Council of the
European Union

Brussels, 26 November 2015
(OR. fr)

7588/2/15
REV 2 DCL 1

GENVAL 9
CYBER 23

DECLASSIFICATION

of document:	7588/2/15 REV 2 RESTREINT UE/EU RESTRICTED
dated:	9 September 2015
new status:	Public
Subject:	**Evaluation report on the seventh round of mutual evaluations 'The practical implementation and operation of European policies on preventing and combating cybercrime'** - **Report on France**

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, 9 September 2015
(OR. fr)

7588/2/15
REV 2

RESTREINT UE/EU RESTRICTED

GENVAL 9
CYBER 23

REPORT

From:	General Secretariat of the Council
To:	Delegations
Subject:	**Evaluation report on the seventh round of mutual evaluations 'The practical implementation and operation of European policies on preventing and combating cybercrime'** - **Report on France**

TABLE OF CONTENTS

1 Executive summary 5
2 Introduction 7
3 General matters and structures 10
3.1 National cyber security strategy 10
3.2 National priorities with regard to cybercrime 11
3.2.1 Strategy of the Ministry of the Interior on cyber threats 12
3.2.2 Inter-ministerial working group on tackling cybercrime 13
3.2.3 Links to the EU 'Cybercrime' priority 14
3.3 Statistics on cybercrime 16
3.3.1 Main trends leading to cybercrime 16
3.3.2 Number of registered cases of cybercrime 18
3.4 Domestic budget allocated to prevent and combat cybercrime and EU financial support 22
3.5 Conclusions 24
4 National structures 26
4.1 Judiciary (prosecution and courts) 26
4.1.1 Internal structure 26
4.1.2 Available capacity and obstacles to successful prosecution 27
4.2 Law enforcement authorities 30
4.2.1 Central services specialising in cybercrime 30
4.2.2 Regional branches of specialised criminal police 32
4.3 Other services 36
4.4 Public-private partnership 36
4.5 Cooperation and coordination at national level 38
4.5.1 Legal or policy obligations 39
4.5.2 Resources allocated to improving cooperation 41
4.6 Conclusions 44
5 Legal aspects 46
5.1 Substantive criminal law pertaining to cybercrime 46
5.1.1 Council of Europe Convention on Cybercrime 46
5.1.2 Description of national legislation 46

A/ Council Framework Decision 2005/222/JHA on attacks against information systems and Directive 2013/40/EU on attacks against information systems ____ 48
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 ____ 48
C/ Online payment card fraud ____ 49
D/ Other cybercrime phenomena ____ 50
5.2 Procedural issues ____ 50
5.2.1 Investigative techniques ____ 50
5.2.2 Forensic examination and encryption ____ 52
5.2.3 Electronic evidence ____ 54
5.3 Protection of human rights/fundamental freedoms ____ 55
5.4 Jurisdiction ____ 56
5.4.1 Principles applied in the investigation of cybercrime ____ 56
5.4.2 Rules in case of conflicts of jurisdiction and referral to Eurojust ____ 57
5.4.3 Jurisdiction for acts of cybercrime committed in the 'cloud' ____ 57
5.4.4 Perception of France with regard to the legal framework for combating cybercrime ____ 57
5.5 Conclusions ____ 58
6 Operational aspects ____ 59
6.1 Cyber attacks ____ 59
6.1.1 Nature of cyber attacks ____ 59
6.1.2 Mechanism of response to cyber attacks ____ 59
6.2 Action against child pornography and online sexual abuse ____ 60
6.2.1 Databases identifying victims and measures to avoid re-victimisation 60
6.2.2 Measures to address sexual exploitation/abuse online, sexting and cyber bullying ____ 62
6.2.3 Prevention of sex tourism, child pornographic performances and other phenomena ____ 64

6.2.4 Stakeholders active in combating websites containing or disseminating child pornography and measures taken ____ 68
6.3 Online payment card fraud ____ 71
6.4 Conclusions ____ 73
7 International cooperation ____ 74
7.1 Cooperation with EU agencies ____ 74
7.1.1 Formal requirements for cooperation with Europol/EC3, Eurojust and ENISA ____ 74
7.1.2 Assessment of cooperation with Europol/EC3, Eurojust and ENISA ____ 74
7.1.3 Operational performance of JITs and cyber patrols ____ 77
7.2 Cooperation between the French authorities and INTERPOL ____ 77
7.3 Cooperation with third states ____ 77
7.4 Cooperation with the private sector ____ 78
7.5 Tools of international cooperation ____ 79
7.5.1 Mutual legal assistance ____ 79
7.5.2 Mutual recognition instruments ____ 80
7.5.3 Surrender/extradition ____ 81
7.6 Conclusions ____ 81
8 Training, awareness-raising and prevention ____ 83
8.1 Specific training ____ 83
8.2 Awareness-raising ____ 87
8.3 Prevention ____ 88
8.3.1 National legislation/policy and other measures ____ 88
8.3.2 Public-private partnership ____ 91
8.4 Conclusions ____ 92
9 Final comments and recommendations ____ 93
9.1 Suggestions by France ____ 93
9.2 Recommendations ____ 93
9.2.1 Recommendations to France ____ 94
9.2.2 Recommendations to the European Union, its institutions and other Member States ____ 96
9.2. Recommendations to Eurojust/Europol/ENISA ____ 99
Annex A: Programme for the on-site visit ____ 100
Annex B: Persons encountered ____ 104
Annex C: List of abbreviations/glossary of terms used ____ 106

1 SUMMARY

- The evaluation visit to France took place in a very positive atmosphere. It was excellently prepared by the French authorities and was particularly well supported by the General Secretariat for European Affairs (*Secrétariat Général aux Affaires européennes* – SGAE), which coordinated the visit. This fact is even more worthy of note given that the visit to France was the first of the seventh round of evaluations, and as such the national authorities did not have the benefit of having experienced previous visits.

- All the services encountered on site were very well prepared and were able to speak with complete transparency, showing themselves to be both receptive and open-minded. The evaluation team was pleasantly surprised by the high degree of motivation and commitment demonstrated by the practitioners they questioned.

- After having emphasised the challenges of cyber defence and cyber security, France has begun a national process of reflection on the issue of dealing with cybercrime that is today at a very advanced stage; in particular, a multidisciplinary working group has been set up under the auspices of a senior judge (the interministerial working group on combating cybercrime, chaired by Public Prosecutor Marc Robert) to draw up a full strategy for this area. This strategy is in the process of being put in place. The evaluation team commends this remarkable initiative which other Member States could learn from.

- One of the main conclusions of the interministerial working group on combating cybercrime, chaired by Public Prosecutor Mark Robert, published in February 2014, was that giving greater consideration to the interdisciplinary nature of the cybercrime phenomenon should be made a priority; the French approach, whilst very proactive, has until now been rather disjointed: as yet there is no national coordinating body, and cooperation between the various public actors involved remains experimental and runs the risk of omissions and doubling-up of efforts.

- Since the adoption of the 1978 law on information technology and freedoms, France has gradually built up a wealth of legal rules that encompass as broad a range as possible of cybercrime-related offences. French criminal legislation uses sentencing of gradually increasing severity and facilitates police investigations according to the seriousness of the offences, particularly to target organised crime. This set of legal rules is updated regularly to ensure that European legal instruments are incorporated into national law, and to adapt to changing criminal behaviour. Procedural constraints remain, however, and mean that the rules on searches and taking evidence need to be better adapted to the realities of the digital world.

- The police authorities have clearly made the issue a priority and, in general, the resources and tools at their disposal are equal to the task; specific training is given to the relevant professionals; the action taken by the various special units is intense and seems to be very effective, although it appears that it could be better coordinated.

- In contrast, the judicial authorities do not treat cybercrime as an area of law in its own right; prosecuting policy is not sufficiently consolidated at the central level, and there is no dedicated route through the court system that could complete the criminal process and ensure its overall effectiveness; it would be worth improving the training offered to judges in this area. To remedy these difficulties and follow up on the report of the interministerial group on combating cybercrime chaired by Public Prosecutor Marc Robert, the Ministry of Justice has just created a horizontal service partially dedicated to dealing with cybercrime.

- There are numerous public-private partnerships; some are national in scope whilst many others are concluded on an occasional basis at the initiative of practitioners, and especially by the police services and the gendarmerie, who have an increasing number of good practices in this area.

- The French authorities expressed regret that significant obstacles to European and international cooperation persist, even in relation to the exchange of basic information such as IP addresses. The assistance provided by Europol/EC3 is very much appreciated. The opportunities provided by Eurojust for facilitating judicial cooperation, including with third countries, remain relatively little known and under-used.

2 INTRODUCTION

Following the adoption of Joint Action 97/827/JHA of 5 December 1997[1], a mechanism for evaluating the application and implementation at national level of international undertakings in the fight against organised crime was established. 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 European polices on prevention and combating cybercrime.

The choice of cybercrime as the subject for the seventh Mutual Evaluation round was welcomed by Member States. 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 which Member States felt warranted particular attention. To this end, the evaluation covers three specific areas: cyber attacks, child sexual abuse/pornography online and online card fraud and should 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] (date of transposition: 18 December 2013) and Directive 2013/40/EC on attacks against information systems[3] (date of transposition: 4 September 2015) are particularly relevant in this context.

1 Joint Action of 5 December 1997 (97/827/JHA), OJ L 344, 15.12.1997 pp. 7 – 9.
2 OJ L 335, 17.12.2011, p. 1.
3 OJ L 218, 14.8.2013, p. 8.

Moreover, the Council Conclusions on the EU Cybersecurity Strategy of June 2013[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'. This Convention is supplemented by a Protocol on the criminalisation of acts of a racist or xenophobic nature committed through computer systems[6].

Experience from past evaluations shows that Member States will be in different positions regarding implementation of relevant legal instruments, and the current process of evaluation could provide useful input also 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 on implementation of various instruments relating to fighting cybercrime only but rather on the 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 the given actors is channelled to the appropriate police and social services. The evaluation focuses on implementing national policies with regard to suppression of cyber attacks and fraud as well as child pornography. The evaluation also covers operational practices in the Member States with regard to international cooperation and the support offered to persons who fall victim to cyber crime.

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 CETS no. 185; opened for signature on 23 November 2001, entered into force on 1 July 2004.

6 CETS no. 189; opened for signature on 28 January2003, entered into force on 1 March 2006.

The order of visits to the Member States was adopted by GENVAL on 1 April 2014. France was the first Member State to be evaluated during this round of evaluations. In accordance with Article 3 of the Joint Action, a list of experts in the evaluations to be carried out has been drawn up by the Presidency. Member States have nominated experts with substantial practical knowledge in the field pursuant to a written request on 28 January 2014 to delegations made by the Chairman of GENVAL.

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 proposal from the Presidency that the European Commission, Eurojust, ENISA and Europol/EC3 should be invited as observers.

The experts charged with undertaking the evaluation of France were Mr Konstantinos SKOUVARIS (Greece), Mr Laurent THYES (Luxembourg) and Mr Yves VANDERMEER (Belgium). Four observers were also present: Ms Julie RUFF (Commission), Ms Catherine DEBOYSER (Eurojust), Ms Andrea DUFKOVA (ENISA) and Mr Benoît GODART (Europol/EC3), together with Mr Gilles DUVAL and Ms Claire ROCHETEAU from the General Secretariat of the Council.

This report was prepared by the expert team with the assistance of the General Secretariat of the Council, based on findings arising from the evaluation visit that took place in France between 28 and 31 October 2015, and on France's detailed replies to the evaluation questionnaire together with their detailed answers to ensuing follow-up questions.

3 GENERAL MATTERS AND STRUCTURES

3.1 National cyber security strategy

The National Agency for the Security of Information Systems (*Agence Nationale de Sécurité des Systèmes d'Information* – ANSSI) is the French authority charged with assisting the Prime Minister in carrying out his defence and information system security duties. ANSSI is at the heart of defining and putting in place cyber defence and cyber security policies in France.

Specialising in the protection, defence and restoration of critical infrastructure information systems, both public and private, this agency has at its disposal considerable resources in line with the priority given to its work; the multidisciplinary human resources assigned to it have been increasing since its establishment in 2009 (100 posts) and this figure is due to increase to almost 700 posts by 2017. These resources are clearly superior to those assigned to the law enforcement authorities to tackle cybercrime (in comparison, the various central services of the police that are specialised in this area employ around 250 investigators in total).

ANSSI does not deal with cybercrime as such, but rather with its consequences for information systems; it generally informs victims of their right to make a complaint but does not itself alert the relevant authorities to the offences it is aware of.

In February 2011 ANSSI published a national strategy[7] which is currently being updated; a new version should be available in mid-2015.

7 The public section of the French strategy is available at this address: http://www.ssi.gouv.fr/fr/anssi/publications/communiques-de-presse/une-autorite-nationale-et-une-strategie-pour-defendre-et-proteger-la-france.html
EN and DE versions are available.

This national strategy can be summarised in four objectives:

- to be a cyber defence world power and be at the forefront of major nations in this area whilst preserving independence,
- to guarantee France's freedom of choice by protecting its sovereign information,
- to strengthen the cyber security of vital national infrastructure,
- to ensure security in cyberspace,

and seven action points:

- Developing anticipatory and analytical capabilities,
- Improving detection, alert and response capabilities,
- Increasing and perpetuating scientific, technical, industrial and human capabilities,
- Protecting the information systems both of the state and of key infrastructure operators,
- Adapting the law,
- Developing international partnerships,
- Communicating to inform and convince.

3.2 National priorities with regard to cybercrime

Dealing with cybercrime is covered by the 4th objective of the above-mentioned cyber security strategy. Entitled: '*Ensuring Security in Cyberspace*', this objective promotes:

- adaptation of the law both to technological changes and to new uses of the internet,
- the strengthening of international legal assistance in relation to prosecuting offences committed on or using electronic communications networks,
- making information available to and raising the awareness of companies and individuals as to potential risks,
- making information available to victims and providing support.

3.2.1 Strategy of the Ministry of the Interior on cyber threats

On the basis both of the above and of the results of the proceedings of the working group bringing together all the directorates-general, the Ministry of the Interior has drafted its own **ministerial strategy on cyber threats**, which sets out six strategic points:

- point 1: to have a clear and current view of the state of cyber threats at all times;
- point 2: adapt and strengthen the Ministry's capacity to respond to cyber threats;
- point 3: improve levels of awareness and prevention of cyber threats amongst individuals, economic actors and territorial authorities;
- point 4: prepare for the future through research and development, bringing together the academic world and industry;
- point 5: strengthen the security of the Ministry's own information systems;
- point 6: promote the international action taken by the Ministry on the issue of tackling cyber threats.

This action plan has been led since December 2014 by the prefect responsible for combating cyber threats, who has been assigned the task of setting up a delegation to combat cyber crime which will be under the auspices of the Minister for the Interior.

One of the first concrete steps taken to put this ministerial strategy in place, and particularly point 2 thereof, is the creation of the Sub-directorate for the Fight against Cybercrime (*Sous-Direction de la Lutte contre la Cybercriminalité* – SDLC) within the Central Directorate of the Criminal Police (*Direction Centrale de la Police Judiciaire* – DCPJ) in April 2014.

This entity aims to adapt the organisational set-up of the National Police Force to respond to the widespread use of new technology when committing offences, by putting in place a structure touching on all aspects of efforts to combat cybercrime, encompassing operational matters, training and preventive measures focusing on the general public, and the economy.

The evaluation team welcomes this highly useful reorganisation, a detailed description of which is contained in the French response to the GENVAL questionnaire. The evaluators would like to highlight here the planned strengthening of national capacities for the **protection of information systems** to provide support to small and medium-sized companies and the general public as regards cyber attacks, which will be the subject of interministerial proceedings co-chaired by the Ministry of the Interior and ANSSI.

3.2.2 Inter-ministerial working group on tackling cybercrime

Finally, in June 2013, a **dedicated inter-ministerial working group on tackling cybercrime** (*groupe de travail interministériel sur la lutte contre la cybercriminalité*) was set up by the relevant ministers (Justice, Economy and Finance, Interior, Digital Economy).

The remit given the chairman of the inter-ministerial working group, Public Prosecutor Marc Robert, was to **develop an overall strategy for dealing with cybercrime.**

In February 2014, this group presented a very detailed report[8] whose conclusions led to a series of 55 recommendations, covering the following areas: organisation, legislation, preventive measures and raising of awareness amongst the general public, adaptation of resources available for investigations and prosecutions, training for professionals, and the strengthening of international cooperation.

A preliminary observation made by the working group is that there is a need to **better define and understand cybercrime**. To do so, it suggests clarifying the concept, establishing a monitoring body charged with collecting and interpreting all the data on this phenomenon, and developing victimisation surveys for both individuals and companies.

A further essential point developed by the report: **preventing cybercrime**. To aid prevention, the group particularly recommends launching campaigns to raise awareness amongst the general public, arranging training for internet users – 'the first line of their own defence' – and mobilising all relevant professionals in order to find appropriate technical solutions.

[8] http://www.Justice.gouv.fr/include_htm/pub/rap_cybercriminalite.pdf

For the authors of the report, it also appears necessary to **increase the resources available for dealing with cybercrime**. Various measures are suggested to meet this goal: putting in place a centre for cyber attack alerts and responses (it is recommended that this CERT, which is intended for the general public, should take the form of an association, cf. recommendation no. 6), strengthening the training given to judges, police officers, gendarmes and customs officers, as well as creating an inter-ministerial delegation and a horizontal service within the Ministry of Justice that is dedicated to dealing with cybercrime.

The French authorities have not indicated precisely which of the Robert Group's recommendations will definitely be selected, nor the criteria according to which the selections will be made. Nonetheless, the importance of acting upon these recommendations was underlined many times over the course of the on-site visit.

