Council of the
European Union

Brussels, 28 July 2017
(OR. en)

8188/1/17
REV 1 DCL 1

GENVAL 42
CYBER 57

**DECLASSIFICATION**

| | |
|---|---|
| of document: | 8188/1/17 REV 1 RESTREINT UE/EU RESTRICTED |
| dated: | 18 May 2017 |
| new status: | Public |
| Subject: | Evaluation Report on the seventh round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating cybercrime"<br>- Report on Sweden |

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

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

Council of the
European Union

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

**8188/1/17**
**REV 1**

**RESTREINT UE/EU RESTRICTED**

**GENVAL 42**
**CYBER 57**



**REPORT**

| | |
|---|---|
| Subject: | Evaluation Report on the seventh round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating cybercrime"<br>- Report on Sweden |

**ANNEX**

**Table of Contents**

# 1 EXECUTIVE SUMMARY

The visit was well prepared by the Swedish authorities and included meetings with the relevant actors with responsibilities in the field of preventing and combating cybercrime as well as in the implementation and operation of European policies, e.g. the Ministry of Justice, the Swedish Prosecution Authority, the Swedish Economic Crime Authority, the Swedish Police Authority, Swedish Civil Contingencies Agency, ECPAT Sweden.

During the on-site visit the Swedish authorities provided the evaluation team with sufficient information on legal and operational aspects of preventing and combating cybercrime, cross-border cooperation and cooperation with EU agencies. Thus the evaluation team was able to satisfactorily review the system, and good practices to be shared with other member states were identified.

Sweden sees the fight against cybercrime as a priority and has already implemented several measures that reflect this. However, Sweden currently does not have a National Cybersecurity Strategy. The Swedish Government is working on such a strategy, one that will set priorities for the various independent governmental agencies and lay down follow-up procedures. This should also ensure sufficient coordination between all actors.

Sweden has not yet ratified the Convention on Cybercrime (signed by Sweden on 23.11.2001). During the on-site visit the authorities confirmed their intention to ratify it during the present term of office (ends 2018). The ratification will certainly strengthen the international cooperation between Sweden and the parties to the Convention (51 States).

In general Sweden has national legislation penalising cybercrime offences that it considers sufficient and in conformity with EU legislation. These offences are described in terms that are as technology - neutral as possible, rather than using the definitions from EU law. This may detach the legislation more from further technological developments, but it could also cause legal uncertainties and difficulties in practice and with regard to comparable statistics.

Sweden has launched several legislative inquiries in order to improve and adapt the legal framework to the problems of cybercrime. Given the fact that the Swedish Code of Judicial Procedure was introduced in 1942 and many sections have not been changed since then, prosecutors underlined some problems with respect to the application of the law in practice that sometimes give rise to legal uncertainty.

In numerical terms the statistics presented to the evaluation team seem to be incomplete. The lack of detailed, comprehensive and standardised statistics on cybercrime may result in difficulties in identifying the main threats to Swedish cyberspace. However, an inquiry is currently ongoing into the gathering of statistics.

Also, as is typical in this area, a large number of cybercrimes go unreported. The private sector is not under an obligation to report crimes, not even when it concerns a critical infrastructure. Sweden is currently in the process of implementing the NIS Directive[1].



[1] Directive 2016/1148 of the European Parliament and the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

The Cybercrime Centre of the Swedish Police (SC3) has been created within the police as a specialised office. SC3 focuses on the most complex cybercrime cases. In addition, it will provide the regional levels with technical support, best practices, training, updates and intelligence building. SC3 closely cooperates with the specialised prosecutors in an informal and supportive manner.

The Swedish Prosecution Authority has implemented measures to strengthen the capacity to investigate cybercrime and increase general knowledge in that regard. A specialised network of prosecutors dealing with cybercrime was established in 2015. The prosecutors in the network have access to a special website where the prosecutors discuss different operational matters and share information regarding, for example, new legislation and relevant judgements. These prosecutors are given advanced training in cybercrime and have special experience in this area.

The practitioners met during the evaluation agreed on the necessity to improve judicial training and expertise in combating cybercrime.

In general, Sweden has very advanced cooperation between the public and the private sectors in combating and preventing cybercrime. Sweden focuses both on prevention and on awareness raising. With regard to combating online child exploitation, Sweden has an impressive and well-integrated approach and cooperates closely with various governmental and private actors. Blocking of online child abuse material is done expediently, regardless of the host location.

In the field of mutual legal assistance (MLA), the Swedish authorities assist foreign states as much as possible and with every measure that is available to Swedish authorities in domestic investigations or proceedings. A comprehensive registration system has been put in place at the SPA for this purpose. As a result, the time spent handling a request for MLA generally does not exceed two months.

A key element in the successful efforts by Sweden to establish cooperation with private US counterparts has been channelling of all requests and responses through a Single Point of Contact (SPOC). Applying the SPOC concept allows for a smooth processing of requests both for the Swedish Police and private US counterparts.

Taking into account Sweden's ambitious approach in terms of countering cybercrime and its intention to continuously strengthen cybersecurity, the evaluators consider that the situation in Sweden is promising.

## 2 INTRODUCTION

Following the adoption of Joint Action 97/827/JHA of 5 December 1997[2], a mechanism for evaluating the application and implementation at national level of international undertakings in the fight against organised crime had been established. In line with Article 2 of the Joint Action, the Working Party on General Matters including Evaluations (GENVAL) decided on 3 October 2013 that the seventh round of mutual evaluations should be devoted to the practical implementation and operation of the European polices on 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 that end, the evaluation covers three specific areas: cyber attacks, child sexual abuse/pornography online and online card fraud. The evaluation should undertake a comprehensive examination of the legal and operational aspects of tackling cybercrime, cross-border cooperation and cooperation with relevant EU agencies. Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography[3] (transposition date 18 December 2013), and Directive 2013/40/EU[4] on attacks against information systems (transposition date 4 September 2015), are particularly relevant in this context.



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

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

Experience from past evaluations show 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's/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 both to suppression of cyber attacks and fraud and to 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.



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

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

7 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. Sweden was the twenty-eighth 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 was drawn up by the Presidency. Member States 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's/EC3 should be invited as observers.

The experts charged with undertaking the evaluation of Sweden were Ms Cristina Schulman (Romania), Mr Robrecht De Keersmaecker (Belgium) and Mr Marcin Golizda-Bliziński (Poland). Two observers were also present: Mr Tjabbe Bos (the Commission) and Mr Murat Ayilmaz (Eurojust), together with Mr Michael Carlin and Mr Sławomir Buczma 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 Sweden between 27 and 30 September 2016, and on Sweden's detailed replies to the evaluation questionnaire together with its detailed answers to subsequent follow-up questions.

# 3 GENERAL MATTERS AND STRUCTURES

## 3.1 National cyber security strategy

The development of a National Cyber Security Strategy is currently under way in Sweden with the aim, inter alia, of further enhancing Swedish capacity and of providing a comprehensive approach to tackle all aspects of cybercrime. It is planned to put in place a National Cyber Security Strategy by summer 2017.

Although at the time of the on-site visit a draft of the document was not available, it was stated that the upcoming strategy on cyber security will include an introduction and it will give overall direction to a range of measures ongoing and planned.

## 3.2 National priorities with regard to cybercrime

In recent years special attention has been paid to a number of policy areas, including legislation, organisation, training, international cooperation etc.

There are a few links between the EU Cybercrime Priority and the work in the cybercrime field within the Swedish Police. Sweden is participating in the international cooperative arrangement based on the priorities. Some work taking place in the Swedish Cybercrime Centre is based upon EU directives and recommendations. For example, the Europol iOCTA (Internet Organised Crime Threat Assessment) is used as a basis when it comes to cybercrime intelligence.

The Swedish authorities expressed the opinion that information on the current priorities and the link between EU priorities and the national priorities could be made more visible for the staff.

### 3.3 Statistics on cybercrime

The Swedish National Council for Crime Prevention (Brå), an authority under the Ministry of Justice, produces and publishes Sweden's official crime statistics. The crime statistics include, for example, the number of reported offences, person-based clearances and court decisions. As not every offence is reported, the data does not represent the actual crime levels. Changes in the tendency to report offences, comprehensive cases (i.e. cases that involve an extraordinarily high number of reported offences) certain years and the authorities' focus on different types of crime can also affect the statistics even though the actual crime level may be unaltered. It is the Police Authority that is responsible for entering a report of a suspected crime into the system. This can take place either on the basis of a complaint or information received from a private citizen or company, or, as is often the case, on the basis of its own work such as in connection with surveillance.

The official statistics comprise all offences that are reported to the law enforcement agencies by individuals or by the public or private sectors. It is not possible to identify all offences that are related to cybercrime but there is data on a number of offences that relate in different ways to information technology. However, the number and/or categories of data reported by the various actors (police, prosecutors etc.) are not always comprehensive and consistent. Brå has compiled a report that maps out the incidence of information technology -related elements amongst the reported offences. The report was published in September 2016.

#### 3.3.1 Main trends leading to cybercrime

In recent years there has been an increase in the incidence of computer fraud and fraud committed using the Internet. It also seems that different kinds of harassment and threat on the Internet, for example in social media, have been increasing, though given a lack of official data such a trend cannot be confirmed by numbers. Main trends include ransomware, DDoS (isolated attacks and attacks including extortion and ransom), banking malware, Crime-as-a-Service and Business Email Compromise.

### 3.3.2 Number of registered cases of cyber criminality

Data on different types of information technology- related offences in Sweden in 2014 and 2015.

| *Offence* | *Reported offences* | *Investigated offences* | *Person-based clearances*[8] | *Court decisions*[9] | *Persons suspected* |
|---|---|---|---|---|---|
| Computer fraud | 42 883/ 67 085 | 13 136/ 14 570 | 745/391 | Data not available | 440/427 |
| Fraud using the Internet | 23 528/ 24 124 | 13 483/ 13 012 | 2 674/ 2 537 | Data not available | 908/909 |
| Internet-related child pornography crimes | 738/488 | 865/502 | 617/307 | Data not available | 214/181 |
| Unauthorized access to or use of a computer system | 8 200/ 6 663 | 3 266/4 050 | 1 089/1 753 | 108/63 | 217/219 |



[8] Person-based clearances are offences that have resulted in initiated prosecutions, issues of summary sanction orders or issues of a waiver of prosecution.

[9] Court sentences (as imprisonment, probation and suspended sentence), prosecutor's fines and waivers of prosecution.

Two other offences which often are committed via the Internet, though the incidence cannot be determined from the official crime statistics, are contact with children for sexual purposes ("grooming") and exploitation of children under 18 years for sexual posing:

| *Offence* | *Reported offences* | *Investigated offences* | *Person-based clearances* | *Court decisions* | *Persons suspected* |
|---|---|---|---|---|---|
| Contact with a child for sexual purposes ("grooming") | 143/140 | 130/110 | 12/4 | 0/1 | 25/12 |
| Exploitation of child under 18 years for sexual posing | 1 513/991 | 1 378/1 119 | 1 017/642 | 20/27 | 101/116 |



### 3.4 Domestic budget allocated to prevent and fight against cybercrime and support from EU funding

The annual budgetary appropriations decided by the Government for the agencies are guided by objectives and specific priorities. The Parliament and the Government decide on the direction of and conditions for central government activities and which activities and responsibilities are assigned to the agencies. The agencies have far-reaching powers in their day-to-day operational work and the Government, under the Constitution, cannot interfere in individual cases. However, it is the task of the Government to direct the agencies and to ensure that they fulfil their responsibilities by means of the regular appropriations process, legislation and regulation, Government commissions, evaluations etc.

Cybercrime is one of the priorities set by the National Programme on the implementation of the Internal Security Fund (ISF). In the coming years, ISF-funded projects on cybercrime and cyber security will therefore be implemented. Furthermore, the Swedish Police has been and is a partner in some projects funded by the Secure Societies strand of Horizon 2020. At present, the Swedish Police are participating in a consortium with the Bundeskriminalamt in Austria and its counterpart in Germany to prepare a bid for Secure Societies on virtual currencies and the Darknet.

### 3.5 Conclusions

- Sweden does not have a National Cyber Security Strategy but one is currently being developed in order to provide a comprehensive approach to tackling cybercrime. The lack of such a strategy does not prevent Sweden from actively pursuing the fight against and the prevention of cybercrime, but, in the experts' view, without a comprehensive National Cyber Security Strategy these efforts risk being piecemeal.

- Sweden lacks also a commonly agreed set of priorities with regard to cybercrime, in particular to combat cybercrime committed by organised criminal groups and generating large criminal profits such as online and payment card fraud, cybercrime such as online Child Sexual Exploitation which causes serious harm to its victims, and cyber-attacks which affect critical infrastructure and information systems in the EU.

