shall be liable to imprisonment of between one month and three years and a fine of between EUR 251 and EUR 50 000. Such acts shall be punishable by imprisonment of between one and five years and a fine of between EUR 251 and EUR 75 000 where the propositions have been followed by a meeting. **Art. 385a** (L. 31 May 1999) Anyone who sells or distributes indecent written material, images, figures or objects to children aged under 16 which are likely to trouble their imagination shall be liable to a fine of between EUR 251 and EUR 25 000. Anyone who publicly displays indecent written material, images, figures or objects in the vicinity of an

DECLASSIFIED

	educational or training establishment attended by children aged under 16 which may trouble their imagination shall be subject to the same penalty. In the event of conviction, confiscation of the indecent written material, figures or objects displayed, offered for sale or distributed shall always be ordered, even if the property does not belong to the convicted person or the conviction is handed down by the police court following the admission of mitigating circumstances. **Art. 386** In the cases provided for in this chapter, offenders may also be sentenced to revocation of the rights set out in Article 11(1), (3), (4), (5) and (7). (L. 21 February 2013) Their sentence may also include a ban of up to 10 years on carrying out any professional, volunteer or social activity that involves regular contact with minors. Any violation of this ban shall be punishable by imprisonment of between two months and two years.'
Intention, negligence/carelessness	Fraudulent intent required.
Aggravating circumstances	See the text of the articles.
Minimum/maximum penalty	Imprisonment of between one month and five years and fine of between EUR 251 and EUR 100 000.
Attempt	Article 383ter of the Criminal Code: yes; same penalties. For the other articles concerned: no.
Penalties applicable to legal persons	See above.
Additional notes	None.

viii. Penalties for offences relating to infringements of copyright and related rights

Budapest Convention Article 10 – Offences relating to infringements of copyright and related rights	1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of

DECLASSIFIED

	Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.
Corresponding provision in domestic law	**Amended Law of 18 April 2001 on copyright, related rights and databases** **'Criminal penalties** **Art. 82** Any malicious or fraudulent infringement of the rights, protected under this law, of copyright holders, holders of related rights or database producers shall constitute the offence of counterfeiting. It constitutes the same offence to knowingly offer for sale, import, export, fix, reproduce, communicate, transmit wirelessly or otherwise, make generally available to the public, or introduce or re-introduce into circulation, whether or not in return for payment, a work, a service or a database without the permission of the copyright holder, the holder of related rights or the database producer. It therefore constitutes the same offence to knowingly make available to the public phonograms, videograms, CD-ROMs, multimedia or any other type of medium, program or database created without the permission of the copyright holder, the holder of related rights or the database producers, as well as to reproduce protected works, services or databases in order to digitise them, store them, distribute them, inject them or generally enable them to be made accessible or to be communicated to the public. **Art. 83** The offences set out in the previous article shall be punishable by a fine of between EUR 251 and EUR 250 000. The confiscation from the convicted persons of counterfeit works or items or the media containing the counterfeits, as well as the plates, moulds, matrices or other implements used directly in the commission of the offences set out in the preceding article, regardless

DECLASSIFIED

	of who owns them, shall be ordered, as shall the materials used to copy them, digitise them or inject them into networks. The judgment may also order the destruction of the confiscated items. **Art. 84** The malicious or fraudulent use on a work or database of the name of a copyright holder, holder of related rights or holder of a 'sui generis' right as a database producer, or of any other distinctive sign adopted by the right holders to distinguish their work, service or production shall be punishable by imprisonment of between three months and two years or a fine of between EUR 251 and EUR 250 000, or both. The same applies to the malicious or fraudulent use of the name of a holder of related rights or holder of a 'sui generis' right as a database producer, or of any other distinctive sign adopted by that right holder, when operating the service of a holder of related rights or of a database producer or on the medium containing that service. Confiscation of the counterfeit items shall be ordered in all cases. The court may also order their destruction. The same penalties shall apply to anyone who knowingly sells, offers for sale, imports, exports, fixes, reproduces, communicates, transmits wirelessly or otherwise, makes generally available to the public, or introduces or re-introduces into circulation, whether or not in return for payment, the items or services set out in the first paragraph of this article. **Art. 85** Any repetition of the offences set out in the preceding articles is punishable by imprisonment of between three months and two years or a fine of between EUR 500 and EUR 500 000, or both. Furthermore, the court may order the closure, either definitively or temporarily for a duration it shall determine, of the establishment used by the convicted person, for a period not exceeding five years. It may also order the judgment delivered in the conviction to be published and posted, at the expense of the convicted person. **Art. 86** Legal persons shall be held jointly and severally liable for the convictions, damages, fines, costs, confiscations, compensation, financial penalties or penalties in kind imposed on their directors, representatives and officers for infringement of the provisions of this law.'
Intention, negligence/carelessness	Fraudulent intent required.
Aggravating circumstances	See Article 85 above on repeat offences.
Minimum/maximum penalty	Fine of EUR 251/two years' imprisonment.

DE-CLASSIFIED

Attempt	No.
Penalties applicable to legal persons	See above and Article 86 above.
Additional notes	None.

DECLASSIFIED