On 15 January 2015 the Ministry of Justice informed the evaluation team that it had just put in place the first recommendation that concerned it, in relation to setting up a horizontal service to be named 'Coordination mission for dealing with attacks on probity and cybercrime' ('*Mission de coordination de la lutte contre les atteintes à la probité et la cybercriminalité*'). Amongst other things, the service will be in charge of coordinating action to prevent and deal with cybercrime by putting in place recommendations from the Robert Report and coordinating the definition of the general instructions on criminal policy that are issued to public prosecutors, as well as the French contribution to the work of European and international courts in its area of expertise.

3.2.3 Links with the EU 'Cybercrime' Priority

The national priorities in part take into account the strategic objectives defined by the EU in the 'Cybercrime' Priority. Similarly, the Robert Group's work is in line with the European strategy defined in February 2013, and existing European instruments for dealing with cybercrime have been taken into account when drafting the recommendations contained in its report.

Some examples of French initiatives which are in line with EU priorities include:
- the White Paper on Defence and National Security of June 2008, and the subsequent White Paper of April 2013,
- the creation of the National Agency for the Security of Information Systems (ANSSI) in July 2009,
- the creation of a platform on which to report illicit internet content,
- the establishment of specialised working groups, such as the Observatory for Payment Card Security (*Observatoire de la sécurité des cartes de paiement*) created within the Banque de France.

France is also putting in place a policy focusing on prevention, the development of reporting and improving the training of those involved, in particular as regards prevention.

For instance, it is participating in the EU's 'Safer Internet' programme, financed by the European Commission, which in France has been managed by the Delegation on Internet Usage (*Délégation aux usages de l'internet*) since 2005. Safer Internet France brings together three complementary services aimed at protecting and educating minors:

- *'Internet sans crainte'* ('Internet without Fear'), the national initiative aimed at raising awareness of internet-related issues and risks among children and young people.
- *'Point de Contact'* ('Point of Contact'), the platform for reporting offensive content, managed by the French Association of Internet Access Service Providers (*Association des Fournisseurs d'Accès et de Services Internet* – AFA).
- 'Net Ecoute' ('Net Listening'), the national helpline for the protection of young people, managed by the '*e-Enfance*' ('E-childhood') association.

At the end of 2013, the French government launched a national campaign to prevent harassment and cyber violence in schools.

3.3 Statistics on cybercrime

3.3.1 Main trends leading to cybercrime

The detailed information provided by the relevant police departments in the French response to the GENVAL questionnaire all points to the same broad cybercrime trends. Their observations are consistent with the summary inserted in the Robert Group's report.

(1) The number of cybercriminals is increasing, largely due to developments in technology, which is becoming simpler to use and more easily accessible to those without expert knowledge. The black market in viruses and other malicious software is flourishing on the internet. The growing use of anonymising services has led to a sharp increase in criminal behaviour, as it gives users a sense of impunity.

(2) Cybercrime is taking increasingly diverse forms.

- **Ordinary cybercriminals** are by far the most common: sex offenders (*child pornography, organised procuring*), violent cyber offenders (*threats, insults, defamation, online harassment, sectarian violence*), online fraudsters – the many types of fraud are becoming even more diverse (*phishing, employment scams, locking computers with ransomware, etc.*) and banking fraud is flourishing (*interception of banking details online, skimming, hacking traders' payment terminals, etc.*), as is counterfeiting linked to the expansion of e-commerce (*counterfeiting of branded products, software, intellectual property products, medicines, etc.*) – and online traffickers (*synthetic drugs, laundering of the proceeds of crime, etc.*).
- **Cybercriminals who aim their attacks at state entities and key operators:** cyber mercenaries, cyber spies (economic cyber espionage is a major threat) and cyber terrorists driven by extremist ideologies

(3) The victims of cybercrime fall into every category: the general public, companies, and public services are all targets.

Children, vulnerable people and the elderly are particular targets for sex offenders and cyber fraudsters. Small and medium-sized enterprises (SMEs) and manufacturers are the preferred targets of cyber attacks on automated data processing systems. According to a recent study carried out by an anti-virus software developer, over a third of French companies with fewer than 250 employees were victims of this kind of attack in 2013, an increase of 42% on the previous year. Targeting SMEs and subcontractors also allows hackers to indirectly attack large industrial and commercial corporations. The state and businesses which are sensitive for reasons of national sovereignty are not immune to attacks either; in the last four years, France has recorded around 100 large-scale cyber attacks on, for example, political institutions, ministries, law enforcement authorities, operators of vital importance, and so on, not all of which have been made public.

(4) The methods used by cybercriminals are becoming more and more diverse and complex.

The use of malicious software is increasingly common nowadays in France. This kind of hacking software, which is mainly sold on websites hosted in the United States, allows even novice users to take remote control of other computers for unlawful or malicious purposes (denial of service attacks, taking remote control of targeted computers, fraudulently capturing personal details, particularly banking details).

(5) As regards the sexual abuse of children and child pornography, the French police have observed the following trends: the continued use of peer-to-peer file sharing, through both conventional platforms and specific software such as Gigatribe, which allows private, encrypted exchanges; more and more frequent use of private internet networks (darknets); and the development of live streaming (paid-for live viewing of sexual assaults on minors).

The French authorities in their response to the questionnaire and the practitioners interviewed during the on-site visit also emphasised the **sharp increase in the proportion of computerised analysis used in investigations.**

Storage capacity is expanding rapidly and increasing the quantity of data to be analysed. Moreover, the analysis is proving trickier to carry out, due to criminals' increasing expertise and the development of new tools which they can use to delete, hide or encrypt data.

3.3.2 Number of registered cases of cybercrime

The on-site visit and the responses provided by the French authorities highlighted two important points regarding the reliability of administrative statistics on cybercrime.

1. Currently, the French statistical framework does not give a precise idea of the number and type of cyber offences recorded and/or punished, or the number of people investigated, prosecuted or convicted for cybercrimes.

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

This is why, from 2015, the statistics department at the French Ministry of the Interior will produce its figures on cyber criminality using new indicators, which are currently being tested. Figures from other public or private sources will be evaluated and progressively analysed during the course of 2015.

The statistical data held by the Ministry of Justice essentially concerns offences identified as cybercrimes which led to a conviction. The data is very limited, either because the reported offences were not prosecuted or the offenders were discharged, or because the convictions they led to were recorded in a different set of statistics.

Instances of information systems hacking which led to a conviction totalled 114 in 2008, 157 in 2009, 254 in 2010, 167 in 2011 and 185 in 2012. 330 convictions for child sexual abuse online and child pornography were recorded in 2008, 319 in 2009, 349 in 2010, 426 in 2011 and 569 in 2012. Offences in which computers and information systems were either the weapon or the target numbered 596 in 2008, 602 in 2009, 519 in 2010, 366 in 2011 and 504 in 2012. Offences identified as cybercrimes accounted for the following annual percentage of all offences leading to a conviction over the five-year period in question: 0.10 % in 2008, 0.11 % in 2009, 0.11 % in 2010, 0.10 % in 2011 and 0.13 % in 2012.

On the basis of these figures, the amount of judicial litigation related to cybercrime in France seems both negligible in relation to the real scope of this criminal phenomenon there, and far too stable in terms of development.

2. The 'dark figure' of cybercrime, i.e. the number of offences, including serious ones, not reported to the law enforcement authorities, is very high.

- According to the Robert Report, many victims do not report offences to the law enforcement authorities, either because according to the law they have an easier way to obtain compensation (e.g. in the case of banking fraud), or because they see little point in doing so; this is most common among private individuals, and many businesses also refrain from reporting offences, mainly to preserve their image.

Internet professionals are not obliged to report any but a few serious offences.

- The evaluation team observed that the transfer of information between the various public entities responsible for the correct functioning of the Internet could be improved, in particular in terms of reporting any criminal offences of which they may be aware to the law enforcement authorities.

During the on-site visit, the evaluation team observed that public entities did not systematically report to the competent judicial authorities offences of which they were aware, but that they did inform victims on each occasion of their right to file a complaint. However, Article 40 of the French Code of Criminal Procedure obliges '*any established authority, public official or government employee who, in the performance of his duties, acquires knowledge of a crime or an offence [to] notify the public prosecutor without delay*'.

Following the visit, the French authorities wished to point out that, in addition to informing victims of their right to report offences, and in certain cases strongly encouraging them to do so, ANSSI was also cooperating directly and on a regular basis with the competent departments of the Ministry of the Interior, and was undertaking to cooperate with the Ministry of Justice in the context of judicial investigations in the field of information and communication technologies; that the permanent secondment of a law enforcement officer to ANSSI, a hitherto unheard-of situation at European level, reflected an intention to harmonise technical incident response operations with the law enforcement authorities; that the officer in question informs victims of their rights, and may in certain cases strongly encourage them to report offences; and that ANSSI also responds to questions concerning the specific features of procedures in relation to information and communication technologies.

The French authorities added that ANSSI acts only in relation to a very limited range of offences linked to cybercrime (attacks on ADP systems); that its permanent links with the law enforcement authorities mean that the latter are notified of virtually all the Agency's commitments, and indeed are themselves involved in the event of a judicial referral; and that, moreover, since ANSSI has no organisational links with judges or cybercrime practitioners, any decision as to whether to bring offences to their attention is left to the judgment of the specialist departments and regular and legitimate partners of those judicial authorities.

The French authorities take the view that, consequently, there is no 'concealment' of such offences or the way in which they are taken into account at national level.

The evaluation team is fully aware that making it obligatory to report offences to the law enforcement authorities could undermine victims' trust in the state in cases in which they wish to remain anonymous. Ultimately, however, this failure on the part of state bodies to report cybercriminal offences is leading to the privatisation of prosecution. It should not be left up to individual operators to decide whether prosecution is appropriate, as their decision on how a criminal threat should be followed up will be based not on the general interest but on their own commercial or financial interests.

Furthermore, systematically reporting cyber attacks to the national law enforcement authorities, even if it does not lead to prosecution, would allow those authorities to share certain information with their foreign counterparts and would make it easier to evaluate the criminal threat, its impact and the counter-measures to be implemented.

Despite these difficulties, the French authorities are making every effort to use the available data (judicial record, operational police and gendarmerie files, victimisation surveys, etc.) as effectively as possible. These elements are made available to the French National Supervisory Body on Crime and Punishment (*Observatoire National de la Délinquance et des Réponses Pénales*), which each year publishes the key figures on crime in France[9]. In 2013, 2 735 attacks on automated data processing (ADP) systems were recorded by the police and the gendarmerie. Between 2012 and 2013, the number of recorded attacks on ADP systems increased by 20%, or 462 incidents. Just under 48 000 fraud offences committed using the internet were recorded in 2013, up from 30 000 the previous year. The same year, the police and the gendarmerie recorded 2 905 attacks on personal dignity and violations of personality rights via the internet (up from 2 300 in 2012) and 550 sexual offences committed using the internet (up from 455 in 2012).

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

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

- Within the National Gendarmerie, in addition to the budgets allocated at the initiative of the central and regional units, the Directorate-General sets aside a large budget specifically to train and equip investigators specialised in the fight against cybercrime. France is seeking EU funding for this under the Internal Security Fund and the Hercules III programme.

9 http://www.inhesj.fr/sites/default/files/ra-2014/synthese_ra-2014.pdf

- The Internet Group of the Child Protection Unit (*Brigade de Protection des Mineurs*) within the Paris Police Headquarters (*Préfecture de police de Paris*) receives specific budgetary allocations, particularly for new technology, from both the Police Headquarters and the multiannual equipment plan. In 2013, in addition to the funds allocated to the IT service of the Paris Regional Directorate of the Criminal Police (*Direction Régionale de la Police Judiciaire de Paris*), which serves its various units, the Directorate also received an additional EUR 53 000 in funding for the purchase of software to fight cybercrime and specialised IT equipment.

- With regard to EU funding, DG HOME published a Targeted Call for Proposals on 'cybercrime' under the ISEC 2013 framework. The French Ministry of the Interior did not submit a project, but a submission by a private French company was selected for EU co-financing. The project, entitled 'EU-PI, European Union anti-Phishing Initiative', was submitted by the company LEXSI and will be implemented in partnership with the companies SMILE (LU), the Signal-Spam association (FR) and ECSG (NL), Luxembourg's Ministry of Economic Affairs and Foreign Trade (LU), Europol (EC3) and the Phishing-Initiative association (FR). The project has a budget of EUR 553 222.64; EU co-financing will total EUR 488 871.64 (i.e. an EU co-financing rate of 88.37%).

- In the context of the shared management of the ISF Police funding, one of the priorities of France's draft national programme is strengthening the ability of the French law enforcement authorities to prevent, detect and prosecute cybercrime. Subject to approval by the European Commission, the programme is intended to focus on public-private partnerships and cooperation with third countries which are the source of offences committed against EU citizens.

France's draft national programme also provides for co-financing of the EU policy cycle. Co-financing from the national envelope of the ISF Police could be requested for the implementation of EMPACT projects related to the fight against cybercrime.

3.5 Conclusions

- The National Agency for the Security of Information Systems (ANSSI) is the main pillar of the French cyber security system, and, as such, receives substantial funding, commensurate with the scale of the challenges it deals with. Cooperation with law enforcement authorities, particularly judicial authorities, is limited to the handling of information attacks targeting operators of vital importance. In other cases, it is not systematic, and is even avoided in order to protect confidentiality.

- The Ministry of the Interior recently set out a ministerial strategy on cyber threats which includes a section on 'cybercrime'; this includes, among other things, an effective reorganisation of the ministry's services. In connection with the implementation of that strategy, a prefect responsible for combating cyber threats has been appointed in the run-up to the creation of a delegation responsible for combating cyber threats in 2015.

- The Ministry of Justice, which is responsible for France's general criminal policy, has not yet implemented a strategy.

- The report of March 2014 by the Robert Group, an inter-ministerial working group, provides a comprehensive picture of the fight against cybercrime and includes a number of forward-looking elements; it contains a list of highly relevant and innovative recommendations for the development of a national strategy to fight cybercrime. This policy review by France is to be applauded, and other Member States must be encouraged to adopt a similar approach.

- The Robert Report contains 55 recommendations. The GENVAL evaluation team was able to confirm the validity of many of these recommendations during its visit. To follow up on this excellent report, a methodology should be drawn up to establish priorities among the recommendations and agree a timetable for their implementation.

- The rate of undetected cybercrime in France can be attributed, inter alia, to insufficient reporting of incidents to the judicial authorities, not only by victims but also by public entities (such as ANSSI and the CNIL) which are aware of offences which, by their nature or their scale, are considered serious.

- Furthermore, failing to systematically report offences compromises the effectiveness of the fight against cybercrime. Except with regard to victims of an attack on an automated data processing system, individuals and companies whose data have been compromised are not systematically identified and informed, and consequently are unable to take the appropriate steps to minimise any damage, while those responsible are not prosecuted and are therefore free to reapply the same methods to other targets, both nationally and internationally.

- The systems currently used by the French law enforcement authorities to record offences yield some very useful qualitative data but are unable to provide a quantitative overview of reported cybercrime, either as a whole or broken down by type of offence. This is a symptom of the broader difficulty that France, like many other countries, still faces when it comes to developing a comprehensive methodology to fight an extensive and diversified criminal phenomenon.

4 NATIONAL STRUCTURES

4.1 Judiciary (prosecution and courts)

4.1.1 Internal structure

France has no prosecution services or criminal courts that specialise in cybercrime. All of the country's jurisdictions are responsible for dealing with cases connected in some form or another with cybercrime, on the basis of the general criteria for territorial jurisdiction defined by law, which are, in order of priority: the place in which the offence was committed; the suspect's place of residence; the suspect's place of arrest or detention.

The on-site visit revealed that the rules for allocating cases to a particular jurisdiction are not clear and that such decisions seem to be taken on a case-by-case basis. Consequently, and because of the complexity of the subject, which deters many practitioners who have not been adequately trained, there have been a number of occasions on which public prosecutor's offices have declined jurisdiction (for example on the basis of place of residence once the perpetrator has been identified). This sometimes has a certain demotivating effect on the police services involved. According to the judges interviewed during the visit to France, it is likely that there are a number of untried cases across France, especially outside Paris.

The above rules on jurisdiction can vary in certain circumstances:
- The Paris public prosecutor's office has specific jurisdiction in terrorism cases.
- In the event of proceedings initiated simultaneously by multiple prosecution services, the proceedings can be grouped together in the main jurisdiction.

- The eight specialised inter-regional courts (*juridictions interrégionales spécialisées*, JIRS) that were set up in 2004 may intervene in certain cases involving cyber attacks or online fraud, but their competence is limited to cases that are very complex owing to the large number of perpetrators, accomplices or victims involved, or to the geographical jurisdiction over which they extend. While this is quite often the case with cybercrime, in practice the JIRS rarely become involved.

In reality, the public prosecutor's offices that deal with the greatest number of cybercrime cases are those in the Paris region and the biggest provincial cities. The practices followed by these jurisdictions indicate that cases involving cybercrime (with the exception of child pornography and the press) are generally dealt with by the economic and financial departments of the relevant public prosecutor's office. In addition, some of those offices have set up their internal organisation to include a 'specialist judge' (*magistrat référent*) for cybercrime, who can provide technical support to colleagues involved in cybercrime cases. The Paris public prosecutor's office – which, given its location, has jurisdiction over most larger-scale cyber attacks – has created a specialised unit comprising two prosecutors and an assistant. While it is commendable to have this kind of specialisation, which appears to be unique in France, the unit seems understaffed in relation to the number of cases that come before the Paris courts.

4.1.2 Capacity and obstacles for successful prosecution

A. Capacity.

- Specialist judges for cybercrime

A 'cybercrime specialist' is appointed within each of France's local prosecution services to act as the preferred contact point for their colleagues and the investigation services. The cybercrime specialist sets up a system for monitoring legislation and case-law and forwards relevant documentation to their colleagues.