- The Ministry of Justice is the main institution responsible for ensuring that these tasks are fulfilled. In addition, cooperation also takes place with other ministries such as the Ministry for Industry and Trade, the Ministry for Foreign Affairs, and the Ministry of Education in accordance with established procedures and practices, i.e. an inter-ministerial working group has been formally set up in the field of cyber security.

- The private sector is not directly involved in drafting the upcoming National Cyber Security Strategy though private sector stakeholders are part of the existing framework of consultative platforms. The next step in finalising the strategy will involve their input.

- Although certain statistics on cybercrime are available, they appear to often refer to information technology in general, and not to specific categories of clearly defined cybercrimes. It was stated that the police collects all data on reporting, but it is unclear why the various actors (different police services, prosecutors, etc.) gave different numbers and/or categories.

- The Swedish Government carries out its strategies through the allocation of funding, rather than hierarchically. The lack of a national cyber strategy seems to prevent a clear overview of the total amounts dedicated to the fight against cybercrime and the prevention thereof.

# 4 NATIONAL STRUCTURES

## 4.1 Judiciary (prosecution and courts)

### 4.1.1 Internal structure

*Courts*

Cybercrime acts are dealt with by the general courts (district courts, courts of appeal and the Supreme Court) in the same manner as other criminal acts. Although no formal cyber crime specialisation for judges is provided for, some training or support appears to exist for judges dealing with cybercrime. The various partners found the lack of in-depth knowledge among judges to be an obstacle hindering efficient law enforcement.

*Prosecution*

Criminal investigation is within the remit of the general prosecution service. Cybercrime is dealt with by the general prosecution service though there are prosecutors specialising in cybercrime who closely collaborate in the form of a network, with an extensive training programme for every prosecutor and an advanced curriculum for the specialists. The public prosecution service consists of the Swedish Prosecution Authority and the Swedish Economic Crime Authority.

*The Swedish Prosecution Authority*

There are seven geographical public prosecution areas and a National Public Prosecution Department. The prosecution areas consist of 32 general public prosecution offices, with a geographical field of operation approximately equivalent to a county. The Authority also has three international public prosecution offices, in Gothenburg, Malmoe and Stockholm.

*The Swedish Economic Crime Authority*

The Swedish Economic Crime Authority is a special prosecution authority for combating economic crime, such as bookkeeping crime, tax crime and crime against the financial interests of the EU. The Authority also has responsibility for coordination between the agencies as regards measures against economic crime. The Authority also employs police officers, forensic accountants and analysts.

### 4.1.2 Capacity for and obstacles to successful prosecution

The Swedish Prosecution Authority has recently implemented measures to strengthen the capacity for and the general knowledge of cybercrime investigation. In 2015, for example, the Prosecution Authority established a network of prosecutors concerned with cybercrime. The network consists of sixteen prosecutors representing different regions and is geographically spread over the country. The prosecutors have participated in different training courses on how to handle cybercrime and have special experience in this area. The prosecutors in the network have access to a special website on the Prosecution Authority's intranet where the prosecutors discuss different matters and problems and share information regarding, for example, new legislation and interesting judgements. They have seminars and co-operate with the police. Other prosecutors can turn to the prosecutors in the network with cybercrime related questions.

Another example mentioned is the web-based guide for prosecutors that was launched in 2015. The guide provides information about, for example, cybercrime-related coercive measures, under what circumstances subscriber information/IP-addresses can be obtained from internet service providers, the MLA process and preservation requests etc. The guide also contains contact details of international internet service companies (Facebook, Google, etc.) which are important since there is often evidence stored under the control of these companies and the prosecutors need to know if it is possible to obtain this information and, in that case, how to proceed. The cybercrime area is in constant change. The web -based guide will be continuously amended and updated.

The main obstacle reported by the Swedish Prosecution Authority is obtaining IP addresses and basic subscriber information from certain internet service providers. Canada is of some interest since the KIK app is Canadian and voluntary disclosure is not permitted. This means that the prosecutors need to use MLA to obtain the information needed.

### 4.2 Law enforcement authorities

On 1 January 2015, the National Police Board and the 21 police authorities were merged into a single unified agency, while the Swedish Security Service became an independent agency. This is the largest reorganisation in the government sector in many years and the largest change affecting the Swedish Police since it was nationalised in 1965. The aim of the reform was to deal with organisational obstacles within the Swedish Police and thereby create better opportunities for the Swedish Police to prevent, take measures against and investigate crime.

Organisationally, the Authority comprises seven police regions, a number of national departments and an office. The seven police regions have overall responsibility for police activities within a certain geographical area. This responsibility includes investigative activities, crime prevention activities and service. Each region is led by a regional police commissioner. The head of the Swedish Police Authority is the National Police Commissioner, who is appointed by the Government. The National Police Commissioner has sole responsibility for the Authority's activities.

On 1 October 2015, the Swedish Police established a **Cybercrime Centre** (SC3) with the key aim of building capacity throughout the Police to investigate all forms of cybercrime. SC3 will gradually be built-up and will include specialised investigators, analysts, forensics and experts. The cybercrime intelligence team at the Swedish Cybercrime Centre is responsible for detecting, preventing and averting serious cybercrime. The team tries to share information with relevant partners about current trends, threats and specific technical information (IOC's – Indicators of Compromise).

The number of personnel at SC3 is currently being increased, the aim being to a full complement of staff by the end of 2017. SC3 is the single contact point not only for prosecutors offices and courts in Sweden but also for private entities in cybercrime. It is also competent to deal with the most important and biggest cybercrime cases. To be able to fulfil its' tasks, SC3 has mobile teams to support regional police departments in cybercrime matters. But Sweden aims to have cybercrime centres in each of its 7 regions. SC3 has its own investigation unit dealing with Internet surveillance, automatic information gathering in the social media, securing web pages and for covert operations. This investigation unit has subunits specialising in requests to ISSs, intelligence, forensic analysis of digital media, method development, coordination, child protection and also a specialized police unit dealing with fighting cybercrime in the Darknet.

SC3 is organising national training sessions for law enforcement. It has also created a special website for law enforcement on which experiences and expertise can exchanged and gained. It also offers training sessions with prosecutors and law enforcement. SC3 is working closely with the EC3, within the Nordic context, Interpol, and also on a bilateral level with many international agencies. It carries out the role of 24/7 via the officer in charge at the National Operative Department. This function was set up many years ago in connection with work under the G8 Lyon Group to operationalise the Budapest Convention.

The **National Fraud Centre** (NFC) was set up in 2013. Experienced police officers from the NFC support investigators regionally and locally in their investigations and share best practice. The National Fraud Centre is also working closely with the National Forensic Centre and the National Cybercrime Centre to be at the forefront. It has no investigative capabilities itself, but only coordinates and supports. Currently, they are concentrating on „card not present"-fraud. In the past they ran an awareness campaign for CEOs on „business email compromise"-fraud.

As an example, the NFC has a database of bank accounts that were already scrutinized in earlier investigations in the past two years. Before requesting information on bank accounts, the police first check this database. It works on a hit/no hit basis. If there is a hit, the investigator receives the case number of the case in which the previous request was made and the actual information can be retrieved through official channels. If it is a no-hit, a new request is automatically sent to the bank. This request is made up in a standardised form, so that the replies from the banks can also be automated. The NFC also created a manual on virtual currencies.

From the perspective of prosecutors, Swedish law enforcement needs to be have more staff for the faster analysis of data. Sweden has in fact already recognised this and aims to improve the situation by staffing up the relevant units. As mentioned by the Swedish Police, the main areas to be improved in conducting successful investigations concern overall structure, guidelines, resources and competence in the field of cybercrime and cyber- related crimes.

Among the obstacles are the fact that crimes are not reported, proof and material such as logs and other crucial evidence are missing or insufficient/flawed, providers do not retain or cannot provide subscriber information, the use of different anonymizer services and the lack of effective tools to share information with other countries. In Sweden, Internet service providers are not obliged to retain traffic data for more than six months.

### 4.3 Other authorities/institutions/Public Private Partnership

*The Civil Contingencies Agency*

The Civil Contingencies Agency of Sweden (MSB) is an agency dealing with prevention in the area of cybercrime. It is supervised by the Ministry of Justice and adheres mainly to three principles it applies: responsibility to support, to act and to cooperate. The MSB is working with private and public stakeholders and is responsible for the sector of energy, health, food, public services, security, social security, transportation and traffic. It has four units (training, coordination and cooperation, prevention and development). The MSB is constantly working on improving the strategy based on the current state of play as regards attacks and dangers. The MSB has also special programmes for public agencies to raise awareness of their staff. The MBS has also created a special website for citizens to obtain information, raise awareness, ask questions and notify attacks. Every public agency has to issue a report about cyber risks and send this report to the MBS, so that it can analyse those and react in accordance with its principles.

The MSB is responsible for the national CERT which for instance can share information about current fraud attempts and how actors can protect themselves. The MSB will be the single point of contact in situations where Directive 2016/1148 of the European Parliament and the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (hereinafter called as NIS directive) applies. A legislative inquiry to implement the NIS directive has already started.

*CERT-SE*

The Swedish civil CERT is working closely with the military CERT of Sweden. There is also close cooperation with CERTs from the private sector. In the framework of this cooperation information, new developments, experiences and expertise are exchanged and discussed.

The Swedish CERT has a very intense and diverse system of warnings. It is responsible for warning the public in the event of attacks. The Swedish CERT issues and publishes weekly and sometimes daily reports about current attacks and summaries of the state of play which are sent to other public and private CERTs. The same applies to daily warnings in the event of attacks and risks.

*ECPAT*

ECPAT Sverige (Sweden) was established as an NGO in 1996, and is a member of ECPAT International's global network with representation in over 70 countries. ECPAT Sweden collaborates with other NGOs, authorities and part of the industry to fight the commercial sexual exploitation of children. ECPAT cooperates closely with the Swedish financial industry in cases of child pornography to follow the money and identify the perpetrators using financial investigation. For that purpose international cooperation with agencies from other countries has been established and is being constantly developed. ECPAT works closely with Swedish law enforcement and the judiciary.

### 4.4.Cooperation and coordination at national level

The Parliament and the Government decide on the direction of and conditions for central government activities and which activities and responsibilities are assigned to the agencies. The agencies have far-reaching powers in their day-to-day operational work and the Government, according to the Constitution, cannot interfere in individual cases. However, it is the task of the Government to direct the agencies and to ensure that they fulfil their responsibilities by means of the regular appropriations process, legislation and regulation, Government commissions, evaluations etc.

In the area of preventing and fighting cybercrime and providing cyber security in Sweden the division of tasks rests on the principle of responsibility. This means that an agency that has been given a task via an instruction, a law, a regulation or a commission by the Government is responsible. For instance, the Police have been given the task under the Police Act and various other laws and regulations, the general task of investigating crimes that are defined in criminal law. This means in turn that the Police also have this task regardless of new crime areas emerging or new penal provisions being established.

Since its establishment, SC3 has entered into a cooperation agreement with the Security Service in the field of cybercrime. At present, SC3 and the Civil Contingencies Agency are further developing cooperation mechanisms at operational as well as at strategic level.

### 4.4.1 Legal or policy obligations

At the level of the Government, the Ministry of Justice is the institution mainly responsible. Within the Ministry, there are units dealing with the Police, the Prosecution, the Courts, the Civil Contingencies Agency etc. Cooperation takes place also with other ministries such as the Ministry for Industry and Trade, the Ministry for Foreign Affairs, and the Ministry of Education. There are established procedures and practices for such cooperation and, in the field of cyber security, in particular, an inter-ministerial working group has been formally set up.

The Swedish Prosecution Authority in general does not have direct contacts with the private sector, e.g. the Internet service providers, financial institutions etc. These contacts are handled by the Police.

The Police are working for instance with ECPAT and the County Administration Board that have set up hotlines that the public can use to report all internet-related sexual abuse of children. The information is forwarded to the Police directly. The Police and ECPAT are also active partners in the Financial Coalition

The Police have in some cases asked for assistance from the private sector for voluntary information sharing and some other measures. Collaboration with the major banks whereby information can be provided and action taken has been established. Some cases has been run in cooperation with CERT-SE and there is good cooperation with the private sector (for example the Internet service providers).

### 4.4.2 Resources allocated to improve cooperation

The Swedish Police are up to date regarding equipment and knowledge. In 2013, a National Fraud Centre (NFC) was established. Experienced police officers from the NFC support investigators regionally and locally in their investigations and share best practice.

The Civil Contingencies Agency has an annual budget of 130 million euro for projects in cooperation with the public sector. This could be used for funding research projects, awareness campaigns, research tools, etc.

As regards network and information security, the Civil Contingencies Agency is coordinating a network, SAMFI, comprising the Swedish Armed Forces, Swedish Defence Material Administration, the National Defence Radio Establishment, the Swedish Post and Telecom Authority, the Swedish Police Authority, and the Swedish Security Service. SAMFI meets regularly to deal, inter alia, with policy issues and regulation, training, information activities, and technical issues.

### 4.5 Conclusions

- No systematic training on cybercrime is provided for judges. The evaluators are of the opinion that given the complexity of cybercrime, judges handling cybercrime cases require a high degree of knowledge.

- On the other hand, there are specialised prosecutors dealing with cybercrime cases. All prosecutors receive a mandatory basic cybercrime training and the specialised advanced training is aimed at those prosecutors who deal with cybercrime cases. The evaluation team was impressed by the specialisation and level of know-how management on the part of the prosecutors met.

- In addition, a web-based guide offers a detailed and extensive overview of know-how and best-practices with regard to cybercrime. The guide contains contact details for international Internet service companies (Facebook, Google etc.). This is important since there is often evidence stored under the control of these companies and the prosecutors need to know if it is possible to obtain this information and, in that case, how to proceed. The cybercrime area is constantly changing. The web- based guide will be continuously adjusted and updated. This approach is regarded by the evaluation team as best practice.

- Furthermore, there is a national network of prosecutors working in the area of cybercrime, in which every Public Prosecutors Region is represented by two prosecutors. This network comprises special training modules for prosecutors as well as the most relevant judgements in the cybercrime area and is a platform where current problems are discussed. One member of this national network of cybercrime prosecutors is the member of the European Cybercrime Network at Eurojust.

- There is a very good level of inter-agency cooperation and coordination between different institutions in Sweden, which is carried out within a unique setting of public institutions. The Parliament and the Government decide on the direction of and conditions for central government activities and on which activities and responsibilities are assigned to the agencies.

- There are many actors involved in combating cybercrime in Sweden. The agencies have far-reaching powers in their day-to-day operational work and the Government cannot interfere in individual cases. In the evaluators' view, strengthening the coordination of the efforts made by all actors involved in fighting against cybercrime at the central level could make the system more effective.

- The Police are responsible for investigating crimes that are defined in criminal law, which include new crime areas emerging or new penal provisions being established. A major police reform took place in Sweden in order to deal with organisational obstacles within the Swedish Police and create better opportunities to prevent, take measures against and investigate crime. The Police were restructured into one national police at the central level and offices at the regional level.

- Furthermore, on 1 October 2015, a Cyber Crime Centre (SC3) was established to build capacity to investigate all forms of cybercrime. It is planned to gradually include specialized investigators, analysts, forensics and experts. It has a national unit in Stockholm with seven regional cybercrime centres as field offices. SC3 was created as a central hub, coordinating all efforts within the police services in the field of cybercrime, e.g. when it comes to know-how and expertise building and training, research and development, contacts with other partners (governmental, prosecutors, international, etc.). However, as it is still in its initial stage, the focus is on SC3 and not on the regional centres (e.g. with regard to personnel capacity).

- In addition, in the opinion of the evaluators, the Swedish Police as a whole could improve in the areas of overall structure, guidelines, resources and competence in the field of cybercrime and cyber -related crimes. Obstacles mentioned by Swedish law enforcement representatives include: crimes are not reported, proof and material, e.g. logs and other crucial evidence, are missing or insufficient/flawed, providers do not save or cannot provide subscriber information, use of different anonymizer services and lack of effective tools for sharing information with other countries, limited data retention periods etc. (in Sweden, Internet service providers are not obliged to retain traffic data for more than six months).

# 5 LEGAL ASPECTS

## 5.1 Substantive criminal law pertaining to cybercrime

### 5.1.1 Council of Europe Convention on cybercrime

Sweden has not yet ratified the Convention on Cybercrime (signed by Sweden on 23.11.2001), and no clear explanation of the reasons for this were given. During the on-site visit, the Ministry of Justice confirmed the intention to ratify it during the government's present term of office (ends 2018).

### 5.1.2 Description of national legislation

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

Sweden has transposed Directive 2013/40/EU into national legislation. In order to fulfil the requirement regarding the maximum penalty, a new penalty scale had to be introduced for gross breach of data secrecy (imprisonment for a minimum of six months and a maximum of six years). The new legislation came into force in July 2014.

Attacks against information systems, e.g. illegal access to information systems, illegal system interference and illegal data interference, are criminalised primarily through the provision on breach of data secrecy (Chapter 4, Section 9 c of the Penal Code). Criminal liability requires intent. When assessing whether a breach of data secrecy is gross, special attention should be paid to whether the act has caused serious harm or covered a large amount of data or otherwise has been of a particularly dangerous type. The penalty for breach of data secrecy ranges from fines to imprisonment for a maximum of two years. If the crime is considered gross, a term of imprisonment for a minimum of six months and a maximum of six years is imposed for such a breach of data secrecy. Incitement and aiding and abetting are criminalised. An attempt to commit a breach of data secrecy is also criminalised except in minor cases.

In certain circumstances attacks against information systems could also be criminalised under the provisions on causing damage (Chapter 12, Section 1 or Section 3), or sabotage (Chapter 13, Section 4 or Section 5) or on terrorist offences (Act on criminal responsibility for terrorist offences, Section 2 and Section 3).

Illegal interception of computer data is criminalised under the breach of data secrecy provisions (see above) and breach of postal or telecommunication secrecy provisions (Chapter 4, Section 8 of the Penal Code). Criminal liability for a breach of postal or telecommunication secrecy requires intent. The penalty is a fine or imprisonment for a maximum of two years. A person who employs technical means with the intention of committing a breach of telecommunication may be sentenced for preparation of such a crime if he or she is not responsible for its actual commission (Chapter 4, Section 9 b of the Penal Code). The penalty is a fine or imprisonment for a maximum of two years.

Misuse of devices (production, distribution, procurement for use, import or otherwise making available or possession of computer misuse tools) is primarily criminalised through the provisions on preparation to commit any of the offences described, e.g. preparation to commit a breach of data secrecy. The penalty for preparation to commit an offence is set below the maximum and may be set below the minimum penalty applicable to its commission (Chapter 23, Section 2 of the Penal Code). Different forms of misuse of devices could also be criminalised under the provision of Chapter 4, Section 9 b of the Penal Code.

Under Swedish law corporate fines can be imposed on legal persons for all crimes (including cybercrime) committed in the exercise of their business activities. Corporate fines are a criminal law sanction and may be as low as five thousand Swedish crowns and as high as ten million Swedish crowns. The corporate fines legislation, including the level of sanctions, has recently been subject to a review by a Committee of Inquiry. At the time of the on-site visit the Committee was tasked with presenting its report in November 2016 and the evaluation team was informed that the report was submitted on time.[10]



[10] The evaluation team did not have knowledge of the report and did not take it into account when drafting its findings.

**B/ Directive 2011/93/EU on combating sexual abuse and sexual exploitation of children and child pornography**

Sweden has transposed into national law Directive 2011/93/EU of 13 December 2011. When implementing the Directive Parliament agreed with the Government in finding that Swedish law, with the exception of certain issues concerning limitations on sanctions and control of records, fulfilled the requirements of the Directive. The necessary legislative changes came into force in 2013.

**Contact with a child for sexual purposes (sexual grooming)**

*Contact with a child for sexual purposes* is criminalised under the provision in Chapter 6, Section 10a of the Penal Code. The objective of the legislation is to prevent children under fifteen years of age from being exploited for sexual purposes during physical encounters with adults. The offence requires intent.

In addition to requiring intent with regard to the actions that the perpetrator actually undertakes (e.g. contacts the child on the Internet, agrees on a time and place to meet), the offence also requires that the perpetrator has an intent to commit a sexual offence against the child at the subsequent personal encounter. When determining the penal value of an individual criminal act, the general provisions on aggravating and mitigating circumstances in Chapter 29, Sections 2-3 of the Penal Code apply.

The penalty ranges from a fine to imprisonment for one year. Conspiracy to commit, preparation or attempt to *make contact with a child for sexual purposes* is not criminalised. Incitement and the aiding and abetting of an offence are criminalised under the general provision on aiding and abetting in Chapter 29, Section 4 of the Penal Code.

**Child pornography crime**

It is a criminal offence to depict a child in a pornographic picture, to make such a picture available to someone else, to acquire such a picture for oneself or offer it to someone else, to facilitate in any way the trade in such pictures, or to possess such a picture (See the provisions on *child pornography crime* and *gross child pornography offences*, Chapter 16, Section 10 a of the Penal Code.). Liability for *child pornography crime* or *gross child pornography crime* presupposes intent or negligence. Since 1 July 2010, the mere viewing of child pornographic pictures that one has gained access to is also punishable as child pornography crime. This includes, of course, so called web-viewing without possession. In the criminal provision concerning child pornography it is expressly stated what constitutes child pornography crime (see the provisions for *child pornography crime* and *gross child pornography crime*, Chapter 16, Section 10 a of the Penal Code.) For this purpose, "child" means a person whose pubertal development is not completed or who is less than 18 years of age. The penal provision states that if the pubertal development of the depicted person is completed, liability for all forms of trade in pornographic images of a child except the actual depiction applies only if it is apparent from the picture and the circumstances surrounding it that the person is under 18 years of age.

*A child pornography crime* is punishable by imprisonment for at most two years, or, if the crime is minor, by a fine or imprisonment for at most six months. *Gross child pornography* crime is punishable by imprisonment for at least six months and at most six years. Aggravating factors to be considered when assessing whether a crime is gross are e.g. whether it was committed for profit, was a part of criminal activity that was systematically practised or practised on a larger scale, or concerned a particularly large number of pictures or pictures in which children are especially young, are subject to violence or force or else exposed to especially ruthless treatment (see the provision on *gross child pornography crime*, Chapter 16, Section 10 a paragraph 5 of the Penal Code). Mitigating factors are, e.g., whether the crime concerned only a single picture (see prop. 1997/98:43 page 92).

The general rules regarding multiple crimes/recidivism in the Penal Code are applied. Incitement, aiding and abetting, and attempting to commit *child pornography crime* described in Section 10a, first paragraph, or *gross child pornography crime* are criminalised.

**C/ Online Card fraud**

No specific legislation exists to penalise online card fraud, as it falls under the definition of the general fraud offence.

In 2013, a National Fraud Centre (NFC) was formed. Experienced police officers from the NFC support investigators regionally and locally in their investigations and share best practice. The National Fraud Centre also works closely with the National Forensic Centre and the National Cybercrime Centre to be at the forefront.

## 5.2 Procedural issues

### 5.2.1 Investigative Techniques

The following investigative measures may be applicable under the Swedish law:

- search and seizure of information system/computer data;

Objects reasonably presumed important to a criminal investigation may be seized, for example a computer (Chapter 27, Section 1 of the Code of Judicial Procedure). A search of premises may under certain circumstances be ordered to look for objects subject to seizure (Chapter 28, Section 1 of the Code of Judicial Procedure). A seized object may be examined by the law enforcement authorities. This means that information stored, for example on a hard drive, is available to the authorities.

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

Under the Code of Judicial Procedure Chapter 27 section 18–19, the following investigative techniques in the form of secret coercive measures are permissible:

- Secret interception of electronic communication (Section 18)
- Secret surveillance of electronic communication (Section 19).

*Secret interception of electronic communication* may be used in the preliminary investigation of:

1. offences in respect of which a less harsh penalty than imprisonment for two years is not prescribed for the offence; or
2. some specific serious offences mentioned in Section 2 second paragraph points 2–7
3. attempt, preparation, or conspiracy to commit such an offence if such an act carries a penalty, or
4. another offence in respect of which due to the circumstances a harsher sentence than the minimum two years' imprisonment is envisaged by the law..

*Secret surveillance of electronic communication* may be used in the preliminary investigation of:

1. offences in respect of which a less harsh sentence than six months imprisonment is not prescribed;
2. offences specially mentioned in the section, such as offences that violate of the Penal Law on Narcotics (1968:64), Section 1, or narcotics offences that violate the Law on Penalties for the Smuggling of Goods (1960:418), Section 1; or child pornography crime that violates the Penal Code, Chapter 16 Section 10 a, or
3. some specific serious offences mentioned in Section 2 second paragraph points 2–7
4. attempt, preparation, or conspiracy to commit an offence mentioned in 1–3 above if such an act carries a penalty.

Issues connected with above -mentioned measures are determined by the court at the request of the prosecutor. The duration of surveillance or interception may not be longer than necessary and may not exceed one month from the date of the decision (Section 21).

In urgent situations and if the investigation is likely to be seriously delayed pending a court decision, the prosecutor is authorized to decide on a temporary order. Such a decision must be reported to the court as soon as possible (Section 21 a).

Telephone conversations or other communications between the suspect and his defence counsel may not be subject to secret interception of electronic communication. If during the interception it appears that it is such a conversation or communication, the surveillance must be discontinued. The same applies to conversations between the suspect and those who may not testify in accordance with the Code of Judicial Procedure 36 Chapter section 5 paragraph 2–6 (e.g. lawyers, doctors and priests). Recordings or notes regarding such communications must be immediately destroyed (Section 22).