The on-site visit revealed that the system of specialists has a lot of room for improvement: there is a high turnover, the specialists do not systematically receive training to fulfil their tasks, and their role is not always very 'visible' to their colleagues.

- Relations between judges and the specialised investigation services

Some public prosecutor's offices regularly meet with the specialised investigation services so that they can gain a greater understanding of the specificities of each other's work and the division of competences between the services. In addition, such meetings help to clarify which investigative tasks can be requested of local police so as not to overburden the specialised services.

B. Obstacles. The French authorities indicate that the main obstacle to successful prosecutions is identifying the perpetrators of the offence. Other specific obstacles were identified by the investigation services:

- Victims do not bring a complaint, because they are discouraged from doing so or fear for their professional reputation.
- Enforcement methods are unsuitable for dealing with mass crimes (e.g. online fraud).
- Special investigation techniques (undercover investigations) are still underused.
- Greater coordination is needed in investigations.
- Legal proceedings are slow (in particular international requests for mutual legal assistance).

- The basic acts need to be simplified at European level (e.g. identification of an IP address, email address, phone number or bank account); in particular, the lengthy judicial process prevents rapid interception of computer servers involved in cyber attacks.
- There is no requirement for foreign operators to respond; responses to requests are inconsistent and often too slow, especially by foreign operators (Facebook, Yahoo, Amazon, Google, etc.) which are under-equipped to provide such a response (N.B. France ranks among the world's top three countries in terms of number of requests).
- It is difficult to trace internet connections made using smartphones (technical issues and/or reluctance on the part of operators).
- Foreign operators have a different legal status and respond according to their own confidentiality rules or only for connections positively identified in France or Europe.
- Certain proxy or VPN servers and many types of information security equipment frequently do not have server logs (despite the availability of such a feature), providing criminals with total anonymity and erasing all evidence.
- Data are not kept for long enough (or at all) in partner countries, including European countries.
- Different countries have different admissibility criteria for evidence.
- There are too few or no specialised courts.
- Judges lack knowledge or training.

These points were raised by the inter-ministerial working group on cybercrime, which translated them into a set of recommendations in the final report. The Ministry of the Interior's working group on cyber threats has also taken account of them in its action plan.

4.2 Law enforcement authorities

4.2.1 Central and regional services specialising in cybercrime

Within the Ministry of the Interior, the central and regional services responsible for combating cybercrime are under the authority of the Directorate-General of the National Police (*Direction Générale de la Police Nationale* – DGPN), the Police Headquarters in Paris (*Préfecture de police*) and the Directorate-General of the National Gendarmerie (*Direction Générale de la Gendarmerie Nationale* – DGGN). It should also be noted that the Directorate-General for Internal Security (DGSI) has jurisdiction over investigations into cyber attacks with a national security component.

I – Police services

THE CENTRAL SERVICES:

► **Sub-directorate for the Fight against Cybercrime (SDLC)**

This service, created in April 2014 as part of the strategy of the Ministry of the Interior, undertakes prevention and enforcement in the field of cybercrime and is also responsible for defining operational strategies, training strategies, and prevention strategies focusing on the public and the economy. The SDLC was created to be the focal point for the actions undertaken by the Ministry of the Interior at national level, and to be clearly identifiable to its institutional partners, stakeholders in the digital economy and private individuals. In particular, it includes the **Strategic Coordination Office** (*Bureau de coordination stratégique)* and an **Awareness and Analysis Division** (*Division de l'anticipation et de l'analyse*), as well as:

- **The Central Office for Combating Information and Communication Technology Crime(*Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication* – OCLCTIC), which is responsible for:**

- organising and coordinating the operational implementation of the fight against perpetrators of offences relating to information and communications technology; the regional directorates of the Criminal Police are closely involved in the operation of the centralised national system for combating cybercrime, in close coordination with OCLCTIC;
- undertaking any investigation activities and technical investigative work at the request of the judicial authority;
- upon request, assisting the police, gendarmerie and customs with cases involving high-tech crime;
- on its own initiative and with the consent of the judicial authority, gathering on-site information concerning local investigations;
- centralising and disseminating information about high-tech crime to all law enforcement services.

The OCLCTIC is the operational point of contact available 24/7, within the meaning of the Budapest Convention. The point of contact can be reached by telephone or at a dedicated email address. The request must be in English and include the formal requirements (details of the investigation, time stamps, etc.). Once compliance with the request is confirmed, it is sent by or to the French host/provider if it is from a foreign country, or to the foreign point of contact if it is from one of the French police services.

The point of contact also oversees the preservation of data and provides initial technical or legal advice to the services that request it.

As regards attacks on the information systems of the state or of key operators, there is a 24/7 operational point of contact within ANSSI, at its Operational Centre for the Security of Information Systems (*Centre Opérationnel de Sécurité des Systèmes d'Information* – COSSI).

The OCLCTIC is responsible for providing training for cybercrime investigators (ICC) which is open to all directorates of the National Police Force (DCPJ, DCSP, IGPN, DCPAF, Police Headquarters in Paris) and the DGSI. 377 cybercrime investigators spread throughout the territory have been trained by the OCLCTIC.

► **Central Office for the Prevention of Violence against Persons (*Office central pour la répression des violences aux personnes* – OCRVP):**

The OCRVP reports to the Ministry of the Interior's Sub-directorate for the Fight against Organised Crime and Financial Crime. This office has jurisdiction over all cybercrimes relating to child pornography and is responsible for organising, coordinating and centralising related investigations by the criminal police in conjunction with the National Centre for the Analysis of Child Pornography Images (CNAIP). It is also responsible for providing documentary and analytical assistance to the regional branches of the national police and gendarmerie. One of the priorities assigned to it is to develop undercover investigation techniques by training 'cyber patrols' throughout the country.

Regional specialised branches of the criminal police:

The inter-regional directorates of the criminal police (*directions inter-régionales de la police judiciaire* – DIPJ) and the regional directorates of the criminal police (*directions régionales de la police judiciaire* – DRPJ). At regional level, the criminal police consist of:

- Nine inter-regional directorates of the criminal police (Bordeaux, Dijon, Lille, Lyon, Marseille, Orléans, Rennes, Strasbourg and Pointe-à-Pitre DIPJ) composed of one or more regional departments (*services régionaux de police judiciaire* – SRPJ) and one or more branch offices;
- Three regional directorates of the criminal police (Paris, Versailles and Ajaccio).
- Their territorial jurisdiction covers from two to eight departments. The DIPJ and DRPJ are closely involved in the centralised national system put in place to combat organised and specialised crime.

Within those territorial services, the Paris Regional Directorate of the criminal police, attached to the Paris Police Headquarters, has specialist services with regional jurisdiction (Paris and the neighbouring departments). There are seven such services, of which three are responsible for dealing with cybercrime:

- **Information Technology Fraud Investigation Unit (*Brigade d'Enquêtes sur les Fraudes aux Technologies de l'Information* – BEFTI)**

The first service created to combat cybercrime (1994), BEFTI
deals with the most complex cases, while simpler cases are dealt with by local police. That being the case, and given that its activities extend over the most dynamic territory in France, it can be classified as a central service.

BEFTI has jurisdiction over offences involving attacks on information systems and the personal data contained therein, software and database counterfeiting and attacks by suppliers and providers of electronic communications. It assists all the services over which it has jurisdiction with forensic investigations, the legal analysis of digital media and digital investigations. It provides other police officers with training on this subject and raises awareness among the public, businesses and public authorities. This very active unit takes part in a number of seminars, conferences and associations to share knowledge and improve practices.

- **Payment Fraud Unit (*Brigade des Fraudes aux Moyens de Paiement* – BFMP)**

The tasks of the BFMP include investigations into offences relating to digital payment methods; in particular, it is in charge of bank card fraud, e-commerce involving fraudulent use of bank card details, and credit fraud including identity theft, forged documents, fraudulent credit and the opening of fraudulent bank accounts.

- **Child Protection Unit (BPM)**

This unit has exclusive competence in cases involving juvenile victims in the greater Paris region. The BPM Internet Group is responsible for cases which contain a 'cyber' component. The group is divided into two main teams:

- The Technological Investigation, Innovation, Research and Assistance Team (*Pôle 'Investigation Innovation Recherche Assistance Technologique'* – PIIRAT) is responsible for investigations into the possession and distribution of child pornography images, the corruption of minors via the Internet and the use of the Internet to commit sexual abuse, as well as providing the other groups with technical assistance in the use of various media which may contain child pornography images. It seeks innovative solutions that will allow data media to be processed quickly and as thoroughly as possible, within custody deadlines and in parallel with hearings.

- The Cyber Infiltration and Internet Initiative Team (*Pôle 'Cyberinfiltration et Initiative Internet'*) comprises specially trained undercover investigators to combat sexual offences against minors committed via an electronic telecommunications network. Working on their own initiative, the cyber investigators set up and maintain online profiles, posing as predators and potential victims in order to make contact with paedophiles.

II – Gendarmerie services

The French gendarmerie is a security force with military status attached to the Ministry of the Interior. It has an integrated structure, i.e. its various roles, one of which is the criminal police, are performed at all regional levels in France. This also applies to the fight against cybercrime. With regard to cybercrime, its actions are steered by the Centre for the fight against digital crimes (*centre de lutte contre les criminalités numériques* – C3N)[10], in cooperation with the other services of the Ministry of the Interior.

The Centre for the fight against digital crimes (C3N):

- coordinates and steers the actions of the gendarmerie in combating cybercrime through the use of both investigation and forensics;
- is the contact point within the gendarmerie for all central offices of the criminal police;
- focuses on three main areas of activity:

[10] After the evaluation visit had started, the gendarmerie's Centre for the fight against digital crimes took over from the Cybercrime and Digital Analysis Investigation Board (*plateau d'investigation cybercriminalité et analyses numériques* – PICyAN) and the Cybercrime Unit (*division de lutte contre la cybercriminalité*).

A. Investigation C3N:

- monitors the various virtual spaces in order to detect and define offences. This monitoring may include undercover investigations. C3N also coordinates undercover investigations by regional units of the gendarmerie.
- leads investigations, or supports investigations led by the central office of the gendarmerie and the regional units, and runs particularly large-scale, serious or sensitive operations.
- administers CALIOPE, the national database of child pornography resulting from criminal investigations, in cooperation with INTERPOL and foreign counterparts in the National Centre for the Analysis of Child Pornography Images (*Centre national d'Analyse d'Images de Pédopornographie* – CNAIP).

B. Forensics At the request of judges and investigators, C3N carries out expert assessments and complex technical examinations of digital evidence:

- Retrieval of data from electronic, magnetic or optical media.
- Analysis of systems and networks.

C. Supporting and managing the regional network of the gendarmerie C3N's work also includes:

- a telephone and internet 'one-stop shop' (*guichet unique téléphonie et Internet* – GUTI) which acts as an intermediary between operators and gendarmerie investigators and liaises with the National Platform for Judicial Interceptions (*plateforme nationale des interceptions judiciaires*). In 2013 it dealt with more than 7 300 cases.
- the provision of training, equipment and information support for the group of specialist investigators within the units.
- research and development.

At regional level, the investigation units and judicial support units comprise 260 specialist investigators who have earned a professional qualification (NTECH) in digital technology (forensics and investigation) and/or are trained in undercover investigation. Furthermore, inter-regional groups to combat cybercrime have recently been created within the investigation units attached to the specialised inter-regional courts (JIRS). These groups carry out targeted online monitoring, run their own investigations or support investigations by other groups in their unit into offences that come under the jurisdiction of the JIRS.

At departmental level, the judicial investigation and intelligence teams comprise more than 200 NTECH investigators (around 260 NTECHs in total, in all units) who essentially provide forensic support to the investigators in their units within their remit.

At local level, there are almost 1700 digital technology correspondents (C-NTECHs) who assist the NTECHs with simple forensic or investigative tasks. These correspondents support the basic units, for whom online training in digital technologies has been set up (P-NTECH).

4.3 Other services

While they were not part of the on-site visit, the Directorate-General of Customs and Excise (*Direction Générale des Douanes et des Droits indirects* – DGDDI) and the Directorate-General for Fair Trading, Consumer Affairs and Fraud Control (*Direction Générale de la Concurrence, de la Consommation et de la Répression des Fraudes* – DGCCRF) were mentioned on several occasions as stakeholders in France's fight against cybercrime. Their contribution was particularly emphasised during the presentation of the PHAROS platform and in relation to the activities of the **'Cyber Customs' Unit (*cellule 'Cyberdouane'*)**, which is responsible for gathering and using intelligence in order to combat online fraud linked to the trafficking of prohibited, restricted or highly taxed goods. This monitoring work can result in judicial investigations by the National Customs Judicial Service (*Service National des Douanes Judiciaires* – SNDJ).

4.4 Public-private partnership

In France there are many examples of public-private partnerships to prevent and combat cybercrime:

- the above-mentioned links that the OCLCTIC maintains with a hundred or so partners;
- the Observatory for Payment Card Security (OSCP), described in 6.2;
- the Signal Spam organisation created in 2003;
- the Phishing Initiative organisation created in 2011 by Microsoft, Paypal and CERT-LEXSI (IT security survey laboratory) to prevent phishing to obtain personal bank details;

- partnerships with certain professionals not primarily associated with digital technology, such as the partnership between the gendarmerie and the insurance company AXA to create the 'Permis Internet' (internet licence) described in 5.A.5, which the police plan to extend into areas for which they are responsible;

- partnerships with child protection associations, such as that of the Ministry of National Education with e-Enfance against cyber bullying in school, and the gendarmerie with Innocence in Danger for the provision of a tool to detect child pornography on peer-to-peer networks;

- participation in the European Commission-funded Safer Internet programme via the Safer Internet France programme aimed at raising awareness among and providing support to young people;

- partnerships with universities (e.g. the gendarmerie's partnership with the University of Technology of Troyes aimed at training investigators in digital technologies) and other teaching and research institutions (e.g. the police with the EPITA computer engineering school for certain projects);

- the Internet Rights Forum (*Le Forum des droits sur l'Internet)*, a 2004 initiative in the legal sphere, as well as all the other public and private professional associations dealing with digital technologies;

- an agreement which will help promote and spread a culture of economic security among chambers of commerce and industry, businesses, industries and competitive clusters at local level is soon to be signed with the Ministry of the Interior.

- the establishment of agreements within the Paris Police Headquarters to take on interns from renowned computer science schools with a view to exchanging knowledge and forming lasting partnerships with the chamber of commerce and industry in the Ile de France region in order to spread the information to very small, small and medium-sized enterprises.

Lastly, **a French Anti-Cybercrime Expert Centre (*Centre expert contre la cybercriminalité français* – CECyF) has been created**. The centre was set up under the European Commission-funded 2CENTRE project, the aim of which is to create centres of excellence in Europe in the field of fighting cybercrime, bringing together institutional, academic and industrial players. CECyF's objective is to visibly group together initiatives and launch, support, conduct or secure funding for collaborative projects in the field relating to training, organisation, monitoring, research and development. The centre has many members, among whom the founding members are the gendarmerie, the customs authority, the tax authority, the University of Technology of Troyes, the University of Montpellier I, EPITA, Thalès Communication & Security, Orange France, Microsoft France, CEIS (co-organiser of the International Forum on Cybersecurity (FIC) along with the gendarmerie), the French-speaking Association of Computer Forensics Specialists (*Association francophone des spécialistes de l'investigation numérique* – AFSIN) and the International Botnets Fighting Alliance (IBFA, which organises Botconf).

4.5 Cooperation and coordination at national level

- Regarding the 'Acts unique to information systems, in particular those related to cyber attacks' part of the definition of cybercrime proposed in the GENVAL questionnaire, preventive and reactive actions are coordinated by ANSSI, the French National Agency for the Security of Information Systems mentioned earlier. The agency is responsible for taking or coordinating all action aimed at foiling attacks on information systems and reacting in the event that their confidentiality, availability or integrity is threatened. Its work primarily serves the state and key private sector operators.

- Unlike cyber defence, the fight against cybercrime is not centralised: it is conducted independently by each of the ministries concerned – primarily the Ministry of the Interior, the Ministry of Justice, and specialised administrations such as Customs. Within the Ministry of the Interior, the police and the gendarmerie are coordinated by different entities for the bulk of their operational work.

Within the Ministry of Foreign Affairs and International Development, there is an ambassador responsible for the fight against organised crime who coordinates the ministry's work in the field of cybercrime in cooperation with the ambassador appointed as 'cyber-security coordinator'.

Lastly, there are several financial and economic coordination and regulatory bodies:

- ARJEL (*Autorité de Régulation des Jeux en Ligne* – French regulatory authority for online gambling), created by Law No 2010-476 of 12 May 2010;
- HADOPI (*Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet* – high authority for the distribution of works and protection of rights on the internet);
- GCB (*Groupement des Cartes Bancaires* – CB bank card group), created in 1984;
- OSCP (Observatory for Payment Card Security), created by Law No 2001-1062 of 15 November 2001.

4.5.1 Legal or policy obligations

- ANSSI's role and means of action in relation to cyber defence were strengthened in 2013; it can now enforce IT security rules laid down in cooperation with key operators, who are obliged to implement them in respect of their critical information systems. In future, key operators must declare certain incidents which occur on those information systems. The Prime Minister can have security checks conducted on the systems. Crisis organisation is tested regularly via Piranet exercises. The process of updating this government plan is currently under way and will be complete by the end of 2015. The 2015 Piranet exercise to take place at the end of the year will be designed to test capabilities for reporting to ANSSI.

- The responsibility and prerogatives of internet access providers and hosts as regards illegal content distributed or hosted by them are governed by Law No 2004-575 of 21 June 2004 on 'confidence in the digital economy', which implements the Directive on e-commerce. That Directive requires hosts to promptly delete any manifestly illegal content of which they aware, failing which they will face civil and criminal liability.

The law also allows anyone who can demonstrate that the illegal content is harmful to their interests to apply for a court order for its deletion, under emergency proceedings, to prevent or put an end to that harm.

The law obliges internet access providers and hosts to join forces to combat the distribution of the most offensive content (child pornography, racism, images detrimental to human dignity, etc.); they must also put in place an easily accessible and visible system enabling anyone to bring such content to their attention. **In this context, OCLCTIC signs agreements with content hosts and publishers on reporting illegal content to the PHAROS platform.**

Hosts or access providers must also save data to enable identification and comply with requests sent via the 24/7 channel.

The private sector must apply decisions by the judicial authority, and comply with its requests and those of the law enforcement authorities.

- Regarding traffic data retention, access providers and hosts are obliged to keep data for one year.

As regards preventing and responding to IT attacks, key private sector operators are obliged to:
- implement the technical measures provided for by ANSSI, at their own expense;
- declare some types of incident that occur on their critical information systems;
- allow security checks on their critical information systems;
- in the event of a major crisis, implement technical measures identified by ANSSI.

4.5.2 Resources allocated to improve cooperation

Observatory for payment card security (OSCP)

The Observatory was created by Law No 2001-1062 of 15 November 2001. Composed of elected members, the Governor of the Bank of France and representatives of government ministries, payment card issuers, the National Consumer Council (*Conseil national de la consommation*) and commercial businesses, it notably includes a representative of the Ministry of Justice, a representative of the Ministry of the Interior and a representative of the Ministry of Defence.

The OSCP's remit is essentially to promote dialogue on the issue of payment card security, raise awareness among issuers and traders, monitor technological developments in the area of payment cards and monitor fraud development. Fraud development is measured annually on the basis of data provided by financial institutions.

The OSCP model was adopted at European level with the creation of the 'SecuRe Pay Forum', though the latter has a broader mission as it is competent for all payment means.

The inter-ministerial working group on cybercrime recommended extending the OSCP's sphere of competence to all payment instruments other than cheques in order to cover, in addition to payment cards (Article L133-4 of the French Monetary and Financial Code):

- online banking (a major cybercrime target via specialised computer viruses);
- SEPA transfers (in particular when carried out electronically);
- electronic money and payment accounts;
- even the digital unit of account bitcoin (primarily used for legal and illegal online transactions and recently the subject of a warning issued by the monetary authorities in view of the unit of account's highly speculative nature and the frequent hacking of electronic portfolios).

Specialised gendarmerie and police investigators have been trained and equipped to deal with the technological constraints involved in fighting payment card fraud.

Lastly, as regards **strengthening and improving cooperation with the private sector**:

- The Central Office for Combating Information and Communication Technology Crime (OCLCTIC) works in partnership with around 100 associations, hosts and internet community service providers.

The office is also preparing for the creation of an **Internet Bureau** (*Bureau de l'internet*) which is to act as an intermediary between internet service providers (hosts, IAPs, social networks, etc.) and investigation services. That unit will record service providers' details and make them available to investigators in local services. It will act as mediator if there are practical or legal difficulties in obtaining investigative data.

- As regards the gendarmerie, cybercrime experts have invested in several successful partnerships mentioned under 9.5. In addition, GUTI, its telephone and internet 'one-stop shop' within the Centre for the fight against digital crimes (*centre de lutte contre les cybercriminalités numériques* – C3N) of the Central Criminal Intelligence Unit (*service central du renseignement criminel* – SCRC), facilitates exchanges between gendarmerie investigators and telephone operators or other internet access providers.

- The role of intermediary is also assigned to the operational department (gendarmerie and police) of the National Platform for Judicial Interceptions (PNIJ), currently in the final phase of development with the Ministry of Justice's department responsible for ordering judicial interceptions (*délégation aux interceptions judiciaires* – DIJ).

- The Paris Police Headquarters carries out actions to the benefit of the private sector and civil society, as well as at major events (e.g. fairs such as the *Foire de Paris* and *Salon des Seniors*), and helps the public sector by working with the officials responsible for the security of ministries' IT systems. It takes part in expert groups on digital security for businesses, and in meetings with CERTs and with security software publishers who have a clear view of cyber threats. It interacts with corporate lawyers requesting advice. This helps to establish and strengthen links, developing a culture of cooperation and exchange. However, few resources can be dedicated to this despite genuine demand from the private sector.

- Within the DGSI, internal speakers are tasked with organising awareness-raising conferences for companies throughout France on threats related to cyber attacks. The conferences are also an opportunity to exchange cyber security best practice with businesses and help strengthen the national cyber defence policy.

- A Cyber Defence Citizens' Reserve (*Réserve Citoyenne de Cyberdéfense* – RCC) network was established in July 2012, grouping together reservists from the three armed forces and the National Gendarmerie. Its objective is to raise awareness, and to organise and encourage events centred around strengthening cyber defence policy by ensuring continuity between civil society and the area of security and defence. In particular, the RCC includes an 'SME/SMI' group in order to raise awareness of cyber security and cyber defence matters among small and medium-sized enterprises and industries.

- Lastly, the Ministry of the Interior is preparing to sign an agreement which will help promote and spread a culture of economic security among chambers of commerce and industry, businesses, industries and competitive clusters at local level.

4.6 Conclusions

- In terms of institutions, France has multiple entities with cybercrime-related competencies coming under various ministries and bodies; relations between those entities take the form of administrative exchanges, with no real coordination. One of the report's main conclusions emphasises the need to consider the cross-cutting nature of cybercrime, and recommends that a national structure be created to coordinate the action of all those involved – a recommendation which the evaluation team would second.

- After the evaluation visit, the French authorities informed the evaluation team that a prefect responsible for combating cyber threats had been appointed on 4 December 2014. His task is to coordinate and group together initiatives in the ministry responsible for internal security and to represent the ministry in interministerial proceedings.

- The Ministry of Justice and the courts take a piecemeal approach to cybercrime, which makes it difficult to really gauge the phenomenon and effectively fight it. Aware of that situation – which is described in detail in the Robert Group report – the Ministry of Justice has recently set up a horizontal service responsible for cybercrime within the Directorate for Criminal Matters and Pardons (*Direction des Affaires criminelles et des Grâces*). The organisation and working methods of the French courts are not sufficiently adapted to the challenges posed by cybercrime. In particular, the Robert Group recommended that specialised sections of the judiciary be created for the fight against cybercrime committed by organised groups, and that the jurisdiction of Paris be given special national competence over attacks on automated data processing systems targeting state services and key operators.

- France has several specialised investigation services with a great degree of technical competence, each of which works efficiently and creatively. Training them and providing them with human resources, equipment and specific software should be an ongoing endeavour so as to keep up with changes in technology and criminal practices.

- Public-private dialogue is well established; there are many varied and interesting initiatives in terms of partnerships between the two sectors. This is a key aspect of the fight against cybercrime, and should be constantly maintained, strengthened whenever necessary and carefully coordinated.

- The Observatory for Payment Card Security, a French creation which inspired the European 'SecuRe Pay' Forum, is a useful dialogue and monitoring tool; practitioners would like to extend its scope to all electronic payment means.

5 LEGAL ASPECTS

5.1 Substantive criminal law pertaining to cybercrime

5.1.1 Council of Europe Convention on Cybercrime

The Council of Europe Convention on Cybercrime was signed by France on 23 November 2001 and ratified by Law No 2005-493 of 19 May 2005 authorising the approval of both the Convention and the additional Protocol thereto on the criminalisation of acts of a racist and xenophobic nature committed through computer systems.

The French authorities wished to stress that, with specific reference to counter-terrorism, efforts to combat the use of the internet for terrorist purposes form part of the fight against cybercrime, for which the international cooperation instruments are mainly linked to the 2001 Budapest Convention on cybercrime. The most important of those instruments is the international 24/7 network for emergencies, which enables data to be frozen, thus allowing digital evidence to be kept. There is also a similar network that was set up on the initiative of the G-8 in 1997 (the G-8 24/7 High-Tech Crime Network). Most cooperation with foreign hosts (hosts and digital platforms) takes place outside the international legal framework. Today there are still three main obstacles to the establishment of genuinely effective cooperation: the complexity of the arrangements for mutual legal assistance, differences in legislation on data storage , and the fact that cooperation with hosts is on an informal basis.

5.1.2 Description of national legislation

When examining France's detailed response to the GENVAL questionnaire, the evaluation team was readily convinced that **France's legislation, and specifically the country's substantive criminal law on cybercrime, is particularly comprehensive and effective**.

It provides for many criminal offences, which seem to largely cover the scope of currently conceivable criminal situations. France strives to continuously adapt its criminal law to developments in cybercrime. Thus, for several years now, there have been regular updates in this area.

At the time of the visit, at least two bills to supplement the legislative framework in this area had been submitted to the French parliament. One of those bills was adopted on 13 November 2014 as Law No 2014-1353 strengthening the provisions on the fight against terrorism. This law transferred the offences of publicly inciting and defending terrorism from the Law of 29 July 1881 on the freedom of the press to the Criminal Code, creating Article 421-2-5. The law also provides for the punishment to be increased where such offences are committed on the internet, and enables the judge hearing applications for interim measures to order that an online communication service be stopped for committing the acts described in Article 421-2-5 of the Criminal Code if they are a manifestly illegal nuisance. (new Article 706-23 of the Code of Criminal Procedure). The new law also amended Law No 2004-575 of 21 June 2004 on confidence in the digital economy, bringing in administrative arrangements for the blocking and de-listing of sites inciting or defending acts of terrorism, and sites disseminating pornographic images and representations of minors. The administrative authorities now have three courses of action available to them: removal, blocking and de-listing.

Lastly, to adapt to the latest data-storage techniques, investigators can now remotely search 'clouds'.

Where general offences (e.g. swindling, breach of trust) have a sufficiently flexible description, they apply as they stand; in other cases, the legislator has deemed it appropriate to introduce an aggravating factor linked to the use of new technologies, or to establish specific offences.

Aiding and abetting, attempt (if specified by law) and repeat offending[11] are still punishable. Similarly, liability of legal entities has become a general principle of French law, meaning that no specific provisions are required.

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

French national criminal law is very well designed to deal with cyber attacks.

Any fraudulent access to or maintenance of a data processing system, any deliberate attack on the integrity or functioning of such a system or on the integrity of the data that it contains is punishable. The law provides for aggravating circumstances or specific offences that carry heavier penalties in cases in which the consequences of an attack are extremely serious or depending on the target aimed at (government systems) or when the offence is committed by an organised gang.

It is also an offence to import, possess or make available to others, without due cause, and whether free of charge or not, a computer program specially adapted for the purpose of committing the above offences.

Lastly, the illegal interception of computerised data incurs a number of penalties, as do violations of the confidentiality of electronic correspondence.

The maximum penalties incurred range from one to ten years' imprisonment, depending on the gravity of the offence committed, in addition to substantial fines and secondary penalties.

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

France has transposed both Framework Decision 2004/68/JHA and its replacement, Directive 2011/93/EU, without encountering any particular problems with their implementation.

11 No provision is made for repeat offending in respect of the four most petty categories of offence.

Additionally, there appears to be a particular focus on the criminal-law protection of minors from all forms of paedophilia and procuring. French criminal law in this area forms a tight framework that takes proper account of the range of criminal practices linked to general use of telecommunication networks and the internet by minors.

The mere fact of an adult using an electronic means of communication to sexually proposition a minor aged 15 or a person purporting to be of that age is punishable by two years' imprisonment and a fine of EUR 30 000. The penalties incurred increase where the proposition has been followed by a meeting (5 years/EUR 75 000), where sexual abuse has taken place and contact between the minor and the perpetrator was due to the use of an electronic communications network to disseminate messages to a non-specific audience (10 years/EUR 150 000), or where an electronic communications network has been used to distribute pornographic images or representations of a minor to a non-specific audience (7 years/EUR 100 000). They can go up to 10 years' imprisonment and a fine of EUR 500 000 where the offences have been committed by an organised gang.

The criminal law in this area protects not only children as persons but also any form in which they may be represented. The only legislative loophole applies to written material; the investigators encountered during the on-site visit stated that they had sometimes found this regrettable in certain instances where such material was a possible indicator that desires would be acted upon.

C/ Online payment card fraud

Online fraud. In French law 'swindling' is the general offence under which fraud perpetrated by the collection of personal data such as bank card numbers using 'phishing' techniques can be prosecuted. Both the fraudulent use of a bank card number by another person to make purchases on the internet and fraudulent access to a bank account via the internet also constitute swindling. Swindling is punishable by five years' imprisonment, possibly rising to 10 years if the offence is committed by an organised group.

Offences involving bank cards. The falsification of means of payment, including bank cards, carries a heavy penalty (maximum ten years' imprisonment and a fine of EUR 1 000 000 if committed by an organised group). Persons who knowingly accept a fraudulent payment and persons who manufacture, possess or make available the means to commit the offence are liable to the same penalties.

D/ Other cybercrime phenomena

Special criminal law in France provides for a host of other offences in the areas of cybercrime, identity theft, malicious messages, intellectual property violations (counterfeiting), terrorism, including inciting or defending terrorism, use of the internet to make threatening, slanderous or defamatory statements, to incite to commit or defend the commission of a crime, racism or xenophobia, illegal interception of messages, breaches of the secrecy of correspondence etc.

In addition, France's legal framework has been expanded by the Law of 13 November 2014 which, in particular, empowers the administrative authority to request that websites inciting or defending terrorism be blocked and 'de-listed' from search engines or directories. The law was implemented by way of a decree of 5 February 2015, which notably gives the French Data Protection Authority (the *Commission nationale Informatiques et libertés*) monitoring powers.

5.2 Procedural issues

5.2.1 Investigative techniques

All the investigative techniques mentioned in the GENVAL questionnaire are authorised under French law: search and seizure of information systems or computerised data, real-time interception and gathering of traffic and content data, preservation of computerised data, order for all stored data, order for user information.

Two other techniques used in France deserve to be mentioned.

- Undercover investigation. This involves interacting with suspects via electronic exchanges in order to gather evidence of an offence but without inciting the commission of an offence. At present this special investigative technique is used mainly by French law enforcement agencies to protect minors from any sexual exploitation, but it can also be applied to combat human trafficking and procuring, gambling, organised crime, terrorism, and trafficking in health products. The Robert Group recommends that it be extended as widely as possible .

Good practice suggested by France. Services specialising in child protection have developed an investigative technique which involves using a two-person undercover team, enabling investigators to work with greater operational efficiency while also being better equipped in psychological terms.

- Computerised data capture (legal 'Trojan'). This involves using a special tool to access data as displayed on screen, as entered on the keyboard, or as received or transmitted by peripheral audiovisual devices. The technique can be used only in the context of combating organised crime and the hardware and software systems it uses must be approved by ANSSI. Consent to its use is subject to strict criteria. An analysis note delivered by the French authorities and endorsed by the practitioners encountered on-site underlines that although they have never been tested in practice, the arrangements governing prior authorisation for remote data capture are vague and complicated, leading to the impression that receiving ANSSI approval will be a slow administrative process; this could considerably reduce the measure's appeal. Introduced in 2011, data capture is yet to be used.

5.2.2 Forensic examination and encryption

- Electronic or remote forensic examination

The French Code of Criminal Procedure provides for the possibility of examining data on the suspect's computer and the information to which he or she has access, provided that it has not been ascertained beforehand that such information is outside French jurisdiction.

Moreover, implementation of the provisions of Article 32 of the Budapest Convention, which allows a Party to access, without the authorisation of another Party, computerised data stored in another State if it obtains the voluntary and lawful consent of the person legally authorised to divulge it, implies that evidence has been obtained that the data is stored on the territory of that State.

- Encryption

A number of problems relating to encryption have been encountered:

- encryption of data by hackers when exfiltrating information from a network that has been attacked;
- data encryption by ransomware hackers (for example, CryptoLocker attacks);
- encryption by the suspect of his or her data media;
- encryption of web streams by online service providers (banking services, encrypted messaging systems, etc.) when data are intercepted.

Two main difficulties are encountered by the OCLCTIC in its own investigations or in cases where it steps in to assist another service's investigation. The first concerns the discovery of encrypted digital media potentially containing evidence. The second relates to the use by the suspect of instant messaging or VOIP via an encrypted protocol (Skype, Viber, etc.) when internet or mobile data are judicially intercepted.

As regards encrypted physical media, a first attempt at decryption is made by the investigators, often with the cooperation of the owner of the medium. If the owner does not cooperate, a decryption attempt is made by an expert or a specialised body such as the SDPTS (technical department of the criminal police) or the IRCGN (the National Gendarmerie's Institute for Criminal Investigations) in order to decipher the sealed files.

In more complicated technical situations, especially where the encryption key is too advanced, the encrypted files are sent to the technical body covered by official state secrecy and designated by decree (Article 230-2 of the Code of Criminal Procedure).

Given the growing use of encryption software by criminals, the Robert Group proposed in Recommendation 43 that law enforcement officials should be able themselves to request the services of an expert or body and that magistrates should be able to refer matters directly to the technical body covered by official state secrecy. That recommendation was put into practice by the Law of 13 November 2014.

As regards the encryption of instant messaging and VOIP intercepted during investigations, the only solution at present is to use international letters rogatory to approach the country within whose jurisdiction the messaging publisher is based in an attempt to clarify matters.

The French authorities would emphasise that the international judicial cooperation procedure for dealing with requests for the decryption of internet messaging is slow and the results uncertain.

French law provides for the possibility of decryption with the cooperation of a private company. In accordance with Article 230-1 of the Code of Criminal Procedure, any natural or legal person may be required to carry out the technical operations necessary to obtain a readable version of this information or the secret key for decoding it in cases where a method of encryption has been used.