The above -mentioned secret coercive measures may only be conducted if someone is reasonably suspected of an offence and the measure is of exceptional importance to the inquiry. The measures may only relate to a phone number or address held by the suspect or which may be assumed will be used by him. Secret surveillance and interception of electronic communication may under certain conditions be used in order to investigate persons against whom there are reasonable suspicions.

- preservation of computer data;

Swedish legislation does not provide for domestic preservation orders. However, the authorities reported that preservation requests are sent to other countries.

The authority may preserve computer data during a search of premises when computer and content cannot be seized. That is when a seizure is disproportionate given the suspected felony or in cases where the consequences for the concerned party/owner of the equipment are deemed too serious if seized.

- order for stored traffic/content data;

Pursuant to Chapter 6, Section 16a and Section 16d, of the Electronic Communications Act (2003:389), Internet Service Providers (ISPs) are obliged to store traffic data for six months. (After six months the information must be deleted.)

In order to obtain the traffic data for use in a preliminary investigation, court permission is normally needed and certain requirements must be fulfilled (see the above -mentioned Chapter 27, Sections 18 and 19, of the Swedish Code of Judicial Procedure).

- order for user information.

Pursuant to Chapter 6, Section 16a and Section 16d of the Electronic Communications Act (2003:389), Internet Service Providers (ISPs) are obliged to store user information (such as name, address, phone number etc.) for six months. After six months the information must be deleted. When a crime is suspected, the ISP must give this information to the prosecution or police authority on request (Chapter 6 Section 22 (2) of the Electronic Communications Act). In line with the obligation to store the data in question for six months, the request must of course be made within that time.

However, a particular challenge is that investigations inside Sweden are hampered by the fact that international cooperation as regards accessibility of information and evidence held by private enterprises in a jurisdiction other than the Swedish is far too less developed. Often, a Swedish criminal investigation must be closed due to non-content data not being disclosed by private enterprises in such jurisdictions. The Swedish experience confirms that cooperation with, in particular US and US-based corporations, are key if we are to succeed in fighting cybercrime. Since it is within the legal powers of these corporations to voluntarily disclose non-content data, Sweden has sought to establish agreed ways and procedures for requesting and accessing such information from a number of US-based corporations. In some cases these efforts have been successful. Since 2013, the Swedish Police have, against this background, established a SPOC in relation to Facebook, Instagram, Ask.fm, Google and Apple. Currently, work is under way to reach a similar agreement with Twitter and Periscope.

Applying the SPOC concept has many advantages both for the Swedish Police and a private, US counterpart. For the Swedish Police, this means that the desk at the Swedish Cyber Crime Centre, SC3, maintains an overview and gains experience over time on how to manage the cooperation in the best possible way. It also allows for an appropriate supervision of data protection issues. For the private, US counterpart, the use of a SPOC allows for smoother processing in that the law enforcement SPOC can provide the credentials necessary for requesting non-content data and receiving voluntarily disclosed information.

Investigating cybercrime requires a team of different specialists, IT forensics, investigators and prosecutors. Special investigative techniques include a strong focus on tactics during house searches (live forensics) in order to achieve maximum success with digital evidence, IT forensic analysis of logs and seized computers, lawful interception of communication (both phones and data traffic), advanced open source intelligence (OSINT) and covert operations.

### 5.2.2 Forensic and Encryption

Encryption is used both in data storage and in Internet communications. In the opinion of the Police, more and more encryption is involved and it is becoming harder and harder to get through the encryption. Therefore, better police tactical measures are required when making an arrest.

In general, decryption is carried out in-house. The cooperation with other governmental agencies is considered to be well established and efficient. Some of the agencies may be regarded as specialized. The following problems with encryption have been reported:
- unsupported encryption format (or container);
- apps with unknown encryption procedures:
- in the case of password -based encryption, excessively complex passwords that are difficult to crack;
- the iPhone is a good example that illustrates the problem of encryption.

More intelligent analysis of a suspect's pattern(s) of password creation and dynamic aggregation of computer power have been indicated as possible solutions for the issues raised above. Moreover, the representatives met suggested that the team of different specialists should work together, also with IT forensics. During a search, it is good practice to have close contact with the prosecutor. During the questioning of the suspect, an IT forensic specialist can be present to make sure all technical details are understood.

### 5. 2.3 E-evidence

There are no admissibility rules for e-evidence, or for any other evidence. The free submission and assessment of evidence is a fundamental principle in the Swedish Code of Judicial Procedure. The procedural system does not contain any formal rules on admissibility and assessment of evidence. Anything that may be of value as evidence in a case may, in principle, be presented in court.

Swedish procedural law is mainly technology-neutral, which means that there are no specific regulations regarding e-evidence. The Government has recently appointed an inquiry to investigate certain issues related to seizure and search of premises. The rules on seizure and search of premises entered into force in the 1940s. The legislation focuses on physical objects and written documents. The task includes analysing how the legislation can be adapted to modern technology. The inquiry is supposed to report in September 2017.

### 5.3 Protection of Human Rights/Fundamental Freedoms

Fundamental rights and freedoms are protected in the Constitution. The Constitution also states under which circumstances limitations can be imposed. Such imitations can be imposed, for example, only to satisfy a purpose acceptable in a democratic society. The same rules apply online as offline.

The protection of fundamental rights and freedoms is equally as strong online as offline. Hence, the Police cannot intervene more easily on the Internet than in real life.

## 5.4 Jurisdiction

### 5.4.1 Principles applied to investigate cybercrime

In accordance with the principles of territoriality and ubiquity, Swedish courts can establish jurisdiction over the (whole) crime as long as part of the crime is committed in Sweden. If a cybercrime act is committed entirely outside Swedish territory, Swedish courts can establish jurisdiction over the crime if it is committed by a Swedish citizen or by an alien domiciled here (the active personality principle), provided that the act is subject to criminal responsibility under the law of the place where it was committed (dual criminality). However, in relation to child pornography crimes where the criminal act consists in depicting a child in a pornographic picture and in relation to gross child pornography crimes, the dual criminality requirement does not apply.

Jurisdiction over crimes committed outside Swedish territory can also be established if the crime is committed against the Swedish nation, a Swedish municipal authority or other assembly, or against a Swedish public institution (the protective principle).

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

Often the problem is not that two or more Member States want to prosecute, but that no country will investigate and prosecute. However, when more than one Member State investigates a crime or part of a crime, the question of where the suspect should be prosecuted is often resolved by an agreement in advance, during the investigation. This could mean either:

- Transferring the proceedings from one country to another. This was done in a case regarding computer intrusions in several countries committed by a Swedish citizen in Sweden. Other states transferred their proceedings to Sweden.

- Dividing the case between the Member States, e.g. one country investigates and prosecutes the victims living in that state and vice versa. This was done in a case involving computer intrusions where the person was initially convicted in Sweden and afterwards transferred to Denmark.
- Each country investigates the person who lives in their territory even if they are all part of an organisation. This was done in a case involving the production of child pornography where the photographer was prosecuted in one country and the persons ordering the pictures were prosecuted in their home states (Spain, Sweden and the US).

Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings has been implemented though Sweden keeps no records of the application of EU instruments. There is no experience of referral to Eurojust to settle conflicts of jurisdiction.

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

Crimes committed “in the cloud” can often be pinpointed both to where the perpetrator was when he or she committed the crime and to where the effect occurred. Depending on the type of cybercrime, the effect may be pinpointed to several member states, which may result in conflicts of jurisdiction when two or more member states can establish jurisdiction over the crime.

When the authorities receive an MLA request related to information in the cloud the information has usually been traced to a server in Sweden. As long as that is the case there is no problem in providing MLA regarding information in the cloud. Sometimes, however, the information in question is gone by the time the request is received and in such cases providing MLA is problematic as there is no legal basis for conducting a formal search in “the cloud”.

This situation is becoming increasingly problematic as for instance accounting services are provided as cloud services. At present the Economic Crime Authority is discussing with cloud service providers the question of access to accounts kept in the cloud during criminal investigations.

### 5.4.4 Swedish perception with regard to legal framework to combat cybercrime

According to the Swedish authorities, requests for MLA are often time-consuming and sometimes replies are received too late to be of any real use. The MLA process regarding e-evidence needs to be improved.

There are shortcomings when it comes to access to data that is stored on remote servers ( whether or not they belong to foreign companies). This field is in need of improvement and cooperation with foreign service providers should be enhanced. Insufficient rules on data retention in some states are also an issue.

There are in particular three areas where improvements are required. The first is harmonisation of relevant legislation in the member states (including data retention). The second is an improved MLA process. The third relates to clear guidelines and requirements (obligations) regarding requests from other countries. This includes 24/7 support, response times and clarification as to which types of data require an MLA and in which cases just a police-police contact is sufficient.

## 5.5 Conclusions

- Sweden has not yet ratified the Convention on Cybercrime and no clear reason was given as to why. During the on-site visit the Ministry of Justice expressed its intention to ratify it during the present term of office (ends 2018). It should be underlined that the prosecutors and police officers stressed the need for ratification, including for preservation orders.

- With the exception of the preservation powers, it was stated that the Swedish legislation ensures the implementation of the Convention. However, acceding to the treaty will likely have a significant impact on other areas, including enhancing the possibilities for international cooperation. The relevant stakeholders, e.g. the prosecutors and the police, underlined the urgent need to ratify the Budapest Convention

- In the field of substantive criminal law, the provisions in the Swedish Penal Code are, as far as possible, general and technology-neutral, the intention being to apply them regardless of whether a crime has been committed in an IT environment or not. It is not the purpose of this report to assess whether such an approach is feasible in practice in the context of the tremendous developments in technology.

- Sweden reported that it had transposed Directive 2013/40/EU into national legislation. In order to fulfil the requirement regarding the maximum penalty, a new penalty scale had to be introduced for gross breach of data secrecy (imprisonment for a minimum of six months and a maximum of six years). The new legislation came into force in July 2014. The offences provided for by Directive 2013/40/EU are not penalised as separate offences, and thus collecting and reporting data in line with the requirements of the Directive could be problematic.

- Sweden also reported that it had transposed Directive 2011/93/EU. There is no specific legislation penalising online card fraud, as this appears to be covered by general legislation.

- Regarding procedural law, the approach is also to be mainly technology-neutral, which means that there are no specific regulations regarding e-evidence. The free submission and assessment of evidence is a fundamental principle in the Swedish Code of Judicial Procedure and it can represent good practice. The procedural system does not contain any formal rules on admissibility and assessment of evidence. Anything that may be of value as evidence in a case may, in principle, be presented in court.

- The Government has recently appointed an inquiry to investigate certain issues related to seizure and search of premises. The rules on seizure and search of premises entered into force in the 1940s. The legislation focuses on physical objects and written documents. The task includes analysing how the legislation can be adapted to modern technology. The inquiry is supposed to report in September 2017.

- Sweden currently has several inquiries also aimed at improving provisions in the Criminal Code and Code of Judicial Procedure, for example with regard to seizures. This is necessary because the current legislation is not practical. New legislation will also be introduced with regard to online abuse and online searches in devices. As regards the latter, Sweden acknowledges the problem of encryption and wants to use the results of the inquiry into online search and seizure measures also to gain expertise and improve the technical methods of investigation.

- With regard to data retention, Sweden was awaiting a decision of the Court of Justice of the EU. At the time of the on-site visit, telecommunication providers were by law obliged to retain the data for six months.[11]

- In the opinion of the evaluators, the preservation powers need to be incorporated into national legislation as a separate measure.[12]

- Dealing with evidence in the cloud (from the legislative point of view) seems to be a particular challenge for prosecutors as there are no clear rules in place. At present, securing evidence is possible only if the server can be located and a MLAT is to be used. Considering the uncertainty regarding access to evidence in the cloud among practitioners, it could be helpful to establish at the national level clear rules (amendments or interpretation regarding the application of existing law and participation in international fora e.g. Cybercrime Convention Committee (T-CY) in which Sweden would be able to participate as an observer and where solutions to these issues are discussed).

- The experience of Sweden represents good practice in the way it has organised cooperation with the private US counterpart. Applying the SPOC concept has many advantages both for the Swedish Police and the private, US counterpart. For the Swedish Police, this means that the desk at the Swedish Cyber Crime Centre, SC3, maintains an overview and gains experience over time in how to manage the cooperation in the best possible way. It also allows for appropriate supervision of data protection issues. For the private US counterpart, the use of a SPOC allows for smoother processing in that the law enforcement SPOC can provide the credentials necessary for requesting non-content data and receiving voluntarily disclosed information.

---

11 Following the judgment of the Court of Justice in Joint cases C-203/15 and C-698/15 rendered in December 2016, the evaluation team was informed that the Swedish Government has appointed a Public Inquiry with a view to review the legal provisions on data retention in the Act on Electronic Communications. The review shall take into full account the judgement of the Court of Justice in the joined cases C-203/15 and C-698/15. A report with proposal is expected at the latest on 9 October 2017.