An author who refuses to communicate the secret decoding key for obtaining a readable version of the encoded data is liable to the penalties laid down in Article 434-15-2 of the Criminal Code (three years' imprisonment and a fine of EUR 45 000).

5.2.3 E-evidence

French legislation covers all the concepts mentioned in point 2.B.3 of the GENVAL questionnaire except for 'networks managed or controlled by suspects of cybercrime'. This concept will be defined as part of the ongoing transposition of the Directive of 14 August 2013.

In all cases the evidence has to be gathered fairly, i.e. without subterfuge or incitement to commit an offence, and in a manner proportionate to the gravity of the offence.

The procedures for the gathering, retention and transfer of evidence are laid down in the Code of Criminal Procedure.

Evidence gathered during searches. The police may access data stored at the location of the search, as well as remote data or data located abroad (in compliance with international agreements). Storage media may be copied or seized. These measures will be authorised by the owner of the premises or a magistrate depending on the circumstances (preliminary investigation, investigation of *flagrante delicto* acts, letter of request from an examining magistrate). Practitioners, however, favour modernisation of the system currently applicable to remote data seizure as it equates to a house search and thus considerably reduces the investigative scope (Article 57-1 of the Code of Criminal Procedure).

Computerised data seized from operators.

- In France the legislation governing traffic data retention compels all operators of electronic communications systems to retain such data (except for the content of communications) for a period of one year. These data may be obtained by the police by simply instructing the operator to provide it. Practitioners regret the fact that annulment of the EU Directive on data retention has reduced the prospects for improving cross-border cooperation involving basic data exchange (e.g. IP addresses).
- During an ongoing investigation an operator may be obliged by order of a judicial authority to retain for one year data pertaining to content consulted by a suspect.

Data obtained during undercover police operations or undercover investigations.

By law specially authorised investigators may also conduct surveillance on suspects by posing as accomplices, accessories or receivers of stolen goods. This authorisation covers offences committed by organised gangs (undercover operations) and those committed online (undercover investigations) and applies only in connection with human trafficking, procuring, child pornography and acts endangering minors in general, organised crime, terrorism, illegal online gambling, and trafficking in health products.

Data obtained from interception of correspondence. This kind of interception is always overseen by a magistrate.

5.3 Protection of human rights/fundamental freedoms

In line with France's tradition of safeguarding human rights, the internet is broadly protected not only by the principles of freedom of expression, information and communication but also by the individual's right to privacy and the confidentiality of personal data and correspondence.

French legislation clearly lays down that fundamental rights and fundamental freedoms may be restricted in the context of cybercrime investigations and prosecutions in order to reconcile respect for these freedoms with the need to safeguard public order, ensuring that the internet is not a lawless area. The restrictions concern:

Freedom of expression and freedom of information. Blocking and filtering are measures used to combat illegal content (the competent authorities can force internet access providers to withhold access to a site that carries illegal content). French law also obliges technical operators to indicate and remove illegal content; these restrictions also cover improper commercial communication on the internet (spam).

The right to privacy and the protection of personal data. France has adopted legislation on traffic data retention for the purpose of investigating, establishing and prosecuting criminal offences. Data are retained by the technical operators for the purpose of being made available to the law enforcement authorities, if the latter so request, in connection with criminal proceedings. These data may never involve the content of correspondence exchanged or information consulted.

The evaluation team would note that, as regards the traffic data retention referred to in Directive 2006/24/EC, which was annulled by the Court of Justice of the EU, the French legislation, adopted prior to the aforesaid Directive, provides better guarantees in terms of data protection and control of requests for access to data.

5.4 Jurisdiction

5.4.1 Principles applied to investigate cybercrime

French territorial jurisdiction with regard to cybercrime makes it possible to investigate, prosecute and punish almost all offences of this nature that are somehow connected with France by means of a territorial link owing to the nationality of the perpetrator or the fact that he or she resides there, or the territorial reach of a constituent element of the offence, or the situation of the victim or the accessory to the offence.

In particular, in order to better combat sex tourism, France has adopted a provision making its law applicable to French citizens and residents who commit such offences abroad, especially where the minor victim has been put in contact with the perpetrator of the crimes via an electronic communication network.

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

Framework Decision 2009/948/JHA on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings has been implemented by France. Subsequently France has never had to refer such conflicts to Eurojust for resolution.

France takes the view that conflicts of jurisdiction are best resolved by instruments for providing mutual assistance in criminal matters, such as transfers of criminal proceedings and the spontaneous communication of information. Eurojust and the European Judicial Network can be requested to assist if the occasion arises.

5.4.3 Jurisdiction for acts of cybercrime committed in the 'cloud'

As stated above, the territorial jurisdiction rules enacted by France are comprehensive. The victim does not always know where his or her data are stored but generally agrees to provide his or her private access to the cloud. As regards suspects, the French law enforcement authorities turn to the cloud host; if there is no reply, a request for mutual assistance is drafted if the country in question is party to the Budapest Convention.

5.4.4 Perception of France with regard to legal framework to combat cybercrime

According to France's reply to the questionnaire and the opinion of the French practitioners encountered during the on-site visit:

- France has a cumbersome legal framework, to the extent that the number of applicable provisions and their fragmented nature could justify some kind of codification, at least in the form of a practical handbook for use by all relevant actors.
- However, this legal framework does not allow the French police to obtain, let alone communicate to authorities abroad, elementary identification data (e.g. IP address, telephone number) outside the framework of requests for international mutual assistance in criminal matters. This regrettable state of affairs causes significant delays with international criminal investigations.

5.5 Conclusions

France has acquired a full range of legal instruments – regularly updated – to criminalise a wide range of behaviour relating to cybercrime wherever it arises; this dense legislation is regularly supplemented and updated; however:

- While the penalties incurred are heavy, it was reported during the on-site visit that the judicial authorities generally make insufficient use of them, which creates an imbalance between the investigative methods used and the results achieved;

- The rules regarding the use of certain investigative methods and the obtaining of digital evidence remain ill-defined in some cases (e.g. the arrangements for investigating and analysing computer systems) or too restrictive in others (e.g. remote capture). This makes them ineffective, to the regret of the practitioners encountered (examining magistrates, prosecutors and police officers).

- French law is ahead of European Union law in terms of the retention of telecommunications data (login information, except for correspondence content). Pending its replacement by a new instrument, the annulment of the EU Directive on this subject has considerably reduced opportunities for information exchange in the framework of cross-border cooperation.

6 OPERATIONAL ASPECTS

6.1 Cyber attacks

6.1.1 Nature of cyber attacks

France replied that the nature of cyber attacks was constantly changing. While the years 2011 to 2013 were marked by attacks that could be described as 'hacktivism', which includes protest defacements and denial-of-service attacks calling for militant action, 2013 saw a big increase in denial-of-service attacks, which had become a popular method in the preceding years. However, a large number of these no longer involved activist demands.

At the same time there was also a big increase in attacks on personal data, which continued into the first half of 2014. These became more evident owing to the declaration obligation in the case of disclosure.

Since 2011 ANSSI has dealt with about a hundred large-scale cyber attacks targeting state information systems or key operators, mainly for espionage purposes.

6.1.2 Mechanism to respond to cyber attacks

Law 2013-1168 of 18 December 2013 enabled ANSSI to require that key operators take the necessary technical measures for responding to a major cyber attack. The crisis organisation is tested regularly under the Piranet crisis-management exercises. This is a government plan currently being updated by the SGDSN (Secretariat-General for National Defence and Security). It is intended to form part of the territorial organisation of the state. The work should be completed by the end of 2015.

As already noted, the OCLCTIC also has a role in coordinating judicial inquiries concerning cybercrime.

Where the identified suspects are living abroad and there is an international dimension to the case, the prosecution services usually open a judicial investigation so that the instruments of mutual legal assistance can be used under letters rogatory.

International mutual assistance is used by prosecution services and investigating magistrates in cybercrime cases. The Budapest Convention is the main legal basis invoked in such requests, in addition to the bilateral or multilateral mutual assistance conventions (United Nations Convention against Transnational Organised Crime).

The data-freezing procedure provided for in the Budapest Protocol is used regularly, both within the EU and vis-à-vis third countries.

The data is usually transmitted after receipt of the request for international mutual legal assistance, i.e. some months after the request for freezing. Ultimately, therefore, the data uncovered during a post-mortem analysis of systems is usually of fairly limited value.

6.2 Actions against child pornography and sexual abuse online

6.2.1 Software databases identifying victims and measures to avoid re-victimisation

In France the CNAIP (National Centre for the Analysis of Child Pornography Images) has a national database of child pornography content, known as CALIOPE. The CNAIP comprises gendarmes who provide support for gendarmerie units and police forces. Its tasks are to:

- administer CALIOPE on the basis of the content (images and videos) discovered during investigations by the gendarmerie or the police, as well as any relevant material relating to such investigations (anthropometric photos, background photography, technical specifications of the equipment for producing the content discovered, references of the cases, identities of the protagonists, content origin, etc.);

- analyse the content in order to identify the victims and perpetrators, mainly using software for matching images and meta-data;
- supply the traceable content used during undercover investigations and the digital fingerprints needed for forensic research; on this second point, the CNAIP is linked to the gendarmerie by methods specific to each region and standard methods at departmental level;
- ensure full complementarity with INTERPOL's International Child Sexual Exploitation image database (ICSE DB).

Where an offence is detected, access to the pornographic image or representation of a minor is disabled and the images concerned are deleted.

In French law, offences relating to child pornography images or videos are formulated in terms of the perpetrator. A person may be prosecuted for having taken, recorded, transmitted, offered, made available, disseminated or viewed a pornographic image or representation of a minor, whatever the image or representation may be, and even if the image or representation has already formed the basis of proceedings against another person.

The images are incorporated in the national and international image databases (in particular the INTERPOL database), and internet users who hold, exchange and disseminate such images are subject to criminal proceedings. In the course of such proceedings, the digital storage media are seized.

The PHAROS platform seeks to eliminate any child pornography content that is reported to it. When it is hosted on French computer servers, the hosts are informed, on the understanding that they will apply Article 6 of the law of 21 June 2004 on confidence in the digital economy, which requires them to delete any manifestly illegal content that is brought to their attention. When it is hosted on foreign servers, a message is sent to the police in the country concerned via the INTERPOL network.

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

Regarding sexual abuse/exploitation online: the linking up of the sexual offender with the victim by electronic means of communication is an aggravating factor in the majority of sexual offences committed against children (in particular corruption of minors, prostitution of minors, rape and sexual assault, sexual abuse, procuring and human trafficking).

Regarding cyber bullying, Law 2011-267 of 14 March 2011 introduced into the Criminal Code an Article 226-4-1 imposing one year's imprisonment and a fine of EUR 15 000 for the offence of 'stealing the identity of another person or making use of one or more items of data of any kind whereby that person can be identified in order to disturb his or her peace of mind or that of others or to damage his or her honour or reputation'. This provision makes it possible to prosecute the theft of a person's identity and also the use of any item of data whereby he or she can be identified (e-mail address, telephone number, pseudonym). It also makes it an offence to disturb another person's peace of mind or damage his or her honour or reputation. This offence will include, for example, the act of participating in an internet forum in order to circulate a person's telephone number and encourage other participants to call that number, or using another person's e-mail address and by this means making that person appear to say things that would damage his or her honour.

Law 2014-873 of 4 August 2014 on real equality between women and men created a new offence of psychological harassment, defined as follows: 'Harassing a person by repeated speech or behaviour aimed at causing or having the effect of causing damage to their life conditions as manifested by an alteration in their physical or mental health.'

Sexting is punishable under the general provisions on child pornography images (Article 227-23 of the Criminal Code).

These offences are dealt with by the PHAROS platform on the basis of the alerts it receives from victims, from individuals who are not directly victims, or from online service providers (social networks, etc.).

They are subdivided into three main categories:

- **Offences committed by close friends or relatives who take advantage of their possession of intimate photographs in order to harass their victims.** These offences are sometimes preceded by identity theft and/or the hacking of social network accounts. As the perpetrators are usually friends or relatives of the victims, the offences are dealt with by the territorial police and gendarmerie forces.

- **Blackmail for sexual purposes**, committed by individuals not known to the victims. They generally approach their victims on the internet, win their confidence, and obtain intimate photographs from them which they then threaten to circulate if the victims do not engage in further acts of exhibitionism.

- **Extortion**: the individuals are usually based abroad and use the methods described above to obtain money.

In all cases, PHAROS contacts the victims and helps them to take measures to preserve evidence before directing them to the territorial investigative services. It gives the victims advice so that they can provide the territorial services with all the necessary pieces of evidence. Where the perpetrators are not known to the victims, PHAROS lists the suspects' digital identifiers (e-mail address, profile, etc.) for cross-checking purposes. The digital identifiers that are kept and cross-checked by PHAROS are public data contained in the alerts (e.g. the URL of the Facebook profile of the perpetrator of an offence).

At the Paris Police Headquarters, the Child Protection Unit is involved in the fight against sexual abuse with an internet component. However, its powers do not cover threats and blackmail on the internet or social networks. Its involvement covers three spheres of action:

- investigating offences within its jurisdiction (sexual exploitation and abuse) which are notified to it through complaints and alerts; collecting evidence to enable the judicial authority to bring criminal proceedings;
- instigatory work (undercover investigation and cyber monitoring) on the social networks or image and video exchange websites most frequently used by child pornographers so that they can be identified;
- making technical analyses of child pornography videos discovered during investigations so as to identify voice elements enabling their source to be located, and forwarding them to the relevant services for further investigation and identification of the victims (OCRVP for French videos, INTERPOL for foreign ones).

6.2.3 Preventive actions against sex tourism, child pornographic performance and others

Any advertising relating to the possibilities of committing sexual abuse and sex tourism involving children is forbidden under French legislation.
For many years sex tourism involving minors has been outlawed, and in order to improve the prosecution of all forms of sex tourism French law has been made applicable to all sexual offences against minors committed abroad by French nationals or persons habitually residing in French territory, without any condition of prior accusation or complaint or of double criminality.

Under Article 2-3 of the Code of Criminal Procedure, proceedings brought by any organisation registered for at least five years whose object is to protect or assist children in danger are admissible even if proceedings have not been initiated by the public prosecutor or the injured party.

Under the Criminal Code, child prostitution is punishable by five years' imprisonment, which is raised to seven where the offence is committed regularly or against several children or where the victim was put in contact with the perpetrator as a result of using an electronic communications network.

Best practices

The Central Office for the Prevention of Violence against Persons (OCRVP) is setting up **partnerships with NGOs**, including ECPAT France: preparation of a handbook of reports of sex tourism activities in hotels; transmission to the OCRVP of reports relating to cases of sex tourism; participation in public information and awareness-raising campaigns.

The Ministry of National Education has run a school **campaign to raise awareness of the dangers of cyber bullying**, including the introduction of a free phone number and a dedicated website.

These new offences are the subject of **awareness-raising measures carried out locally by the prosecution services**, with trained investigators. The measures are aimed at the educational managers of schools and the children themselves.

In 2012 the juvenile department of the public prosecutor's office of Saint-Malo took the initiative of proposing a forum on offences relating to digital networks, during which the local public prosecutor spoke alongside IT staff from the gendarmerie and military personnel from the Saint-Malo juvenile delinquency squad and investigation squad . The public prosecutor's office of Cherbourg has been involved in a training scheme in schools on the risks posed by the internet.

The public prosecutor's office of Valence is carrying out projects in schools to discuss with middle and secondary school pupils the risks relating to multimedia (Facebook, happy slapping, invasion of privacy, image rights). The public prosecutor's office of Mulhouse has set up a multi-partner prevention project to improve the processing of criminal proceedings in connection with sexual offences committed against and by children; the juvenile department of the Mulhouse public prosecutor's office found that many cases do not come under the Criminal Code – for lack of a genuinely clear absence of consent by the complainants – but reflect an alarming sociological reality: adolescents becoming sexually active at an increasingly early age, sometimes with violent sexual practices linked to the utilisation of the new means of telecommunication and the widespread use of the internet, which increase the risk factors of actual sexual assault. The project seeks to make adolescents more aware of the risk situations. The idea is that they should understand the ways in which social networks and the new means of telecommunication increase the number of risk situations, and also the ways in which they can avoid such situations without giving up on the use of the technology. Under this project adolescents are encouraged to create their own awareness campaigns among their peers.

The **national helpline for children at risk** (*Service National d'Accueil Téléphonique de l'Enfance en Danger* – SNATED), usually known as '119-Allô enfance en danger', has two aims:
- prevention and protection: receiving calls from children at risk or potentially at risk and from anyone facing this type of situation, in order to help trace them and protect the child at risk;
- communication: forwarding any reports flagging up concerns about such children to the relevant departmental services, i.e. the incident reporting units (*cellules de recueil des informations préoccupantes* – CRIP).

The **national telephone helpline for victims**, 08 VICTIMES (08 842 846 27), has the following tasks:

- Listening, to ensure a better understanding of the victim's request
- Providing information so that the victim knows where to go (who to complain to, how to seek compensation)
- Referral to the nearest victim support organisations or services registered with the Ministry of Justice. In the most serious cases such referral may involve, for the victims who so wish, communicating their details to the geographically appropriate association, which will then get in touch with the victim.

In France there are **a large number of information websites for children and parents.** They include the PHAROS platform's official portal 'www.internet-signalement.gouv.fr', which has headings entitled 'advice to young people', 'advice to parents', 'careful internet use' and 'protecting your computer', as well as links to other government websites, including the CNIL).

The National Gendarmerie has created the ***'Permis Internet'*** **(internet licence) scheme for primary school pupils**. This provides teachers with a ready-made programme warning about the dangers of the internet and presenting best practice for its use, with the participation of security forces personnel. The necessary teaching materials were produced by a public-private partnership. Since December 2013, 600 'Permis Internet' projects have been carried out in 550 schools, including 70 abroad. As a result, more than 15 000 pupils have been made aware of the dangers of the internet. The national police force is also going to be involved in carrying out this operation.

Information is provided to young people in schools by specialised organisations approved by the Ministry of National Education, such as 'e-Enfance', 'Internet sans crainte' and 'Droit @ L'Enfance'. They have access to appropriate teaching materials.

6.2.4 Actors and measures counterfeiting websites containing or disseminating child pornography

Under French law there is no general obligation on internet providers and website hosts to monitor 'the information which they transmit or store', nor any 'general obligation to seek facts or circumstances indicating illegal activity'. They may be requested by the national judicial authority to carry out targeted, temporary surveillance activities. Internet providers and website hosts must also comply with court decisions aimed at ending or preventing damage, and the law provides for the disabling of certain websites. Blocking or disabling may be ordered by the judicial authority, and may also be the result of an administrative police measure.

The law of 21 June 2004 on confidence in the digital economy was the first to provide for a mechanism aimed at combating illegal content. The injured party was given the right to demand that the website host established in France remove manifestly illegal content and to appeal to the judicial authority to ensure that this was done.

The law requires internet providers and website hosts to 'set up an easily visible and accessible system enabling anyone to bring content of this type to their attention'.

In the campaign against child pornography content, and given that the great majority of such images are disseminated by websites hosted abroad, French law introduced in 2011 a system to protect internet users against pornographic images of children by filtering websites containing child pornography images.

It is no longer hosting services but access providers who are required, on pain of criminal penalties, to block illicit child pornography content if its internet address has been identified by the Ministry of the Interior. The system is based on a list of addresses updated in real time. Located on the servers of internet access providers (IAPs), the list is designed to prevent internet users from accessing listed sites, or at least hinder access to those sites, by replacing them with an official information page.

The French Constitutional Council considers that this kind of administrative blocking procedure is constitutional given its proportionality and purpose. The law has now been put into effect by implementing decree No 2015-125 of 5 February 2015, making the OCLCTIC responsible for drawing up and distributing the lists of addresses to which access must be denied, under the supervision of a qualified person on its staff appointed by the CNIL (French Data Protection Authority).

The law also requires Internet access providers to make parental control software available to their subscribers so they can restrict access to or select certain services.

When a server is hosted abroad, a variety of police cooperation mechanisms are used, including those of the EU. These mechanisms might include a request to preserve the data on the server as part of investigations conducted by a French service, pending the submission of an international letter rogatory. The 24/7 network is the preferred option in such cases because of its quick response time. The Council of Europe's 24/7 network and the network established by the G8 are used interchangeably. The INTERPOL NCBs are used in other cases.

When the server is hosted in a Member State of the EU, requests for cooperation are sent using the secure information exchange system, SIENA. These messages are used to inform the States that there are servers hosting illicit content in their country (this type of message follows up on alerts issued via the OCLCTIC's PHAROS platform or the work of any specialised investigation service). Messages can also be sent for operational purposes (e.g. requests for information). The NCBs are used if the host country is not a member of the EU.

The Central Office for the Prevention of Violence against Persons (OCRVP) is the INTERPOL National Central Bureau and the national gateway for child pornography matters. It also has a national remit. It consists of 10 highly skilled investigators who are assigned to the central group for juvenile victims and deal with cases involving child pornography and child sex tourism. In particular, the unit comprises cybercrime investigators responsible for handling digital media.

The regional and local police units deal with offences relating to child pornography, but seldom on their own initiative. Cases opened by the OCRVP are referred to these services via the judges of the courts with territorial jurisdiction. Locally, cybercrime investigators provide the benefit of their expertise on these types of offences.

The Department dealing with illegal activity on the internet is a unit of the gendarmerie that includes a section for child abuse and violence against persons (*section des atteintes aux mineurs et violences aux personnes* – SAMVP) responsible for monitoring networks, leading and coordinating the gendarmerie in undercover investigations, training for such investigations, running specific investigations and coordinating large-scale operations and providing assistance for the regional units.

At the request of a range of stakeholders (organisations, national education bodies, medical establishments, etc.), the Paris Child Protection Unit carries out ad hoc awareness-raising and training by speaking at conferences or round tables. It is regularly called on to suggest legislative developments and awareness-raising or training activities within its area of expertise (cf. the inter-ministerial working group on tackling cybercrime).

Both human and technical capacity-building are a major concern for its continued effectiveness in addressing cybercrime-related challenges and developments. In terms of staff, a proactive recruitment policy will see the group grow from six to nine investigators by the end of 2014. The technical means available to it are very satisfactory following the budgetary efforts that have been made. Those efforts have also enabled the group to be at the forefront of developments later shared at national level (establishment of an EWS computer room, adoption of the LACE software, etc.). They must be maintained over the long term, in particular to respond to the extremely rapid changes in new technologies. Lastly, in order to maintain a sufficient level of knowledge to cope with such changes, the group has sometimes participated in private training courses.

6.3 Online card fraud

Victims do not always lodge a complaint in cases of online card fraud, but they have the option of reporting the facts using a dedicated facility.

While making a report or a complaint helps to make the investigation services aware of particular types of fraud, the majority of victims no longer file a complaint given the compensation arrangements in force pursuant to the monetary and financial code: in the event of an unauthorised transaction reported by the user under the conditions laid down by law, the payer's payment service provider must immediately reimburse the payer for the amount of the unauthorised transaction and, where appropriate, restore the debited account to its previous state.

The obligation to reimburse applies even when the card-holder is still in possession of the bank card and includes the cost of the bank fees.

These provisions apply regardless of whether or not a complaint has been made.

Facilitation of online reporting. When an individual discovers a site that leads them to suspect an offence has been committed on the internet, they can report it on the PHAROS platform website at the following address: https://www.internet-signalement.gouv.fr/.

Reports are dealt with by the OCLCTIC and may serve as the starting point for a criminal investigation.

In 2013, PHAROS received 123 987 reports (compared with 119 788 in 2012 and 101 171 in 2011), which is an average of 2 384 reports per week. The vast majority of these reports fall into three categories:

- fraud and extortion: 56 % (stable)
- child abuse (child pornography, predatory sexual behaviour, etc.): 12 % (stable)
- xenophobia and discrimination: 10 % (compared with 8 % in 2012)

Of the 123 987 reports made to PHAROS, 7 698 (around 6 %) were sent to a competent authority, including 1 488 which were submitted for investigation to the French investigation services.

For the time being, France does not have an appropriate tool for dealing with mass disputes of this kind. It was one of the recommendations of the inter-ministerial working group on cybercrime. A project is under way to create an online complaints system that will make it possible to gather all the relevant data, enabling connections to be made between cases.

6.4 Conclusions

- The efforts made to prevent and reduce the risks associated with cyber attacks seem to be orientated more towards protecting the reputation and resistance of the relevant infrastructures than protecting possible future victims against cybercrime.

- In general, the fact that there is no clear synergy between the different police bodies involved in the various operational aspects could lead to disparity among the public strategies and a waste of resources. Two initiatives – undercover investigations and the PHAROS platform – show that a common or collaborative approach provides an effective response to the challenges.

- Undercover investigations, especially those carried out by the police specialising in the protection of minors against sex offences, are a highly rated and particularly effective work tool. French practice in this area should therefore be of great interest to other Member States.

- Another very encouraging experience is PHAROS, the platform for reporting illicit online content, which is worth highlighting for its originality and success. PHAROS, which is made up of specially trained police officers and gendarmes, enables reports made by internet users, organisations and operators to be analysed, and ensures they are followed up with enforcement measures where appropriate.

7 INTERNATIONAL COOPERATION

7.1 Cooperation with EU agencies

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

There are no formal requirements or specific procedures for cooperation on cybercrime between the national authorities and Europol/EC3, Eurojust and ENISA.

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

France is a member of Focal Point CYBORG. Cooperation with OCLCTIC services and gendarmerie services is effective. In that regard, Operation Mousetrap (which is the subject of an OAP under the 'Cybercrime' EMPACT project) and Operation Price (in the field of social engineering) are worthy of note.

The French authorities were very satisfied with the cooperation between the above agencies, and especially with Europol/EC3. They replied to the GENVAL questionnaire as follows.

Europol/EC3.

The creation of EC3 fulfils a real need for a European service which specialises in the fight against cybercrime and can:

- carry out an analysis of the phenomenon as a whole, assisted in particular by the specialised Focal Points work files, such as TERMINAL for bank cards,
- coordinate the activities of all those involved.

Even though it was set up too recently to carry out a real assessment, it is clear that EC3's analytical capabilities are proving very useful to investigations being carried out in several countries at once.

In terms of the fight against child pornography, the support provided by Europol's FP TWINS includes data analysis, the compilation of objective records, and operational coordination.

Eurojust. The French authorities welcomed the outcome of a case involving the Rennes and Paris JIRS. The case followed up on operational intelligence from the FBI which reported that an investigation had been carried out by the US to identify and question the US designers and users of a piece of malware (the malicious software '**Blackshades**'), which allowed attackers to control other computers remotely and in particular to gain access to all the data on an infected computer.

Led by Eurojust and with the participation of Europol, a coordinated action was carried out by the United States and the nine European countries affected (Belgium, Germany, Estonia, France, Netherlands, Austria, Romania, Finland and the United Kingdom). The OCLCTIC was entrusted with a preliminary investigation to identify those committing offences on French territory. For that purpose, the FBI was able to formally provide the OCLCTIC with a list of the IP addresses of the software's French buyers, combined with identifying information (name, post code, email address, telephone number). Europol also helped coordinate this action, which led to the questioning of 70 people in France, 20 of them by the BEFTI – which shared responsibility, within its geographical area of remit, with the OClCTIC – and the detection of around 20 cases of interest.

Cooperation between France and several Member States has also taken place within Europol and Eurojust on a number of proceedings relating to fraud using fake international payment orders or to so-called 'content' offences committed via websites hosted in France, in particular for the purposes of jointly and simultaneously executing international letters rogatory.

According to the evaluation team, Eurojust might also support the creation of a European network of judges specialising in cybercrime. Such a network would encourage the exchange of best practice, facilitate cross-border cooperation, and allow for the circulation of up-to-date information on the status of cybercrime in the EU and on the development of information technologies and the threats they pose.

ENISA. ANSSI represents France on the ENISA management board and cooperates with ENISA in the course of its work on the security of information systems.

France notes that ENISA's primary mission is not to combat cybercrime but to improve the overall security of information systems (SIS) in Europe. However, SIS plays an important role in the prevention of cybercrime. ENISA therefore organises an annual conference bringing together the SIS and law enforcement communities, and recently signed a cooperation agreement with Europol (EC3). France is satisfied with this cooperation, which should allow the two agencies to share information on their respective areas of expertise, while also ensuring that their activities do not overlap.

As to whether they had **any recommendations for making better use of the above EU agencies**, **the French authorities responded as follows**.

- It is essential to avoid any overlap between the activities of Europol and those of ENISA. While EC3 is intended to combat cybercrime, ENISA is concerned with strengthening the technical security of information systems. As an example, protecting critical infrastructure from cyber threats – dealt with at national level by the cybersecurity agencies – falls wholly within ENISA's remit and not Europol's.

- European training (organised on a regional basis where necessary to take account of language barriers) on the use of Europol/EC3 could be given to specialised and experienced investigators from each Member State so that they fully understand the European cooperation mechanisms and can be put at the service of joint investigation teams.

- More effective use could be made of Eurojust if each Member State had a specialised national court whose judges received training in European cooperation.

7.1.3 Operational performance of JITs and cyber patrols

As yet France has no specific experience to share on this subject.

7.2 Cooperation between the French authorities and INTERPOL

Exchanges with INTERPOL are carried out using the dedicated messaging system within INTERPOL's national central bureaux (NCBs).
The OCLCTIC and the gendarmerie also take part in working groups, meetings and conferences organised by INTERPOL. In addition, operational interaction occurs between the international ICSE database and the national CALIOPE database on child pornography content.

7.3 Cooperation with third states

Cooperation policy is based primarily on the existing tools for tackling cybercrime, in particular the Budapest Convention. The OCLCTIC has participated as an expert in various Council of Europe projects (cybercrime@IPA, GLACY, etc.) to help third countries (Balkans, Morocco, Senegal, etc.) set up tools to combat cybercrime, such as 24/7 contact points, appropriate legislation, or cybercrime units.

Since 2008, the OCLCTIC has regularly provided training to West African countries (Senegal, Côte d'Ivoire, Burkina Faso, Benin, Togo) in order to equip them with specialist cybercrime investigators. Thanks to the strong political will of the countries concerned, these actions have made it possible to develop tools for dealing with cybercrime, such as a reporting platform in Côte d'Ivoire which has been set up within a department of IT and digital forensics (*Direction de l'Informatique et des Traces Technologiques*) at the Ministry of the Interior. Senegal, meanwhile, is in the process of ratifying the Budapest Convention.

The national gendarmerie also carries out training abroad, in particular for African countries, and in Senegal has taken part in the Council of Europe GLACY project.
The BEFTI is also involved as an expert, hosting trainees in-house for periods of two weeks to two months (e.g. from Côte d'Ivoire and Algeria) and running training courses abroad with the BFMP or the OCLCTIC (e.g. in Morocco, United Arab Emirates, Madagascar).

The 24/7 contact points are frequently used because they provide an easy channel for exchanging information. Finally, the network of internal security attachés or the liaison officers are of great importance because they offer the possibility of exchanging information simply and directly with the appointed contacts.

7.4 Cooperation with the private sector

Cooperation with the national private sector has already been described above.
The main issue involved in cooperation with foreign companies is the recognition of French law. Certain private-sector partners, particularly the major internet companies, are reluctant to do so for both organisational and cultural reasons. Nevertheless, when these companies receive judicial requests their level of cooperation, while inconsistent, is becoming increasingly satisfactory. They have acknowledged the concept of processing judicial requests directly without requiring international letters rogatory to be issued by the French judicial authorities. However, further progress is expected, in particular the establishment of a French representation with a mandate to cover legal obligations, in order to provide an intermediary (with Facebook and Twitter) and guarantee the confidentiality of the requests sent by investigators. The inapplicability of French law to foreign technical service providers engaged in economic activities on French territory is one of the main problems in international cooperation involving the private sector. This difficulty was highlighted by the interministerial working group on combating cybercrime chaired by the Prosecutor-General Marc Robert.

Law enforcement authorities cooperate regularly with the local branches of private companies which have their main headquarters in a third state, in particular the United States. The replies may be partial or unsatisfactory but the procedure is not affected because the judge alone may decide on the admissibility of evidence. Since coercive means are not used to obtain information from these local branches or the foreign countries concerned, the replies obtained are admissible as evidence.

7.5 Tools of international cooperation

7.5.1 Mutual Legal Assistance

There is no specific legal basis for mutual assistance in criminal matters in respect of cybercrime. Consequently, in the absence of any other convention, the provisions of the Code of Criminal Procedure on mutual legal assistance will apply by default. Depending on the procedural stage at which the request for mutual legal assistance is made, the competent authority to make such a request is the public prosecutor, the examining magistrate or the trial court. As regards the execution of incoming requests for mutual legal assistance, the public prosecutor or the examining magistrate is competent depending on the procedural steps to be carried out under national law.

The transmission channels are laid down by the Conventions or, failing that, by the Code of Criminal Procedure. In the absence of any applicable Convention, the Code of Criminal Procedure provides that, in urgent cases, requests may be transmitted directly between the judicial authorities competent for their execution (Article 694).

When the provisions of the Budapest Convention should be applied, for example, in the absence of a mutual legal assistance treaty, France has stated that, even in urgent cases, requests for mutual assistance from the French judicial authorities addressed to judicial authorities abroad are to be transmitted via the intermediary of the Ministry for Justice, and requests for mutual legal assistance from judicial authorities abroad to the French judicial authorities are to be transmitted via diplomatic channels. The provisions (Article 29) of the Convention relating to the freezing of data via the H24 network may, nevertheless, be applied.

Since a high proportion of mutual legal assistance files are processed through the channel of direct transmission between the competent judicial authorities, the Ministry of Justice (*Bureau de l'entraide pénale internationale* (BEPI) – Office for International Mutual Assistance in Criminal Matters) has no statistics on them, nor does it have accurate information on their actual processing or their outcome.

Those we met emphasised the need to shorten time limits for replying to international requests for mutual legal assistance: they suggested that might be facilitated by creating forms and streamlined procedures for certain types of requests – by distinguishing, for example, between traffic data and content data, in compliance with basic legal principles; they also stressed the need for simplification at European level to get basic information in good time (e.g. identification of an IP address, email address, telephone number or bank account number).

Within the territory of the EU, or part of it, and for categories of offences covered by the European Arrest Warrant, an area could be defined within which (non-exhaustive list):

- exchange of intelligence and observations (including undercover) could be carried out freely;
- requisitions would be enforceable everywhere;
- full access to a remote IT system from an initial system, both located within this area, would be authorised in the course of a search or from service premises (going beyond the framework of Art. 32 of the Budapest Convention).

7.5.2 Mutual recognition instruments

As regards the implementation of mutual recognition instruments, and for the reasons indicated above (direct transmission between competent authorities), the Ministry of Justice has no detailed information to provide.

7.5.3 Surrender/Extradition

European arrest warrant. Since the 'computer-related crime' category (*cybercriminalité* in the French version) referred to in the Framework Decision on the European arrest warrant is not defined in French law, it is for the authority serving the arrest warrant to assess whether the offence in question comes under this category. Some offences come directly under this category (offences on automated data processing systems) and others may also come under another category such as 'fraud'. 15 surrenders have been made between France and another Member State in the framework of this surrender procedure, under the 'computer-related crime' category.