12 A clarification of the differences between the two measures is made in the Assessment Report on the Implementation of the preservation provisions of the Budapest Convention on Cybercrime adopted by the T-CY at its 8th Plenary (5-6 December 2012), as well as in the Explanatory Report (149-162) of the Budapest Convention.

# 6 OPERATIONAL ASPECTS

## 6.1 Cyber attacks

### 6.1.1 Nature of cyber attacks

No statistics currently exist on the precise nature of the cyber attacks, but they tend to follow international trends: DDOS attacks, ID theft, CEO fraud (spearphishing) and Card-Not-Present-fraud cases are on the rise.

The Police obtain information from filed police reports. There are a lot of cyber attacks that are not reported or are reported to agencies other than the Police.

### 6.1.2 Mechanism for responding to cyber attacks

When assessing whether a crime is gross, the fact that the act has caused serious harm or covered a large amount of data or has otherwise been of a particularly dangerous nature is taken into account. The penalty for gross breaches of data secrecy (imprisonment for a minimum of six months and a maximum of six years) was adopted in 2014 in order to meet the requirements regarding penalties in Directive 2013/40/EU.

On 1 April 2016, a regulation for mandatory reporting of serious IT incidents affecting government agencies entered into force in Sweden. This will provide Swedish authorities with a better overview of the threats and with the opportunity to take the right precautions.

In line with EU legislation, telecom operators are obliged to report security breaches and data breaches to the national regulator of electronic communications. The reason behind the breaches (for example, a criminal cyber attack) is irrelevant in this regard. The procedures for this are established by EU secondary legislation. There is no obligation to report directly to law enforcement agencies.

The Swedish Civil Contingencies Agency has developed a National Response Plan for the handling of serious IT incidents. Two processes are key: creating situational awareness and working via a national cooperation mechanism. The mechanism rests on the principle of responsibility, which means that no involved actor assumes another actor´s responsibility when handling the incident. An important base for the mechanism is the national CERT. Both agencies and private corporations can take part in the mechanism.

It is the operator's responsibility to provide their own business with satisfactory protection. Operators also interact with other operators in their respective sectors to exchange information. Sector collaboration is established, e.g. in the telecom and financial sectors.

No or very little interest on the part of the victims is seen as an obstacle. This applies especially to private companies and even state agencies and authorities. Cybercrime should be reported and there should be cooperation with an investigation once started. Incidents are therefore underreported.

According to the Swedish authorities, there is a need for the Swedish Police to gain more experience of these types of crime.

## 6.2 Actions against child pornography and sexual abuse online

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

Software databases specifically designed to identify victims are used by Swedish Police e.g. Griffeye, ICSE and NetClean. The International Child Sexual Exploitation Database at Interpol is used on a daily basis.

The images in the database are only available for a limited number of personnel. Confiscated material is always destroyed.

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

Sextortion is in view of the Swedish authorities a problem that requires attention and against which counter measures must be taken.

Developments in society and technology have increased opportunities for communication and information dissemination and thus also the possibility of committing acts that involve threats and violations.

A Committee of Inquiry has recently conducted a broad review of the protection provided by criminal law for individual privacy, particularly with regard to threats and other violations. The committee proposes that criminal law protection of personal privacy should be strengthened and modernised, e.g. by introducing a new penalty provision on unlawful violation of privacy. The new provision will entail criminal liability in certain cases for those who violate someone else's privacy by spreading images or other information in a way that is intended to cause material harm to the person who is subject of the information. The proposals are currently being considered by the Government.

A Committee of Inquiry was appointed on 17 June 2014 to review the application of the provision on contact with a child for sexual purposes (sexual grooming) in Chapter 6, Section 10a of the Penal Code. The committee submitted its report to the government in October 2015. The report is now subject to consideration at the Ministry of Justice.

Furthermore, a government inquiry, "the 2014 Committee on Sexual Offences", is carrying out a review of the crime of rape. The review includes analysing whether penal law provides sufficiently strong protection against certain forms of sexual abuse committed via the internet. The evaluation team was informed that the Committee reported its findings on 1 October 2016.[13]

The Police co-operate with communities for children and young persons, in particular with popular sites and social forums for children in Sweden. When children and adolescents see or get information about sexual abuse or exploitation, they give us the information we need to initiate an investigation. The Police are also working to establish a "stop button" for children to press when they need or want to make a report about being contacted by adults for sexual purposes.



[13] It is to be reported that the evaluation team did not take its findings into account.

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

Since 2009, Sweden has had a dedicated team with nationwide responsibility for investigating child sex tourism. In order to detect and prevent child sex tourism, campaigns to raise public awareness have been launched, training for LEA officers and people in the travel business, etc., has been provided, and cooperation with foreign LEAs as well as domestic and foreign NGOs, including participation in joint actions and JIT's, has been developed.

On 22 June, the Government adopted a new Action Plan on protecting children from trafficking in human beings, sexual abuse and exploitation. The Action Plan incudes a series of measures that are relevant in the fight against child sex tourism, for instance actions involving the tourism and travel industry and the foreign service in order to improve detection.

Over the past few years, a series of successful investigations on live-streamed sexual exploitation has been carried out and has led to convictions for instigation of gross rape of a child. Cooperation has been established with the Financial Coalition and the internet- based payment providers in order to detect and stop the flow of money in these cases.

The Swedish Police cooperates with ECPAT and receives information from its hotline. The homepage of the Police makes it possible for a crime to be reported by a victim or a person having information about this type of crime. On the same page you can also read about the crimes, how to protect yourself and what to do if you or someone you know is exposed. In collaboration with NGOs, special information material directed at both children and their parents has been developed.

The Swedish Media Council is a government agency with the task of empowering children and youngsters to become conscious media-users and protect them from harmful media influences. The agency therefore produces educational material for use in the classroom or at home by teachers, librarians, parents and students. Some of this educational material has been translated into English, Somalian and Arabic for the immigrant population in Sweden. Some has also been published specifically for children with intellectual and mental disabilities.

Between 2013 and 2015 the Swedish Media Council implemented the Council of Europe's No Hate Speech Movement Campaign in order to prevent racism, sexism and other forms of hate online. Since 2015 the Campaign has been continued, but this time at the national level, with the added aspect of preventing violent extremism and propaganda online. Within the framework of this campaign the Media Council has produced educational material, podcasts and online material where online regulations and legal matters are explained by a legal expert. The Campaign also offers advice to youngsters and parents on how to deal with illegal and/or harmful content produced by others.

In September 2015, the Government also gave the National Agency for Education (NAE) the task of presenting proposals for national ICT strategies for the Swedish school system. The strategies are to contain goals and initiatives for strengthening the preconditions for equal access to ICT within the school system and enhancing the digital competence of teachers and students and the strategic competence of school leaders in the area of ICT.

The strategies are aimed at making sure that full advantage is taken of the potential that digitalisation has for school development and development of the tutoring. The proposals are to include work being carried in schools on preventing cyberbullying and promoting online integrity and security and the critical assessment of information.

The NAE was already in 2008 tasked with promoting the safe use of ICT in schools, including protection of personal integrity and a critical approach to digital and online information. As part of this task, the NAE has published online learning material and support for schools and teachers concerning these issues. It can be accessed here: www.skolverket.se/kollakallan.

### 6.2.4 Actors and measures counterfeiting websites containing or disseminating child pornography

There are rules that aim to prevent the spread of child pornography in the Act on Responsibility of Electronic Bulletin Boards (1998:112). Electronic bulletin boards (BBS) are defined as a service for mediation of electronic messages in the form of text, images, sound or other information. Those who provide BBS are obliged to supervise their content. The provider is also obliged to remove, or in some other way prevent, the dissemination of messages, if it is obvious that the content is child pornography. A person who deliberately, or by gross negligence, violates this obligation can be fined or sentenced to a maximum of six months imprisonment.

Furthermore, blocking of websites with a child pornographic content in Sweden is carried out in voluntary cooperation between the Police and the Internet Service Providers. 85-90 % of subscribers to the Internet in Sweden are covered by this voluntary cooperation.

The cooperation operates in the following way: the Police receive information on child pornographic websites via different channels such as Europol, Interpol, child rights organisations or the general public. Information is also collected by the Police in their daily work combating child pornography on the Internet.

The information is verified and then shared with the Internet Service Providers who make the technical arrangements for blocking at the level of the end user. This means that anyone trying to access the website in question instead will see a message (see annex) saying that this site is blocked due to its child pornographic content.

The formal borders of the EU are irrelevant as to whether an ISP in cooperation with the SE Police will block a website or not. In other words, websites with child pornographic content will be blocked and made inaccessible in Sweden regardless of whether the site is located within or outside the EU.

In the procedure to verify that the website contains child pornographic material, the Police also check the location of the website. In connection with the blocking and on that basis, information is sent to the appropriate judicial or law enforcement authority in the country where the website is located. This information informs the authority that a website located on its territory contains illegal material. However, no further steps are taken since it might interfere with, for instance, an ongoing investigation in that country.

The Swedish Cybercrime Centre has dedicated officers working exclusively with child sexual abuse material for the purpose of identifying children and perpetrators. The investigations are conducted in the police regions and, most often, by specially trained officers. Since 2006 about 300 officers have been trained in victim identification and about 500 educated and specially trained to deal with child investigations (the persons are not always the same and not all of them still work with CSE.)

Some regions, not yet all seven, have specialized units dealing exclusively with child sexual abuse material and investigations. However, centralised statistics on figures about the composition and size of the regional units do not exist.

## 6.3 Online card fraud

### 6.3.1 Online reporting

There is no online tool for reporting cybercrime offences to the Swedish Police. In nearly all cases the Police only get information from filed police reports. There are a lot of cyber attacks that are not reported or are just reported to agencies other than the Police. The Police are obliged to file a report when they become aware of a possible crime. Often, therefore, victims (e.g. CEOs, companies) hesitate to contact the Police in the case of cyber attacks, fearing further damage following unwanted publicity. To mitigate this underreporting, the National Fraud Centre has the possibility to put a case under embargo, thus not informing the Police.

Citizens usually report these cases to the Swedish Police since Swedish banks generally require a police report to compensate for the losses. Private companies tend to report less frequently. A possible reason could be that they estimate the time spent and the cost of reporting outweighs the prospects of success in their case.

Card-Not-Present-fraud (CNP) data: in the first six months of 2016, a total of 38,700 police reports were made regarding CNP. In 2015, 21,100 reports were registered during the same period.

Information regarding personal and financial data in Sweden is relatively open and available. The Police inform interested parties regularly that this is a problem and that legislative changes are needed to prevent the information from becoming available to criminals.

### 6.3.2 Role of private sector

The Swedish Police, banks, payment providers, petrol companies and logistics companies have been cooperating closely for many years. A new modus operandi is always shared by both sides.

The Swedish Police are involved and are working together with Swedish banks in the area of online card security and the vulnerability of the magnetic stripe.

The private sector is actively involved through various committees, discussion groups and fora in the pooling of efforts to fight cybercrime and raise awareness. For instance, the private sector worked together with the Swedish Contingencies Agency on developing educational tools for users in both public and private organisations.

## 6.4 Conclusions

- A National Response Plan for handling serious IT incidents has been developed by the Swedish Civil Contingencies Agency. Currently critical infrastructure entities in the private sector are not legally obliged to report cybercrime attacks to the police. However, this will change once the NIS Directive is implemented. Public authorities in Sweden are obliged to report cyberattacks, private entities are not.

- The authorities in Sweden have carried out a broad range of measures to tackle sexual abuse and sexual exploitation of children that include prevention and awareness campaigns, as well as legislative measures and the blocking of websites with illegal content. Such measures are aimed at educating the public, parents and children about the risks of harmful/illegal behaviour online.

- The strategies are aimed at making sure that full advantage is taken of the potential that digitalisation has for school development and development of tutoring. New proposals are under consideration to prevent cyberbullying and promote online integrity and security and the critical assessment of information.

- The Swedish Cybercrime Centre has dedicated officers working exclusively with child sexual abuse material for the purpose of identifying children and perpetrators, and some regions have specialized units dealing exclusively with child sexual abuse material and investigations.

- Over the past few years, a series of successful investigations on live-streamed sexual exploitation has been carried out and has led to convictions for instigation of gross rape of a child.

- The Police are working with ECPAT and the County Administration Board which have set up hotlines where the public can report all internet-related sexual abuse of children. The information is forwarded to the Police directly. The Police and ECPAT are also active partners in the Financial Coalition. The overall approach and the measures taken by Swedish authorities in this area represent good practice to be shared with other Member States.

- With regard to online card fraud, Swedish law enforcement closely cooperates with the banking sector (e.g. automated and standardized requests). In general, fraud is investigated locally and often investigators lack experience of cross-border investigations and cooperation.