Extradition. It is not the nature of an offence that determines whether it falls within the field of extradition but the penalty incurred, the length of which varies according to the applicable convention. The French authorities are therefore not in a position to provide a list.

In relation to cybercrime – as is the case for other categories of offences – the authorities responsible for sending/receiving surrender/extradition requests and for deciding on such requests are the same as for other offences, and they vary according to the Convention establishing the legal basis for the request. Within the European Union, requests are transmitted directly between competent judicial authorities when the mechanism of the European arrest warrant is implemented.

7.6 Conclusions

- The French police departments cooperate closely with Europol/EC3 and the support they provide has been the subject of very positive feedback from the investigating authorities encountered on site. In general, France is very involved in the functioning of the European arrangement that has been put in place to step up the prevention and combating of cybercrime; the priorities set at European level are reflected in the action taken by the French police authorities.

- According to the information gathered during the on-site visit, there seems to be less familiarity with or use of the possibilities offered by Eurojust to facilitate judicial coordination and cooperation with third countries in the field of cybercrime.

- The Budapest Convention is considered by French practitioners as the reference instrument in the field of international cooperation on cybercrime, notably thanks to the possibility to request, in emergencies, through national contact points, the immediate preservation of digital data for a minimum period of 60 days pending a request for mutual legal assistance. However, the duration varies from country to country.

- The slow pace of legal proceedings in international mutual assistance is one factor that prevents the rapid interception of computer servers involved in cyber attacks. This situation could be significantly improved, at least at European level, by streamlining procedures or the right to requisition, in particular as regards crucial information to be found in traffic data (e.g. IP address).

- Cooperation between the French authorities and INTERPOL (ISCE) is good; the G8 and G20 channels are well used.

8 TRAINING, AWARENESS RAISING AND PREVENTION

8.1 Specific training

Trainees at police, gendarmerie and judicial academies obviously receive basic training (a few hours) on cybercrime. Those courses can be supplemented, over the years, by conferences or scientific and technical police workshops.

1. Training of the judiciary

Every year the French National School for the Judiciary (*Ecole Nationale de la Magistrature*) proposes two types of ongoing training for judges:

(a) A five-day training session on cybercrime, the objective of which is to create awareness about the issues related to this phenomenon and its international dimension, recent legislative developments, specific aspects of digital investigations and judicial handling of this crime. This training course is multidisciplinary in terms of target audience and participants (90 French and foreign judges, police, gendarmerie and customs officers etc.).

(b) A university diploma in cybercrime, in partnership with the University of Montpellier, allowing for a better understanding of the different crimes and responsibilities linked to the security of information systems in general and the fraudulent use of digital networks in particular. This training, open to around fifteen participants, is broken down into several modules and spread over a period of six months; it ends with exams confirming that the participants have acquired the skills and knowledge taught on the course. Only a few judges, who register on a voluntary basis, follow or have followed this course.

Moreover, once a year, the OCLCTIC organises a training course for French judges entitled 'approach to cybercrime'. Participants spend a week familiarising themselves with specific legal aspects related to cybercrime, the means used to fight it and the special investigation techniques.

However, although the French National School for the Judiciary has introduced some modules on cybercrime in its training offer for magistrates, this training is neither systematic nor compulsory, not even for the 'specialists'. Practitioners likely to deal with cybercrime files still do not have sufficiently developed knowledge in a highly technical field where lawyers are very often specialised.

2. Training of police and gendarmerie officers

- Within the national police force, the creation of the Sub-directorate for the Fight against Cybercrime (SDLC) has been accompanied by the recent establishment of a dedicated training department. The department is responsible for organising the courses for cybercrime investigators described below, a course entitled 'Approaches to cybercrime' aimed at judges, and various other training programmes for first responders (of which 800 have been planned over five years).

The **'first responder' training course** is aimed at police officers who have to carry out basic investigative procedures in a digital environment. They need to be able to gather evidence in such a way as to ensure its legal validity, and perform initial scans of digital devices. They also receive training on the specific aspects of recording complaints related to cybercrime and on initial investigative procedures (i.e. searches and requisitions). The course is scheduled to run over two weeks, with the first consisting of distance learning sessions and the second, which covers the practical aspects, done as face-to-face training.

The **training course for cybercrime investigators** (CCIs) is run by the Central Office for Combating Information and Communication Technology Crime (OCLCTIC). The course lasts eight weeks. Two sessions are organised per year with 18 places each, which means that 36 CCIs can receive training each year. There are already 377 active CCIs. At the end of the training course, CCIs are able to analyse and categorise criminal offences that are specific to or related to cybercrime, to copy and analyse digital media without compromising the integrity of the evidence, to provide technical reporting and to conduct investigations in the field of information and communication technology. The CCI training course culminates in a theoretical and practical examination and is recognised as equivalent to a bachelor's or master's degree. In order to be certified, trainees must have three years of experience and must submit a technical file for evaluation by a panel of professionals.

The OCLCTIC participates in the meetings of the European Cybercrime Training and Education Group (ECTEG) and takes an active role in the creation of training content.

In addition to the CCI course, an annual training course on bank card fraud is organised for criminal police investigators. It is open to 15 participants and runs over four days. Its estimated cost is EUR 2 500.

- **Within the Paris Police Headquarters**, in addition to the CCI training course, BEFTI participates in some private-sector training and offers two approved training courses listed in the professional training catalogue (FD06 and FD15), which are also open to the judiciary and customs officers. The first consists of a week-long immersion course at the department and is designed to gauge the participants' interest and create a pool. The second, one-day course is related to digital police investigations, covering the recording of complaints, initial investigations and the technical environment, and in-depth digital investigations, to allow participants to work independently on straightforward investigations. Furthermore, all those with experience in this area share their knowledge in order to raise the level of technical expertise at minimal cost. Within the BEFTI, practitioners adapt and deliver training to reflect developments in investigations and technology without delay. Colleagues with new expertise can thus pass it on by providing ongoing training at BEFTI within the CCI community, and soon for all CCIs at Paris Police Headquarters, as provided for in the programme for adapting Paris Police Headquarters to combat cybercrime.

- Within the National Gendarmerie, building on the harmonisation activities carried out at EU level by the European Cybercrime Training and Education Group (ECTEG) and the work of the inter-ministerial working group on cybercrime, the following strategy has been adopted:

- Level 1: raising awareness among all military staff and the staff of local general and judicial units, in particular by providing an online training course lasting a few hours for first responders dealing with digital technology (P-NTECH level). Content of the course (developed with the national police as part of the EU project 2CENTRE): definition and aspects of cybercrime; measures used and parties involved in combating cybercrime; legal instruments; recording complaints; identifying and requisitioning technical service providers; open source research; participating in searches in a digital environment; self-assessment exercises.
- Level 2: regional face-to-face training courses organised over several days to train digital technology correspondents in local general and judicial units (C-NTECH level). Content of the course: mainly practical training to allow P-NTECH level staff to extend their activities by carrying out simple forensic examinations (particularly on mobile phones) and open source investigations.
- Level 3: training digital technology investigators (NTECH level) working exclusively on complex forensic examinations or network investigations in departmental, regional or central judicial units. This training takes the form of a professional diploma taught over 14 months, comprising 10 weeks of face-to-face training split between the gendarmerie's criminal police training centre and the University of Technology of Troyes, work carried out remotely, practical work done under the supervision of a tutor, and a technical thesis. Content of the course: legal aspects and operational framework; technology and architectures; operating systems; internet and networks; researching information; forensic tools; security of information systems; industrial partners; pedagogy; giving evidence before a court in English, etc. The NTECH professional diploma has been approved by the French Ministry of Higher Education and Research.
- Expert level: ad hoc training courses for experts in digital forensics or network investigations from central judicial units.

Budgetary aspects. The budget allocated nationally to the training courses for cybercrime investigators (CCIs) organised by the OCLCTIC is around EUR 100 000 per year (for transport, accommodation, training rooms, meals, etc.) excluding training equipment and the cost of trainers. In addition to this, around EUR 60 000 was invested in e-learning in 2011.

Within the gendarmerie, training costs vary according to the level. Costs are negligible at level 1 (P-NTECH) and fairly low at level 2 (C-NTECH), but significant at level 3 (NTECH), with annual costs for 16 trainees reaching EUR 69 200, comprising EUR 44 800 in teaching expenses and EUR 24 400 in travel expenses. If the cost of individual equipment (totalling EUR 720 000 for one intake) is factored in, level 3 training becomes very expensive.

8.2 Awareness-raising

Many awareness-raising programmes are organised in France, initiated by every competent department and aimed at all audiences. They have been described extensively in this report.

However, it should be noted that some of the awareness-raising programmes for first responders organised by various police departments overlap, and that the material published by Europol/EC3 ('Cyber bits' notes) has not been translated into French. Given that the content of awareness-raising programmes aimed at professionals is continually evolving to keep track of developments in technology, there is little point in duplicating those programmes.

8.3 Prevention

8.3.1 National legislation/policy and other measures

In France, many initiatives to prevent cybercrime are run by local government, professional bodies or other organisations. Often, these initiatives are carried out in partnership.

- The Ministry of the Interior, by its presence at local level, can make a significant contribution towards increasing alertness amongst individuals, economic actors and territorial authorities. Point 3 of its strategic action plan **relates to improving levels of awareness and prevention of cyber threats amongst individuals, economic actors and territorial authorities:**

- fostering a policy of prevention and awareness of cyber security, organising communication and awareness-raising campaigns bringing together internet practitioners and associations that have entered into partnership agreements with the Ministry of the Interior's services (particularly the PHAROS platform);
- contributing to strengthening the inter-ministerial scheme for district 'observatories' to monitor the security of information systems. Those observatories should be able, to the fullest extent possible, to carry out their tasks of raising awareness among and issuing alerts to economic actors and territorial authorities;
- strengthening the cyber security awareness capabilities of the 'economic intelligence networks' and 'security specialists' within the gendarmerie and the national police, raising awareness in secondary schools and universities, and launching an awareness-raising operation aimed at territorial authorities;
- continuing to develop awareness-raising initiatives aimed at economic actors via a partnership agreement concluded with the French Chamber of Commerce and Industry (CCI-France).
- promoting the 'Permis Internet' (internet licence) project mentioned earlier, aimed at primary school pupils.

The pilot project launched by the gendarmerie is to be rolled out in September 2014 and the possibility of extending it to the police is being studied;

- participating in consolidating the regional networks of the Cyber Defence Citizens' Reserve that was deployed over the course of 2013-2014. These reservists, who come from a range of fields and are particularly involved in spreading the cyber defence message, make excellent intermediaries for spreading good practices.

The interministerial working group on combating cybercrime, chaired by Prosecutor-General Marc Robert, has itself identified prevention as a priority and has issued a number of recommendations, aimed both at protecting internet users (human approach) and at ensuring that offences are not committed (technical approach):

- involving the state to a greater extent in terms of leadership, synergy, defining objectives and long-term planning of cybercrime prevention policy, through awareness-raising campaigns aimed at the general public (data protection, vigilance against fraud) or at more specific sections of the public (skills centres), harmonising and rolling out the various preventive media used, creating a public internet emergency number and systematically carrying out risk assessments on the new regulated services;
- making internet users the first line of their own defence, through digital education in schools in partnership with practitioners, by developing information areas that are accessible online or by telephone, setting up an online search engine to make cyber offences easier to detect, and ensuring greater involvement of victim support and consumer organisations;
- mobilising practitioners by ensuring more consistency in awareness-raising initiatives, establishing a list of preventive obligations to be adhered to by public and private establishments operating on the internet (online businesses, access providers, download platforms, digital device traders, etc.), advocating a prevention plan for large companies and encouraging the creation of a CERT to respond to the requirements of small and medium companies;
- mobilising French and European research and industry in order to develop appropriate technical and technological solutions.

Preventive initiatives conducted by the police and the gendarmerie have already been discussed.

More and more local enforcement services are becoming involved in prevention. Many such departments organise awareness-raising meetings, often in cooperation with special investigators, aimed at children and young people as well as at teaching staff in schools.

Thus, in 2014, the public prosecutor's office of Versailles launched an action plan to combat cybercrime as a result of both the increase in the number of offences falling within the category of cybercrime, and the technical nature of the cases in this area. In the first instance, this involves assessing the state of criminality in this area and reviewing the legislative instruments and techniques that are available to the prosecuting authorities. This action plan will involve:

- firstly, organising a **meeting of the public prosecutors and their deputies with the directors of the competent central offices**. A proactive policy will have to be defined in coordination with the special investigation services; the latter can help prosecution authorities to better target objectives, by providing key information for understanding the phenomenon, and practical tips for searching for and gathering digital proof.

- secondly, organising a **training day,** in the framework of the Court of Appeal of Versailles' decentralised continuing training programme, which will provide an up-to-date technical and legal foundation, and **facilitate the exchange of best practices** in order to assist prosecuting authorities in overcoming difficulties (applicable texts, local jurisdiction, problems arising from extraneous elements).

A scheme by the public prosecutor's office of Lons-le-Saunier represents another excellent local initiative: it involves creating prevention courses on sexual offences committed by minors as an alternative to prosecution, in order to make the perpetrators of such offences aware of the need to respect other peoples' bodies, as well as the dangers of social and online networks that present certain inappropriate sexual behaviour as normal.

Finally, the juvenile department of the Paris public prosecutor's office plans to set up a course for the perpetrators of offences linked, inter alia, to the possession of child pornography images. This course, ordered as an alternative to prosecution, would essentially be based on partnership with an association, under a protocol. It would involve very rigorous medical and psychological follow-up, carried out over an extended period of time. The aim is to oblige the offender to truly reflect on the offences committed, and to combine this with a longer, obligatory follow-up period.

8.3.2 Public/private partnership (PPP)

There are many examples of public-private partnerships to prevent and combat cybercrime, some of which were mentioned earlier in point 4.3.

The following are some of the initial measures which the French Anti-Cybercrime Expert Centre (CECyF) has proposed or plans to propose to its members:

- an assessment of training requirements and an inventory of available training, together with a process for awarding a seal of approval to these existing training courses;
- helping to create tools to raise awareness, e.g.: drawing up, together with its Signal Spam and Paypal member, a brochure to raise awareness of classified advertisement scams;

launching, together with Signal Spam, an information site (prevention, detection and removal) on botnets, as part of the European ACDC project: www.antibot.fr;

- the development of distance training courses, for investigating authorities as well as for companies and territorial authorities;
- an analysis of research and development needs, together with a process for awarding a seal of approval to R&D projects;
- the development of open source digital forensics tools;
- taking part in conferences to promote exchanges between the communities involved on the different aspects of preventing and combating cybercrime;
- organisation of a French-language conference on incident response and digital investigation (CoRI&IN, Lille, January 2015) and official support for other events;
- contributions to specialist journals;
- an open-access academic publication on technical, legal and criminological subjects: 'Le Journal de la Cybercriminalité et des Investigations Numériques' ('The Journal of Cybercrime and Digital Investigation') (CybIN; journal.cecyf.fr);
- workshops for identifying and developing new projects.

8.4 Conclusions

- There is an abundance of training on offer for investigation services, which is undeniably a very positive point. Nonetheless, due to the extensive compartmentalisation of the different investigation services, the offer is also highly diverse, to the extent that there is a risk of duplication and disparities in investigative methods that could hamper the overall efficiency of prosecutions. Although the police and gendarmerie must be able to retain the multi-level training model suited to their respective organisations, harmonisation of content and methods can nonetheless be aimed at by using shared reference frameworks to develop this training provision.

- The specialisation of certain judges in the area of cybercrime is due to their practical experience and does not result from any policy or strategy. 'cybercrime specialist' judges are appointed without the need for any certified training, as this is not obligatory.

- The French authorities have a wealth of good initiatives in the area of raising public awareness and prevention of cybercrime (see, amongst others, the example of the CECyF, above).
- A dialogue between private-sector operators and the authorities should be developed, inter alia in order to improve the mechanisms for identifying illicit content (child pornography, incitement to terrorism), and the arrangements for removing it whenever necessary.

9 FINAL REMARKS AND RECOMMENDATIONS

9.1. Suggestions by France

The prevention and combating of cybercrime could be improved by defining an overall inter-ministerial strategy in this area in order to render the action taken by different actors more consistent, and strengthening training and prevention initiatives.

As far as prevention and response to cyber attacks are concerned, if the Member States were to implement similar measures to those included in the law adopted in France in 2013, it would be possible to tackle the recurring issue of information systems deployed in a number of countries. This is the idea behind the draft 'Network and Information Security' Directive proposed by the Commission on 7 February 2013 and approved by the European Parliament in March 2014.

The terrorist attacks in Europe at the beginning of 2015 were a reminder of the importance of the digital space in the fight against terrorism. Given the similarities in the issues identified as regards the prevention and punishment, in the digital space, of terrorist offences and offences linked to ordinary crime, we propose that, on this aspect, two specific recommendations be made, highlighting the need for dialogue with the main Internet operators and for guarantees to ensure that encryption capacities do not constitute an insurmountable technical obstacle for the services responsible the prevention, detection and prosecution of criminal offences, and in particular for combating the most serious offences, including terrorism.

9.2 Recommendations

As regards the practical implementation and operation of the Framework Decision and the Directives, the expert team involved in the evaluation of France was able to satisfactorily review the system in France.

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

The evaluation team saw fit to make a number of suggestions for the attention of the French authorities. Furthermore, based on the various good practices, related recommendations to the EU, its institutions and agencies, Europol in particular, are also put forward.

9.2.1 Recommendations to France

France should:

1. Examine and describe the action taken in response to the report by the interministerial working group on cybercrime chaired by Prosecutor-General Marc Robert (cf. in particular 3.2, 3.3, 3.5, 4.6, 5.2 and 8.3);

2. Enhance coordination of the actions of all involved, by entrusting coordination, if necessary, to a national body tasked with implementing all aspects of the strategy, in collaboration with the cyber defence and cyber security authorities (see, for example, the points made in this regard by the Robert report) (cf. 3.2.2, 4.5 and 4.6);

3. Develop a national qualitative and quantitative tool for measuring the cybercrime phenomenon, using a standardised classification system and vocabulary, in order to gauge its actual scale and reduce the 'dark figure' proportionately (cf. 3.3.2, 3.5);

4. Promote the implementation by the competent authorities of strategic judicial guidelines on cybercrime to improve the monitoring of litigation in this area and of prosecution, and to bring crime policy up to date, including the definition of priorities, taking into account the existence of specialised courts and developing training tools for judges (cf. 3.2.2, 3.5, 4.1, 7.1, 8.3, 8.4);

5. Strengthen national capacities to protect IT systems, for the benefit of small and medium-sized companies as well as individuals (cf. 3.2.1, 3.5);

6. Analyse the conditions in which public entities carrying out activities in the online sector alert the law enforcement authorities to acts brought to their attention which appear to constitute a criminal offence; a comprehensive policy to combat cyber threats can be defined only if the law enforcement authorities are made aware of as many of the offences being committed as possible, it being incumbent upon them to define an appropriate criminal response (including case closure) (cf. 3.1, 3.3.2, 3.5);

7. Make it compulsory for economic operators to report fraud committed using electronic payment methods, with the help of a system that would allow the vital data specific to this large-scale litigation to be collected and that would be able to reduce the rate of undetected cybercrime (cf. 3.3.2, 3.5);

8. Resolve the real difficulties practitioners must overcome in searching for and gathering proof of cybercrime offences when faced with the vast number of – and the ambiguities contained in – the procedural texts currently applicable; consider creating a consistent, complete set of procedural rules specifically for gathering digital proof that would be adapted to the needs of criminal investigations by combining efficiency with respect for fundamental rights (cf. 4.1.2, 5.2.3, 5.5);

9. Continue efforts to provide the specialised and general investigation services with human resources, equipment and training, without which the excellent results achieved by these services could not be maintained and with they will be able to enhance their skills and the quality of response to victims (cf. 3.2.2, 4.2, 4.6, 6.2);

10. Consider creating a common training base for cybercrime investigators from the different criminal police services, thereby ensuring that job profiles are standardised and a cross-service network of experts is created to promote efficiency of investigations and the growth of national expertise (cf. 8.1, 8.4);

11. Standardise the documentation on combating cybercrime that is made available to the different investigatory bodies by developing a common approach and, in particular, by making use of the resources created and distributed by Europol (see also Recommendations 15 and 23) (cf. 8.2, 8.4);

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

The European Union should:

12. With Eurojust and Europol, and while respecting fundamental rights, consider solutions to overcome obstacles to and delays in the exchange of digital information, including basic information, between the law enforcement authorities of the Member States, since quickly obtaining such data can be crucial to resolving cybercrime cases; give consideration to defining a simplified system of cooperation between EU Member States in criminal matters, for cybercrime, for the purpose of obtaining data and implementing decisions aimed at putting an end to illegal activities ('digital Schengen') (cf. 5.2.3, 5.4.4, 5.5, 7.5.1, 7.6);

13. Following the annulment of Directive 2006/24/EC of 15 March 2006, reflect on the appropriate way to remedy the lack of harmonisation of national laws in the area of electronic traffic data retention, whilst complying with the case-law of the Court of Justice of the European Union on the protection of fundamental rights (cf. 5.2.3, 5.5);

14. Invite Member States (and, where appropriate, third States) that have not yet done so to ratify the Council of Europe Budapest Convention on Cybercrime and promote further reflection, within the framework of the Council of Europe, on how to adapt the Budapest Convention to the requirements of cross-border investigations, possibly via the adoption of a protocol; in particular, making foreign legal entities subject to the national legal obligations in countries where they officially conduct an economic activity is the main problem in international cooperation involving the private sector. This difficulty has been highlighted by the Robert working group on combating cybercrime (cf. 6.1.2, 7.3, 7.4, 7.6);

15. Support the standardisation of the training provided for practitioners (judges and police and gendarmerie officers) with reference to defined profiles such as, for example, the *Training Competency Framework* drawn up by Europol/EC3 in conjunction with CEPOL, ECTEG and Eurojust; facilitate recognition of such training within the Member States through the implementation of a European certification system (cf. 8.1, 8.2, 8.4);

16. A dialogue with the main Internet operators, hosting companies and Internet access and/or service providers must be organised rapidly at both the EU and the international level, in order to strengthen their cooperation in the context of judicial investigations and redefine an overall framework appropriate to the obligations of these service providers. The implementation of the European Agenda on Security could provide an opportunity to develop some initiatives along these lines (cf. 9.1);

17. Technical or legal solutions should be put in place at Union level to prevent the increasingly systematic use of encryption by operators, in particular on the Internet, becoming an obstacle to the exercise by the competent services of their investigating powers in accordance with the law (cf. 9.1).

Member States should:

18. Facilitate, with the support of Eurojust, the creation of a European network of judges specialising in the fight against cybercrime, aimed at improving and facilitating judicial cooperation in this field (see also Recommendation 20), (cf 7.1, 7.6);

19. Launch, based on the French model, a process of reflection involving the institutional, economic and community stakeholders concerned with a view to establishing a national strategy to combat cybercrime (cf. 3.2, 3.5);

20. Make use of the following French best practices, which have the potential to achieve excellent results, while respecting fundamental rights:
- undercover investigations, which are particularly useful in protecting minors against sexual offences,
- granting powers to investigators, under conditions clearly defined by law, to penetrate information systems and capture remote data by means of spyware,
- the French Anti-Cybercrime Expert Centre (CECyF), set up as part of the European 2CENTRE project financed by the European Commission and aimed at establishing centres of excellence in Europe to combat cybercrime,
- the PHAROS police platform, which records illicit online content and whose originality and success deserve to be highlighted,
- the national database of child pornography content (CALIOPE), which operates in liaison with INTERPOL,
- the Observatory for Payment Card Security established at the Banque de France, whose mission is to improve the security of payment cards.

9.2.3 Recommendations to Eurojust/Europol/ENISA

Eurojust should:

21. Raise the awareness of the law enforcement authorities regarding the possibilities offered by Eurojust for facilitating and accelerating cooperation with the competent authorities of Member States and third States in the field of cybercrime (cf. 7.1.2, 7.6);

22. Promote exchanges between specialised judges in the field of cybercrime with a view to identifying best practices and improving judicial cooperation (cf. 7.1, 7.6);

Europol should:

23. Continue and step up the support offered to Member States in implementing, with due regard for the judicial and operational culture of each State, the training courses and awareness-raising material designed for practitioners by the agency (cf. 8.1, 8.2, 8.4);

24. Improve the distribution of operational products and services to investigation services; improve the dissemination of information on European projects, such as the 'Freetools' project, which can support the work and meet the needs of specialised services (cf. 7.1);

25. Capitalise on the deployment of the SIENA system in the investigation services in order to encourage the exchange of operational information (cf. 6.2.4);

26. Heighten the visibility of EMPACT projects by mapping actions undertaken in connection with operations initiated by Focal Points TERMINAL, CYBORG, TWINS and J-CAT (cf. 7.1.2).

ANNEX A: PROGRAMME FOR THE ON-SITE VISIT

Tuesday, 28 October 2014

General Secretariat for European Affairs (SGAE), Paris

09.00 to 10.15: Welcome to the SGAE – Salle Lisbonne
Ms Isabelle JEGOUZO, Deputy Secretary-General/SGAE
Mr Frédéric MOLLARD, Head of sector, European Security Area, SGAE

10.30: General Secretariat for National Defence and National Security/National Agency for the Security of Information Systems (ANSSI), Paris

- introduction by Deputy Director-General
- general presentation of the political and strategic context and overview of the development of cyber capacities in France
- presentation of ANSSI
- presentation of the Operational Centre for the Security of Information Systems (COSSI), with a practical demonstration of how incidents are dealt with
- presentation on cooperation among State operational services by Mr Laurent Verdier.

12.00: lunch at ANSSI

14.15: National police – Central Directorate of the Criminal Police, Nanterre

- presentation of the Sub-directorate for the Fight against Cybercrime, in particular its operational arm in the shape of the investigation teams
- focus on the internet section, comprising the PHAROS reporting platform, the fraud information system and the new internet office

- presentation on international cooperation, with a focus on three essential issues:
- preservation of technical data;
- exchange of digital data;
- presentation of the 24/7 contact points and their strategic role in international cooperation
- presentation of the Central Office for the Prevention of Violence against Persons (OCRVP), which is responsible for the fight against child pornography on the internet

Wednesday 29 October

9.30: French Data Protection Authority (CNIL), Paris

- welcome address by the General Secretary of the CNIL, Mr Edouard GEFFRAY: general presentation of the CNIL's core tasks
- outline of a priori data monitoring powers, in particular the conduct of operations in the police/justice sector
- presentation on the CNIL's monitoring powers, and a practical demonstration of its sanctioning powers by means of specific cases

13.00: lunch at the National Gendarmerie's Judicial Centre (PJGN)

14.30: **National Gendarmerie – Sub-directorate of the Criminal Police/National Gendarmerie's Judicial Centre (PJGN), Rosny-sous-bois**

- general presentation of the gendarmerie's general set-up, and also of the Cybercrime and Digital Analysis Investigation Board (PICyAN) within the PJGN/SCRC+IRCGN
- visit to the electronics/informatics department (INL) of the IRCGN/practical demonstrations
- Cybercrime Unit: child abuse (monitoring, coordinated operations) and the National Centre for the Analysis of Child Pornography Images (CNAIP)
- Cybercrime Unit: presentation of the internet investigations department (D21)
- Cybercrime Unit: presentation of the 'one-stop shop' for information technologies (GUTI)

Thursday, 30 October

09.00: Ministry of Justice – Directorate for Criminal Matters and Pardons, Paris

- Office for General Criminal Law Matters (BPAPG)
- Criminal Police Office (BPJ)
- Economic and Financial Law Office (BEFI)
- Office for Combating Organised Crime, Terrorism and Money Laundering (BULCO)
- Office for International Mutual Assistance in Criminal Matters (BEPI)

12.00: lunch

14.30: **Police Headquarters/Criminal Police Directorate/Sub-directorate for Economic and Financial Affairs, Paris**

- presentation of the set-up of the specialised criminal police at regional level and its links with the national structure
- the specific case of Paris and how it fits in with the national structures (national police / National Gendarmerie)
- Information Technology Fraud Investigation Unit (BEFTI) and its remit: attacks on automated data processing systems and on personal data, pirating of software
- Payment Fraud Unit (BFMP) and bank card fraud, fake payment orders, e-commerce and the Economic and Financial Crimes Prevention Unit (BRDA): internet fraud
- Child Protection and Child Pornography Unit
- visit to BEFTI

- workstations and equipment linked up to the electronic analysis and investigation system and the universal extraction mechanism for digital investigation and analysis
- list of equipment and software
- best practices: minimum requirements for the taking of evidence (loyalty and integrity) in the French system based on the personal conviction of the judge.

18.30: Ministry of Foreign Affairs and International Development (MAEDI), Paris

Meeting with Ms Michèle RAMIS, Ambassador responsible for the fight against organised crime

Friday 31 October 2014:

09.15 to 11.30 – Closing meeting at the General Secretariat for European Affairs, Paris

Mr Frédéric MOLLARD, Head of the 'Security of the European Area' sector, SGAE

in the presence of representatives from the Ministries concerned by the evaluation.

ANNEX B: PERSONS ENCOUNTERED

Meetings on 28 October 2014

Venue: General Secretariat for European Affairs (SGAE), Paris

Person interviewed/met **Person interviewed/met**	**Organisation represented**
Ms Isabelle Jegouzo	SGAE
Mr Frédéric Mollard	SGAE
Ms Faiza ABDELOUAHAB	SGAE

Venue: National Agency for the Security of Information Systems (ANSSI)

Person interviewed/met **Person interviewed/met**	**Organisation represented**
Mr Dominique RIBAN	Deputy Director-General (ANSSI)
Mr Christian Daviot	Officer in charge of strategy (ANSSI)
Mr Laurent VERDIER	ANSSI

Venue: Central Directorate of the Criminal Police (DCPJ)

Person interviewed/met **Person interviewed/met**	**Organisation represented**
Valérie Maldonado, Divisional Superintendent, Deputy Head, SLDC and Head, OCLCTIC	SDLC/OCLCTIC
Delphine GAY, Commander	OCLCTIC
Pierre Yves LEBEAU, Commander	OCLCTIC
Mathilde CERF, Deputy Superintendent, Head, OCRVP	OCRVP
Chantal ZARLOWSKI, Commander	OCRVP

Meetings on 28 October 2014

Venue: French Data Protection Authority (CNIL)

Person interviewed/met **Person interviewed/met**	**Organisation represented**
Mr Edouard Geffray	CNIL

Meetings on 30 October 2014

Venue: Directorate for Criminal Matters and Pardons (DACG)

Person interviewed/met **Person interviewed/met**	**Organisation represented**
Frédérique Dalle	In charge of negotiation – DACG
Claire Vuillet	BPPG – DACG
Clément Incerti	BPJ – DACG
Aurélien Letocart	BULCO – DACG
Vincent Filhol	BEFI – DACG
Amélie Rodrigues	BEPI – DACG

Venue: Ministry of Foreign Affairs and International Development (MAEDI)

Person interviewed/met **Person interviewed/met**	**Organisation represented**
Ambassador Michèle Ramis	Ministry of Foreign Affairs and International Development (MAEDI)
Mr Léonard ROLLAND	Directorate of Strategic Affairs, Security and Disarmament
Ms Anne LEBOURGEOIS	European Union Directorate

ANNEX C: LIST OF ABBREVIATIONS/GLOSSARY OF TERMS USED

LIST OF ACRONYMS, ABBREVIATIONS AND TERMS	ACRONYM IN FRENCH OR IN ORIGINAL LANGUAGE	FULL NAME IN FRENCH OR IN ORIGINAL LANGUAGE	ENGLISH
ANSSI	*ANSSI*	*Agence Nationale de la Sécurité des Systèmes d'information*	National Agency for the Security of Information Systems
BEFTI	*BEFTI*	*Brigade d'Enquête des Fraudes aux Technologies de l'Information (Préfecture de police de Paris)*	Information Technology Fraud Investigation Unit (Paris Police Headquarters)
BFMP	*BFMP*	*Brigade des Fraudes aux Moyens de Paiement (Préfecture de police de Paris)*	Payment Fraud Unit (Paris Police Headquarters)
BPM	*BPM*	*Brigade de Protection des Mineurs (Préfecture de police de Paris)*	Child Protection Unit (Paris Police Headquarters)
CERT			Computer Emergency Response Team
COSSI	*COSSI*	*Centre Opérationnel de la Sécurité des systèmes d'Information*	Operational Centre for the Security of Information Systems
CNAIP	*CNAIP*	*Centre National d'Analyse des Images Pornographiques*	National Centre for the Analysis of Child Pornography Images
CNIL	*CNIL*	*Commission Nationale de l'Informatique et des Libertés*	French Data Protection Authority
DACG	*DACG*	*Direction des Affaires Criminelles et des grâces (Ministère de la Justice)*	Directorate for Criminal Matters and Pardons (Ministry of Justice)
DCPJ	*DCPJ*	*Direction Centrale de la Police Judiciaire (Ministère de l'Intérieur)*	Central Directorate of the Criminal Police (Ministry of the Interior)
DGGN	*DGGN*	*Direction Générale de la Gendarmerie Nationale*	Directorate-General of the National Gendarmerie (Ministry of the Interior)

LIST OF ACRONYMS, ABBREVIATIONS AND TERMS	ACRONYM IN FRENCH OR IN ORIGINAL LANGUAGE	FULL NAME IN FRENCH OR IN ORIGINAL LANGUAGE	ENGLISH
DGSI	*DGSI*	*Direction Générale de la Sécurité Intérieure (Ministère de l'Intérieur)*	Directorate-General for Internal Security (Ministry of the Interior)
ENISA	*ENISA*	-	European Union Agency for Network and Information Security
GENVAL	*GENVAL*	*Groupe de travail "Questions Générales y compris l'Evaluation"*	Working Party on General Matters including Evaluation
GUTI	*GUTI*	*Guichet Unique des Technologies de l'information*	'One-stop shop' for information technologies
IP	-	-	Internet Protocol
JIRS	*JIRS*	*Juridictions interrégionales spécialisées*	Specialised interregional courts
OCLCTIC	*OCLCTIC*	*Office Central de Lutte contre les infractions liées aux technologies de l'information et de la communication*	Central Office for Combating Information and Communication Technology Crime
OCRVP	*OCRVP*	*Office Central de Répression de la Violence aux Personnes*	Central Office for the Prevention of Violence against Persons
OSCP	*OSCP*	*Observatoire de la sécurité des cartes de paiement*	Observatory for Payment Card Security
PI-Cyan	*PI-Cyan*	*Plateau d'Investigation Cyber-Analyse Numérique (Gendarmerie Nationale)*	Cybercrime and Digital Analysis Investigation Board
PJGN	*PJGN*	*Pôle Judiciaire de la Gendarmerie Nationale*	National Gendarmerie's Judicial Centre
SGAE	*SGAE*	Secrétariat Général des Affaires Européennes (Premier ministre)	General Secretariat for European Affairs (Prime Minister)
STAD	*STAD*	Système de Traitement Automatisé de Données	Automated data processing (ADP) system
VOIP	-	-	Voice Over IP