- Cooperation has been established with the Financial Coalition and the internet-based payment providers in order to detect and stop the flow of money in these cases. However, this cooperation is on a voluntary basis and thus the scale of online fraud may not be sufficiently recognised by the Swedish authorities.

- In the evaluators' view cybercrime investigations involving proceeds need to be accompanied by financial investigations to search, seize and confiscate such proceeds. And vice versa, financial investigations involving offences against and by means of computers need to be accompanied by cybercrime investigations. In practice this means close cooperation between cybercrime units, financial investigation units and Financial Intelligence Units.

- Information regarding personal and financial data in Sweden is relatively open and available. The Police regularly inform interested parties that this is a problem. There may be a need for legislative changes to prevent the information from becoming available to criminals.

- The evaluators consider that there may be insufficient investigative resources, considering the large number of cases.

# 7 INTERNATIONAL COOPERATION

## 7.1 Cooperation with EU agencies

### 7.1.1 Formal requirements to cooperate with Europol/EC3, Eurojust, ENISA

The Prosecution Authority has cooperated with EU agencies on several occasions, e.g.:

- on Operation Onimous – Cooperation with Europol,/theEC3 and Eurojust. Crimes committed on darknet – Silk road;
- on Operation Black Shades – cooperation with e.g. the EC3 and Eurojust. Malware and fraud;
- on Operation Ateljé – co-operation with the help of Eurojust. Production of child pornography.

The Swedish Police have participated in numerous operations and some projects involving two or more Member States. In most cases Europol has provided support and coordination. Eurojust has been involved sometimes too. A good example of an operation is Onymous in November 2014. The aim of the operation was to shut down multiple marketplaces on the hidden network TOR. Related to this operation is the EU- financed project ITOM (Illegal Trade on Online Marketplaces). Sweden participated both strategically and operationally.

Another case example given by the police is the multinational operation Bygbyte/Shrouded Horizon where one of the largest criminal hacking forums was shut down and arrests, search warrants and seizures were executed at the same time in many countries all around the world. Cooperation led by the EC3 on banker trojans was also carried out, for example regarding Retafe and Dridex.

No such requirement or procedures are provided for concerning ENISA.

Concerning child sexual exploitation, the use of the ICSE database and requests for different kinds of information are frequent. The Swedish Police also attend all expert meetings.

Eurojust is also used for its relations with countries such as the US, Norway and Switzerland, which makes contact and cooperation easier. Moreover, the procedure whereby third countries are invited to cooperation meetings at the premises of Eurojust works well, according to the Prosecution Authority.

There are many third countries and agencies in house at Europol in The Hague, which has contributed in a good way to the cooperation. The third countries/parties are participating in different fora and working groups. Sweden has a good bilateral relations with many of these parties, but it becomes easier when they are represented at Europol.

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

Eurojust has played an important part in cases involving more than one MS on several occasions.

There is cooperation with ENISA and Europol.

ENISA can provide its technical expertise in the area of network and information security issues and collect and disseminate expertise from other sources. The added value is more on prevention and awareness raising than on mitigation or investigation. Its network of people with network and information security skills is an asset. No experience of cooperation with ENISA in cybercrime cases has been gathered.

Europol's work is based on Member State contributions in terms of data provided but also on steering directives when it comes to priorities. To obtain some good results from Europol, Sweden needs not only to contribute information from ongoing and closed investigations, intelligence cases, but also to give them clear and specific requests. The Swedish Police could utilise the expertise at the EC3 more than it does today.

As regards ENISA and Europol, the Swedish authorities are of the opinion that changing procedures or mandates would probably have limited impact. Adding more resources would probably have more impact, if there was a way of earmarking those resources for this purpose.

According to the Swedish authorities, participation in J-CAT from Sweden is absolutely necessary in order to work in a more structured, efficient and smoother way in cybercrime cases. Crime as such knows no frontiers and Sweden needs to play a more active part in work of the international community.

Moreover, the need was identified to send more staff in general to the EC3 where they could learn from international law enforcement and at the same time contribute to a joint, international effort, as well as promoting particular Swedish interests and the Swedish Police.

### 7.1.3 Operational performance of JITs and cyber patrols

Operation Ateljé concerned the production and procuring of child pornography. A JIT was established between three MS and several meetings were held. Eurojust arranged coordination meetings at which the JIT members and several other states participated. The cooperation between the JIT members worked very smoothly and the JIT played a big part in the success of the operation.

Since 2014, the Swedish Cybercrime Centre has been engaged in an EMPACT activity (Priority G Cyber attacks) which is aimed at establishing an internet patrol. This activity has evolved from an operative idea into a more theoretical one with a capacity- building purpose.

According to the Prosecution Authority a JIT is an excellent tool for facilitating cooperation between the MS; it is important that the possibility to apply and receive funds for the investigations continues.

### 7.2 Cooperation between the Swedish authorities and Interpol

The Swedish authorities reported that some operational information has been sent from Interpol, but not that much and it was not that relevant in their opinion. A few cases have been initiated and coordinated by them and the cases have all looked good from the beginning, but have also taken a long time and been too diffuse. To avoid misunderstandings and duplication, the practitioners met think that Sweden should strive to work in the international arena via Europol as far as it is possible. The connection to Interpol can be made through the Interpol liaison officer at Europol.

### 7.3 Cooperation with third states

When it comes to MLA, for instance, the underlying principle is that Swedish authorities assist foreign states as much as possible and with every measure that is available to the Swedish authorities in domestic investigations or proceedings.

Many times requests have been made to and been received from the US and Canada. The legal basis is bilateral agreements with the US and Canada respectively. These requests concern many different types of MLA and have had varying results.

In the case of both countries it usually takes a long time to receive answers.

### 7.4 Cooperation with private sector

NetClean or Griffeye are installed on computers at many private companies in order to detect employees´ use of child pornography.

Internet- based payment providers report suspicious activity to the police. There are no obligations, but the Police have in some cases asked for assistance from the private sector for information sharing and some other measures. Collaboration with the major banks enabling them to provide information and take action has been established. Some cases have been run in cooperation with CERT-SE and there is good cooperation with the private sector (for example, the Internet service providers).

Pursuant to Chapter 6, Sections 16a and 16d of the Electronic Communications Act (2003:389), Internet Service Providers (ISPs) are obliged to store traffic data and user information (such as names, addresses, phone numbers etc.) for six months. After six months the information must be deleted. In order to obtain traffic data for use in preliminary investigations, court permission is normally needed and certain requirements must be fulfilled. Where a crime is suspected, the ISP must give user information to the prosecution or police authority on request (Chapter 6, Section 22 (2) of the Electronic Communications Act). ISPs are also bound to secrecy when it comes to requests, etc., from law enforcement authorities. If an ISP does not comply with its obligations, the Swedish Post and Telecom Authority may issue an injunction. A website that contains child pornography is normally blocked voluntarily by the ISP after the Police have informed it of its content.

When the information is stored in a third state or the prosecutor needs investigative measures executed in a third State, the prosecutor will usually have to request MLA and go through the judicial authorities in that State. It is not always possible to go through a local branch in order to receive the information. For example, Facebook has servers in Sweden and a local branch. However, in order to get information from those servers, the prosecutor still needs to go through the headquarters in the US. When it is possible to have direct contact, it will usually go through the police.

Coercive measures against private companies in third states are always subject to MLA. Such measures have been carried out on numerous occasions. Coercive measures against private companies in Sweden is common, both when someone working at the company is suspected and when information is stored there.

However, on some occasions it has not been deemed possible since the amount of information is so enormous and it is impossible for an outsider to know where the information is stored and find it.

SC3 would welcome more resources allocated to improving co-operation with the private sector. After all, it is within privately owned and operated infrastructures that cybercrimes are committed and within which evidence and traces for investigation can be found.

In fighting child pornography on the Internet, the Police are working with ECPAT Sweden and in the financial and telecom sector with the Financial Coalition with the aim of stopping and tracing payments for such material.

On the subject of online card fraud, it has been noted that the Swedish Police, banks, payment providers, petrol companies and logistics companies have been cooperating closely for many years.

As regards cyberattacks, improving cooperation and coordination between all actors when it comes to protecting the information and communication infrastructure is also highlighted in the National Programme for the Internal Security Fund.

The Swedish Prosecution Authority does not have direct contacts with the private sector, e.g. the Internet service providers, financial institutes etc. These contacts are handled by the Police.

### 7.5 Tools of international cooperation

#### 7.5.1 Mutual Legal Assistance

The authority responsible for receiving requests for MLA in cybercrime investigations is the Swedish Prosecution Authority (SPA). The requests are usually handled by one of the International Public Prosecution Offices in Stockholm, Gothenburg and Malmoe. A prosecutor will make the decision on whether to execute the request. If the request cannot be executed, e.g. because the crime in question is of a political military nature, or compliance with the request would be contrary to fundamental Swedish judicial rights, the decision to deny legal assistance is made by the Government.

Requests from another MS can be sent directly to the International Public Prosecution Offices. Requests from outside the EU should be sent to the Ministry of Justice.

The prosecutor in charge of the preliminary investigation is also responsible for sending MLAs. The prosecutor will send the request directly to the competent judicial authority in the other Member States. The prosecutor will often use the EJN Atlas in order to establish the correct address. If the request is to be sent to a state outside the EU, it will be sent through the Ministry of Justice.

All incoming requests are entered in an SPA registration system (CÅBRA). This system makes it possible to follow the case from registration to the answer being sent to the requesting country. In addition, the International Public Prosecution Office in Stockholm (which is the Prosecution Office that handles most incoming requests for MLA) has created an even more improved and detailed system in which every MLA case is followed separately.

Incoming requests received by the International Public Prosecution Office in Stockholm are dealt with in an increasingly efficient manner, with most cases being processed within two months. Occasional delays in answering a request are not due to a lack of resources or prioritization, but rather to the time taken to collect information (e.g. bank information, encrypted servers), an inability to contact the relevant person, the complexity of the request, or the need to complement information from the requesting country.

Pursuant to Chapter 2, Section10 of the Swedish Act on International Legal Assistance in Criminal Matters, an incoming request for MLA must be handled urgently. In Chapter 2, Section 3 of the Internal Directives of the SPA (ÅFS 2007:12), the time taken to handle a request for MLA should not exceed two months.

If the MS sending the request states a reason for the request being especially urgent, an effort will be made to handle it as quickly as possible. The Swedish Act on International Legal Assistance in Criminal Matters states in Chapter 2, Section 10, that a request for mutual legal assistance must be executed promptly.

Statistics are collected from the registration system. There is no record of the international instrument under which a request for mutual legal assistance has been made in this system since international instruments are transposed into national law, i.e. the legal basis for making a request or responding to a request is national law, not the international instrument. Neither is it possible to obtain statistics on the type of cybercrime a request concerns. The total number of requests for mutual legal assistance sent from the Swedish Prosecution Authority during 2015 was 491. During the same period 836 requests were received.

All measures that can be taken for other crimes can also be taken for cybercrimes. However, certain types of assistance, e.g. wiretapping, may require a particular minimum punishment. The most common reason for MLA requests is IP address tracing.

When the authorities receive a request for MLA related to information in the cloud, the information has usually been traced to a server in Sweden. As long as that is the case, no serious problems with providing MLA regarding information in the cloud have been noticed.

Sometimes, however, the information on a server is gone by the time the request is received. If the information is gone, it is cumbersome to provide MLA - there is no legal basis for conducting a formal search in "the cloud". This constitutes a problem, especially since it is becoming increasingly common that for instance accounting services are provided as cloud services. At present the Economic Crime Authority is discussing with cloud service providers access to accounting kept in the cloud during criminal investigations.

Outgoing MLA requests are often difficult since it is often hard to identify where to send a request.

The Swedish Prosecution Authority makes use of MLA when possible. However, the process is often too slow.

### 7.5.2 Mutual recognition instruments

Statistics are collected from the registration system. There is no record of which international instrument has been used for international cooperation in this system. Neither is it possible to obtain statistics regarding whether a case of international cooperation concerned cybercrime. It may be noted that recognition of financial penalties is in practice more or less exclusively used for traffic offences.

### 7.5.3 Surrender/Extradition

An offence does not have to be on the EAW list to give rise to surrender. Other offences can also give rise to surrender (or extradition) provided that they are considered a crime in Sweden. When it comes to extradition, under Swedish law the offence also has to be punishable by a custodial sentence or a detention order for a maximum period of at least 12 months or, where a sentence has been passed or a detention order has been made, for sentences of at least four years. Most cybercrimes fulfil this requirement, except, for instance, minor cases of fraud.

Some Swedish cybercrimes fall within the scope of the EAW list but do not fulfil the requirement of being punishable by a custodial sentence of at least three years (for instance minor or normal cases of fraud or minor crimes related to child pornography). Severe or gross cases of fraud or child pornography also fulfil the three -year requirement.

Sweden has a multilateral agreement with Finland, Norway, Denmark and Iceland regarding the Nordic Arrest Warrant which is used instead of the agreement between the EU Member States, Iceland and Norway. This agreement is often used.

European and Nordic Arrest Warrants in relation to all types of crime are issued by a Public Prosecutor if it concerns prosecution. If it concerns the execution of a sentence, the arrest warrants were issued by the National Police Authority at the request of the Prison and Probation Service.
Following the Court of Justice of the EU judgment rendered in case C-452/16 *PHU, Poltorak*, the Prosecution Authority has been recently appointed to issue the arrest warrants in those cases.
Requests for extradition are issued by a public prosecutor or the Prison and Probation Service and channelled through the Ministry of Justice.

Incoming European and Nordic Arrest Warrants in relation to all types of crime are handled by a public prosecutor. A court will decide on the requests. Concerning Nordic Arrest Warrants, the prosecutor can decide on the request under certain circumstances. Requests for extradition are received by the Ministry of Justice and then forwarded to the Prosecution Authority for handling, but it is the Swedish Government that takes the decisions on requests for extradition.

European or Nordic Arrest Warrants can be sent directly between the competent authorities. SIS is also used. EJN and Eurojust can be used in order to find the right receiving authority.
Requests for extradition can be sent directly to the Ministry of Justice.

Statistics are collected from the registration system. In this system there is no record of the international instrument under which a request for surrender or extradition has been made. Neither is it possible to obtain statistics on the type of cybercrime a request concerns.

The total number of European Arrest Warrants issued by Swedish prosecutors during 2015 was 258. During the same period of time 142 European Arrest Warrants were received. The total number of Nordic Arrest Warrants issued by Swedish prosecutors during 2015 was 33. During the same period of time 47 Nordic Arrest Warrants were received. The total number of requests for extradition sent from Sweden during 2015 was 30. During the same period of time 21 requests for extradition were received.

There are no specific procedures or conditions that need to be fulfilled as regards requests related to cybercrime. Cybercrime-related requests for surrender or extradition are, like all requests for surrender or extradition, treated expeditiously. Provisional arrests are possible and such arrests are made in most cases. During 2015 the average time for the full surrender procedure under an EAW where the person consented to surrender was 13 days. The average time where the person did not consent was 35 days.

### 7.6 Conclusions

- Sweden cooperates closely with the EU agencies, especially Europol, the EC3, J-Cat and Eurojust. The Swedish judicial authorities often use the expertise and the possibilities provided by Eurojust, which is in matter of cybercrime often crucial. Sweden deems the cooperation with EU agencies both necessary and satisfactory with regard to combating cybercrime, even when cooperating with third states, where these agencies can act as intermediaries.

- Although cooperation with Interpol in the field of cybercrime was found to be satisfactory, the Swedish Police are much more active in the cooperative activities in the context of Europol.

- Sweden has a multilateral agreement with Finland, Norway, Denmark and Iceland regarding the Nordic Arrest Warrant which is used instead of the agreement between the EU Member States.

- Sweden cooperates with other countries on the basis of international or bilateral agreements (e.g. with the US or Canada). However, the practitioners met raised the need for greater Swedish involvement in cooperation in various international fora. Since crime knows no frontiers, the evaluators believe that Sweden needs to play a more active part in the work of the international community in order both to learn from other countries and to share experience with them.

- With regard to cooperation with ISPs and other countries, Sweden has established very good contacts with the most important stakeholders in the public and private sector, especially by having single point of contact for requests. This single point- of -contact system has been very fruitful so far, especially as regards building trust, gaining experience and constantly trying to improve the exchange of information or execution of requests. This system also brings added value with regard to expertise and being interlinked. An answer from Facebook currently takes – on average – two weeks.

- With respect to MLA, the underlying principle is that Swedish authorities assist foreign states as much as possible and with every measure that is available to them in domestic investigations or proceedings.

- Although the police have strong informal contacts with most US-based international private sector service providers, certain judicial requests have to go through official MLA channels. This often takes long time.

- Sweden has a single database for registration and follow-up of incoming MLA requests (SPA), significantly reducing the time taken to deal with them. In this system is possible to follow the case from registration to the answer being sent to the requesting country. In addition, the International Public Prosecution Office in Stockholm (which is the Prosecution Office that handles most incoming requests for MLA) has created an even more improved and detailed system in which every MLA case is followed up separately. This practical tool could be recommended as an example of best practice.

# 8 TRAINING, AWARENESS RAISING AND PREVENTION

## 8.1 Specific training

Judges

The Swedish Judicial Training Academy provides training for judges. There is no specific training directed towards issues on cybercrime. However, the Academy organises annual criminal law seminars on relevant topics.

Starting in 2010, the Judicial Training Academy offered a series of training sessions regarding cybercrime. It consisted of three different training sessions with a length of two days each. Thirteen judges participated in the first part in 2010 and twelve judges participated in the second part which was first offered in 2011. In 2012 the first and second part of the training sessions were offered again, but unfortunately the number of judges who applied to take part was too small and the training sessions were cancelled. The third part of the training session series was cancelled for the same reason. In addition, a two- day seminar for judges was organised in 2015 on the issue of cybercrime and IT.

The Academy also gives annual training programmes in technical evidence and IT forensics. On average 50-60 judges attend these criminal law seminars and training programmes every year. In 2016 the Academy planned to send judges to the EJTN seminar entitled “Linguistics seminar on the Vocabulary of Cybercrime” in Madrid.

Furthermore, the training programme for judges in training contains a training session regarding technical evidence which takes place at the Swedish National Forensic Centre in Linköping. This training session is similar to the one offered to permanent judges and was described in our earlier reply. During this training session, the participants are offered lectures and demonstrations by the experts working at the Swedish National Forensic Centre, including an expert in IT forensics. Apart from this training session, no special training regarding cybercrime is included in the programme for judges in training.

The Prosecution Authority

The Training Centre of the Swedish Prosecution Authority provides a cybercrime- related course in the mandatory initial training and in the further training for prosecutors.

During the initial training there is a total of 8 + 6 lessons which comprises specific cybercrime-related training. Examples of topics included are: basic structure of the Internet, coercive measures in an IT environment, IP tracing, sexual crimes on the Internet and child pornography.

In the further training, the IT- related crime course consists of a one- week training for 25 prosecutors that is offered twice a year. The subjects are: the structure of the Internet and different tracing techniques, coercive measures and digital evidence, legal instruments within the Code of Judicial Procedure, child pornography on the Internet, new methods of payment on the internet, and a study visit to the Police.

In autumn 2016 a new one -week course for experienced prosecutors was held in cooperation with the Swedish Police and this will continue once a year in the future. It focused on more complex cases and how to plan and execute investigations and the use of different coercive measures in the Internet environment.

The in-house web - based guide concerning cybercrime was launched in 2015. The guide is accessible for to all personnel within the Prosecution Authority. Due to the constant changes in the area, this guide will be continuously amended and updated – as has already been the case.

The Police

The Police provide training for prosecutors, judges and for LEA agents working with child pornography and also host an annual cybercrime conference for LEAs working in the field of cybercrime and victim identification. The number of participants increased from 200 to 300 between 2015 and 2016, a sign that human resources are in an upward trend.

The Swedish Police are setting up a new platform for education that also includes cybercrime investigators.

The Swedish National Forensic Laboratory and SC3 are working to develop training opportunities further. In the future, external actors such as universities are also to be involved.

The Swedish Police do not have figures specifically for cybercrime- related training readily available.

There have been some JIT courses in which personnel from SC3 have participated. CEPOL provides different types of training such as Webinar seminars (appr. 60-90 minutes) and ordinary training courses (5 days).

SC3 carries out "in-house" training for the seven police regions. The training platforms now under development by SC3 and the National Forensic Centre are intended to involve external actors from, e.g., academia in the future.

There are specially designed three-year college courses available in IT forensics and information security, for instance at the University of Halmstad and University of Skövde in the west, Blekinge Institute of Technology in the south and Luleå Technical University in the north.

## 8.2 Awareness raising

The Swedish Media Council has been tasked by the Government with analysing the role of the public sector, private actors and civil society in protecting children from online racism, sexism and extremism. The aim of this analysis is to see what more could be done by these actors to increase the protection of children against such harmful influences. The task goes on during 2016-2017.

The Swedish Media Council produces educational material for teachers and for school librarians to discuss with students inside or outside the classroom. Research conducted by the Media Council shows that children in Sweden start using the Internet when they are two years old. Therefore, the Council has started a partnership with antenatal clinics in Stockholm in order to inform parents of children 0-2 years old about children's behaviour online and how to supervise/protect them.

## 8.3 Prevention

### 8.3.1 National legislation/policy and other measures

On 22 June 2016, the Government adopted a new Action Plan to protect children from human trafficking, exploitation and sexual abuse. The Action Plan encompasses 23 measures including a series of important actions to protect children from crimes related to the Internet.

The Police

Joint actions are under way with ECPAT and the County Administration Board: information pamphlets have been produced, LEAs are given training, cooperation with NGOs is being developed, and targeted action is being aimed at the travel sector etc.

Information campaigns (awareness rising) aimed at the public is planned. Recently the campaign RESEKURAGE (Travel Courage) against child sex tourism, a cooperative venture on the part of the County Board, received an award.

A new prevention method has been initiated and incorporated into the work of the Cybercrime Intelligence Team. As a part of a preventive approach, the tactical intervention 'proactive talks' is supposed to be used against individuals (youngsters) at risk of committing cybercrimes in the future (there should be specific indicators, but not so serious or so many that the subject will be investigated or even charged).

The National Agency for Education (NAE)

The Swedish National Agency for Education (NAE) was in the summer of 2015 given the task of providing teachers, principals and education providers in compulsory and upper secondary education with extensive continuing professional development, so called national development programmes, in different areas. One of these designated areas is digital skills – to strengthen digital competence in tutoring. The task also includes providing support for schools in working with the fundamental values stated in the Education Act and in school curricula, e.g. gender equality and a norm -critical perspective in schools, as well as preventing bullying and harassment.

Human rights, in the form of fundamental democratic values, constitute the basis of the Swedish school system. In accordance with the Education Act (2010:800) and the national curricula, everyone working in school should without exception encourage respect for the intrinsic value of each person and the environment we all share.

Chapter 6 of the Education Act (2010:800) also contains regulations concerning active measures to prevent school bullying and makes schools responsible for investigating and taking appropriate measures against degrading treatment. This can include cyber bullying related to education in school.

The Swedish Schools Inspectorate scrutinises schools. The Child and School Student Representative is a part of the Schools Inspectorate and has supervision over the section of the Education Act that deals with degrading treatment.

### 8.3.2 Public Private Partnership (PPP)

Sweden uses Public Private Partnership (PPP) in the prevention of and fight against cybercrime. For instance, in fighting child pornography on the Internet, the Police are working with ECPAT Sweden and the financial and telecom sector in the Financial Coalition with the aim of stopping and tracing payments for such material. The Police are working with Internet Service Providers in the cooperative arrangement aimed at voluntary blocking described above.

The Swedish Police, banks, payment providers, petrol companies and logistic companies have been cooperating closely for many years (please refer to section 6.3.1).

As regards cyberattacks, the National Response Plan should be mentioned (please refer to section 6.1.2). Improving cooperation and coordination between all actors in protecting the information and communication infrastructure is also highlighted in the National Programme for the Internal Security Fund.

## 8.4 Conclusions

- Sweden has an elaborate training programme for prosecutors and police in the field of cybercrime, with a mandatory basic training for ordinary prosecutors and more advanced courses for specialised services. However, the judges seem to lack such a training, since only ad hoc or piecemeal sessions exist.

- It is to be noted in particular as best practice the way the training for prosecutors is organised, including the specialised network for prosecutors. The discussion revealed that often judges lack the necessary skills to adjudicate this type of crimes. Moreover, it turned out that other units within the police lack knowledge of cybercrime and electronic evidence although cybercrime was included in the basic training. Furthermore, the knowledge of judges and prosecutors could be enhanced by using IT experts more widely in pending cybercrime cases.

- In the opinion of the evaluators, training on cybercrime and electronic evidence is needed across the judiciary to ensure that the necessary criminal justice capabilities are there to collect, analyse and use electronic evidence not only in relation to crimes involving computers but also in relation to any crime. Since any offence may involve electronic evidence, more or less all law enforcement officers and judges need to be trained, not just a few.

- Sweden has a national plan on raising awareness and focuses especially on children, even from the age of two years old. The programme is well integrated and relies on the cooperation of a multitude of governmental institutions involving agencies and private actors.

- Further cooperation between the Ministry of Social Affairs, the Ministry of Culture and the municipalities was established to improve the work in schools. Sweden has currently no programme aiming at raising the awareness of elderly people. Sweden relies in this area on the private sector and its initiatives.

- With regard to prevention the Swedish Ministry of Culture has a programme aimed at raising the awareness of children, for example with podcasts, with Facebook projects to fight and prevent racism and hate speech. To this end close cooperation with ISPs was established. Also, close cooperation with the Baltic Countries was established to analyse and prevent the influence of Internet trolls aiming to influence public opinion with false information.

- In general Sweden has very advanced cooperation between the public sector and the private in the fight against and prevention of cybercrime.

# 9 FINAL REMARKS AND RECOMMENDATIONS

## 9.1. Suggestions from Sweden

The Swedish Prosecution Authority has had a large number of different cybercrime cases successfully investigated and prosecuted. For example, a number of serial online sex offenders have been prosecuted and convicted. In many of these cases there have been more than 50 plaintiffs. Today the Prosecution Authority has several experts in cybercrime with extended knowledge and experience in this field. However, cybercrime and questions related to that area are increasing. Hence, the prosecutors are working on improving education, expertise and experience among a larger number of prosecutors in order to enhance the capabilities in this area even further.

Sweden assesses that the Police have a low to moderate capacity. This is due to the lack of resources, capability, priorities and some legal framework issues. Insufficient investigative resources compared to the large number of cases was also mentioned as one of the obstacles to cross-border cooperation specifically regarding online card fraud.

Furthermore, improved external collaboration at the Swedish Cybercrime Centre is very important for preventing and investigating cybercrime. This needs to improve further and not only be carried out at a lower level (officer to officer).

However, Sweden believes certain of its policies to be considered best practices.
Specifically, the specialisation of prosecutors, police together with effective cooperation and the sharing of know-how between them and between the MS involved is the key to an effective process.

In order to build on the success factors available to law enforcement, the importance of the concept of "team work" is cannot be stressed enough. The likelihood of success increases just by having a coordinated effort between intelligence officers, investigators, prosecutors, a swat team and digital forensics specialists.

When it comes to strengthening prevention and combating cybercrime, cooperation is the most important and efficient tool for law enforcement bodies, in particular the Police, for fighting cybercrime properly. First and foremost, this is about taking a more active part of the work in the international community.

Sweden believes it should join the J-CAT and through this, and other channels, be able to really influence and learn from EU cybercrime law enforcement. This would also assist and simplify investigative and intelligence work in Sweden. Other relevant international fora, such as the NCFTA in the US where police officers from many countries (in Europe too) work together in the same building with private sector and other agencies, are also important

The Swedish Cybercrime Centre is expected to lead the way when it comes to cooperation in the fight against cybercrime and initiate and host different activities which relevant partners can join. There should be a structured way of working with private parties and other forms of cooperation. The Swedish Cybercrime Centre should also be open to letting private companies and other agencies sit in-house when there are joint cases ongoing.

### 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 Sweden was able to satisfactorily review the system in Sweden.

Sweden should follow up the recommendations given in this report 18 months after the evaluation and report on the progress to the Working Party on General Affairs, including Evaluations (GENVAL).

The evaluation team thought it appropriate to make a number of suggestions for the attention of the Swedish 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 Sweden

1. Sweden should finalise and adopt its National Cyber Security Strategy and include in it a chapter on cybercrime; (cf. 3.1 and 3.5)

2. Sweden should ensure at strategic level a coherent policy and adequate measures against cybercrime, such as: introducing an online reporting system for cybercrime, improving the institutional setup (e.g. strengthening high-tech crime or other specialised units at the local level), providing law enforcement and judicial training in cybercrime and electronic evidence, promoting public-private cooperation, taking measures to protect children online, in particular against online sexual exploitation, conducting financial investigations, as well as having frameworks and mechanisms for efficient international cooperation in cybercrime investigations; (cf. 3.2, 3.5 and 6.4)

3. Sweden should improve the collection of statistics on cybercrime in a more detailed, standardised and comprehensive way and the management of statistical data, both at the level of investigation and prosecution on the one hand, and convictions relating to cybercrime on the other. Such data would provide a complete picture to be considered for strategic purposes e.g. national and training strategies. The statistics collected should provide data for at least each offence requested to be criminalised under Directive 2013/40/EU; (cf. 3.3, 3.5 and 5.1.2)[14]

4. Sweden should consider strengthening the capacity and capability of the Swedish Police, e.g. overall structure, guidelines, resources and competence in the field of cybercrime and cyber-related crimes, with sufficient human resources to cope with the large number of cases; (cf. 4.3 and 4.5)

5. Sweden should strengthen at the central level the coordination between the various actors involved in fighting and preventing cybercrime; (cf. 4.4 and 4.5)

6. Sweden should ratify the Convention on Cybercrime as soon as possible and specifically implement Article 16 and Article 29 (expedited preservation), as well as Articles 17 and 30 on expedited preservation and partial disclosure respectively; (cf. 5.1 and 5.5)

7. Sweden should ensure that the procedural law is adapted to modern technology, inter alia as regards access to evidence stored in the cloud and the obtaining of subscriber information in an expedited manner; (cf. 5.2.1, 5.2.3, 5.4.3 and 5.5)

8. Sweden should consider playing a more active part in the work of the international community, both to learn from and share experience with other countries and to improve the capacity for cross-border investigations and cooperation; (cf. 7.6 and 9.1)



[14] After the on-site visit the evaluation team was informed that the Council on Crime Prevention is in progress of analysing the solution regarding the need to collect comprehensive and overall statistical data on cyber-related crime. The Council has proposed that the nation-wide system for follow-up is established for it-forensic activities within the Police.

9. Sweden should provide training in the investigation of fraud and electronic evidence by giving the criminal justice system the capabilities necessary to collect, analyse and use electronic evidence, not only in relation to crimes involving computers but also in relation to any crime; (cf. 8.1 and 8.4)

10. Sweden should set up a comprehensive and structural training system for judges and prosecutors and expand training opportunities for police officers. Consideration should also be given to enhancing the scope for using IT experts more widely to improve the knowledge of the judiciary in cybercrime cases; (cf. 8.1 and 8.4)

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

1. Member States should consider setting up a comprehensive and structural training system with regard to cybercrime for prosecutors, like the Swedish system for training prosecutors and the web-based guide for prosecutors; (cf. 4.1.2 and 4.5)

2. Member States are recommended to develop or strengthen effective cooperation between police and prosecutors in the fight against cybercrime, along Swedish lines; (cf. 4.1.2 and 4.5)

3. Member States are recommended to use public-private partnerships to combat child abuse and child pornography online by developing tools to block illegal content on the Internet, as is the case in Sweden; (6.2.4 and 6.4)

4. Member States are recommended to strengthen the effectiveness of the communication process with other Member States and third countries by establishing an MLA registration system and an MLA management system making it possible to follow a case from registration to the answer being sent to the requesting country, as with the SPA in Sweden; (cf. 7.5.1 and 7.6)

5. Member States are recommended to enhance their cooperation with neighbouring countries to strengthen their policy of fighting cybercrime, following the model of Swedish cooperation with other Nordic countries as well as with Latvia, Lithuania and Estonia; (cf. 7.5.3 and 7.6)

6. Member States are recommended to develop campaigns aimed at raising the awareness of parents and children with regard to the safe use of the Internet, as the Swedish Media Council has done; (cf. 8.2 and 8.4)

7. EU institutions should address the issue of data retention as soon as possible; (cf. 5.5)

8. The EU should consider a common European approach on cross-border access to electronic evidence, including on agreements with big private companies to facilitate cooperation in criminal matters (e.g. Facebook, or Google); (cf. 7.5.1 and 7.6)

### 9.2.3 Recommendations to Eurojust/Europol/ENISA

1. Eurojust, Europol and ENISA should, where relevant, ensure and increase awareness of their capacity to support cybercrime investigations at national level and in particular in relation to cross-border cooperation; (cf.7.1.1 and 7.1.2).

## ANNEX A: PROGRAMME FOR THE ON-SITE VISIT AND PERSONS INTERVIEWED/MET

**Tuesday 27 September**

| | |
|---|---|
| 09:30-12:00 | Ministry of Justice |
| *Location:* | *Government Offices, Jakobsgatan 24, Kajutan, floor 7* |
| 12:30-13:30 | Lunch at the Government Offices |
| *Location:* | *Government Offices, Rosenbad* |
| 13:45-16:30 | The Swedish Prosecution Authority and the Swedish Economic Crime Authority |
| *Location:* | *Government Offices, Jakobsgatan 24, Cittran, ground floor* |
| 18:30 | Dinner at Brasserie Godot |
| *Location:* | *Grev Turegatan 36* |

**Wednesday 28 September**

| | |
|---|---|
| 10:00-16:00 | Swedish Police Authority |
| *Location:* | *Polhemsgatan 30* |
| 12:00-13:00 | Lunch at the Swedish Police |

**Thursday 29 September**

10.00-12:00 Swedish Civil Contingencies Agency

*Location:* *Fleminggatan 14*

12:00-13:00 Lunch at the Swedish Civil Contingencies Agency

**Friday 30 September**

10.00-12:15 Round-up and further questions

*Location:* *Government Offices, Jakobsgatan 24, Kajutan, floor 7*

Including participation in part by Secretary-General of ECPAT Sweden, Mr Anders Pettersson

12:30- Lunch at the Government Offices

*Location:* *Government Offices, Rosenbad*

## ANNEX B: PERSONS INTERVIEWED/MET

**Meetings 27 September 2016**

*Venue: The Ministry of Justice*

| Person interviewed/met | Organisation represented |
|---|---|
| Mr Nils Hänninger | Director, Ministry of Justice |
| Mr Henrik Sjölinder | Deputy Director, Ministry of Justice |
| Mr Mikael Kullberg | Deputy Director, Ministry of Justice |
| Mr Jonas Brunberg | Legal Adviser, Ministry of Justice |
| Mr Emil Karlsson | Legal Adviser, Ministry of Justice |
| Ms Jenny Engvall | Legal Adviser, Ministry of Justice |
| Ms Homa Abdolrasouli | Administrator, Ministry of Culture |
| Ms Julia Berglund | Administrator, the Swedish Police Authority |

*Venue: The Swedish Prosecution Authority*

| Person interviewed/met | Organisation represented |
|---|---|
| Mr Jan Tibbling | Vice Chief Prosecutor, Economic Crimes Authority |
| Mr Christer Dahlström | Prosecutor, Economic Crimes Authority |
| Mr Per Hedvall | Head of Bureau, The Prosecution Authority |
| Mr Niklas Lagrell | Head of Training, The Prosecution Authority |
| Mr Henrik Olin | Vice Chief Prosecutor |
| Ms Ingmarie Olsson | Specialist Prosecutor |
| Ms Cathrine Rudström | Specialist Prosecutor |

**Meetings 28 September 2016**

*Venue: The Swedish Police Authority*

| Person interviewed/met | Organisation represented |
|---|---|
| Mr Richard Ahlgren | Head, Cyber Crime Intelligence Unit |
| Mr Tommy Nordström | Head, High-Tech Unit |
| Mr Lena Larsson | Head, Cyber Crime Investigation Unit |
| Mr Per-Åke Wecksell | Desk officer Child Sex Exploitation online |
| Ms Bo Norgren | Desk officer, Desk Unit |
| Mr Jörgen Härberg | Head, Desk Unit |
| Ms Julia Berglund | Administrator |

**Meetings 29 September 2016**

*Venue: Swedish Civil Contingencies Agency*

| Person interviewed/met | Organisation represented |
|---|---|
| Ms Linda Ericson | Head of Strategic Support and Analysis Section |
| Ms Anne-Marie Alverås | Head of Section (cert.se). |
| Mr Christoffer Karsberg | Head of Section |

**Meetings 30 September 2016**

*Venue: The Ministry of Justice*

| Person interviewed/met | Organisation represented |
|---|---|
| Mr Henrik Sjölinder | Deputy Director, Ministry of Justice |
| Mr Anders Pettersson | Secretary General of ECPAT Sweden |
| Mr Mikael Kullberg | Deputy Director, Ministry of Justice |
| Mr Jonas Brunberg | Legal Adviser, Ministry of Justice |
| Mr Emil Karlsson | Legal Adviser, Ministry of Justice |

## ANNEX C: LIST OF ABBREVIATIONS/GLOSSARY OF TERMS

| LIST OF ACRONYMS, ABBREVIATIONS AND TERMS | SWEDISH OR ACRONYM IN ORIGINAL LANGUAGE | SWEDISH OR ACRONYM IN ORIGINAL LANGUAGE | ENGLISH |
|---|---|---|---|
| | | | |
| Brå | *Brå* | | The Swedish National Council for Crime Prevention |
| ECPAT | *ECPAT* | | End Child Prostitution in Asian Tourism |
| IOC's | *IOC's* | | Indicators of Compromise |
| MSB | *MSB* | | The Civil Contingencies Agency of Sweden |
| NAE | *SV* | | The National Agency for Education |
| NFC | *NBC* | | The National Fraud Centre |
| SC3 | *SC3* | | The Swedish Cybercrime Centre |
| SPA | *ÅM* | | The Swedish Prosecution Authority |