Council of the
European Union

Brussels, 8 June 2017
(OR. en)

13204/1/16
REV 1 DCL 1

GENVAL 104
CYBER 113

DECLASSIFICATION

of document:	13204/1/16 REV 1
dated:	9 December 2016
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" - Report on Denmark

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

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

Council of the
European Union

Brussels, 9 December 2016
(OR. en)

13204/1/16
REV 1

RESTREINT UE/EU RESTRICTED

GENVAL 104
CYBER 113

REPORT

Subject:	Evaluation report on the seventh round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating cybercrime" - Report on Denmark

ANNEX

Table of Contents

1 EXECUTIVE SUMMARY

- The evaluation team has been able to assess the general capability of Denmark to prevent, investigate and prosecute cybercrime as high, although there is, on the one hand, room for improvement in some areas and there are, on the other, unanswered questions about the way the Judiciary (Courts) are involved in the fight against cybercrime.

- The general atmosphere of work within the competent entities was casual but yet very efficient. The Danish Administration commits itself to continuous improvement via a long-term approach to work that seeks to achieve small, incremental changes in processes in order to improve efficiency and quality, and regularly review progress ("Lean approach").

- From 2014 Denmark showed a strong political will to better tackle cyber issues and appropriate budgets were allocated. The on-site visit made clear that budgets allocated for both prevention and the fight against cybercrime and cybersecurity were well spent and may benefit the national economy to a large degree.

- There is a solid alignment of response between the Danish Centre for Cybersecurity, the intelligence services and the police, together with other national structures set up to respond to critical incidents. Roles are clear and relevant information is shared.

- The National Cyber Crime Centre (NC3) has overall responsibility for the prevention, disruption and investigation of cybercrime and cybercrime-related offences in Denmark. It performs forensics, analysis and provides other kinds of investigative assistance to local police. NC3 employs highly skilled police investigators, IT forensic examiners and IT specialists. NC3 has been operating since 2014 and significant progress has been made in a short time-frame.

- The pairing of the National Police and the Public Prosecution Service, both serving under the authority of the Ministry of Justice, is one specific feature of the Danish legal system. In practice this results in genuine cooperation between police officers and prosecutors, and significantly facilitates successful prosecution.

- Although the evaluation team detected room for improvement in the national case management system, as that is reflected in the recommendations to Denmark, the team appreciated the fact that the CMS is common to Police and Prosecution services.

- In coordination with relevant stakeholders including those involved in the defence of fundamental rights, Denmark is currently reforming its Internet traffic data retention rules; in this respect it was opted to give preference to the setting up of an insightful, sophisticated Internet data retention model viable for as long as possible, rather than a quicker but short-term solution. National authorities are, however, recommended to swiftly adopt and implement the forthcoming law.

- The contribution of Denmark to Europol/EC3 activities is substantive. The fact that Denmark will no longer be an Europol member as a consequence of the Danish referendum of 3 December 2015 will result in a damaging loss for both parties.

- The national member of Eurojust is well known to local practitioners both amongst Police and Prosecution. It is considered easy for local practitioners to contact Eurojust and to receive the necessary assistance. Denmark is beginning with JITs and should be encouraged in this direction.

- The role of the private sector is reflected in several ways in cyber cooperation:
  - Major companies and government agencies may subscribe to a service provided by the Danish Centre for Cybersecurity to protect them against the top 10% of threats which cannot be adequately covered by private sector internet security providers;
  - NC3 cooperates actively between police and the financial sector;
  - Further cooperation between police and the private sector (confidential exchange of information among members and training of infrastructure stakeholders) is covered by the NC3 *Skyt* programme.

- Training was a recurring positive issue arising from the evaluation. A major programme to upgrade the cyber skills of the police and prosecutors was referred to on all days at all levels. Basic training for prosecutors and front line police staff is mandatory and carried out with e-learning modules. There are two further levels: "Advanced" consisting of a mixture of e-learning and tuition and "Expert" consisting of the development of key skills in an international setting.

2 INTRODUCTION

Following the adoption of Joint Action 97/827/JHA of 5 December 1997[1], a mechanism for evaluating the application and implementation at national level of international undertakings in the fight against organised crime was established. In line with Article 2 of the Joint Action, the Working Party on General Matters including 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 policies on prevention and combating cybercrime.

The choice of cybercrime as the subject for the seventh Mutual Evaluation round was welcomed by Member States. However, due to the broad range of offences which are covered by the term cybercrime, it was agreed that the evaluation would focus on those offences which Member States felt warranted particular attention. To this end, the evaluation covers three specific areas: cyber attacks, child sexual abuse/pornography online and online card fraud and should provide a comprehensive examination of the legal and operational aspects of tackling cybercrime, cross-border cooperation and cooperation with relevant EU agencies. Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography[2] (transposition date 18 December 2013), and Directive 2013/40/EU[3] on attacks against information systems (transposition date 4 September 2015), are particularly relevant in this context.

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

Moreover, the Council Conclusions on the EU Cybersecurity Strategy of June 2013[4] reiterate the objective of ratification of the Council of Europe Convention on Cybercrime (the Budapest Convention)[5] of 23 November 2001 as soon as possible and emphasise in their preamble that "the EU does not call for the creation of new international legal instruments for cyber issues". This Convention is supplemented by a Protocol on Xenophobia and Racism committed through computer systems[6].

Experience from past evaluations shows that Member States will be in different positions regarding implementation of relevant legal instruments, and the current process of evaluation could provide useful input also to Member States that may not have implemented all aspects of the various instruments. Nonetheless, the evaluation aims to be broad and interdisciplinary and not focus on implementation of various instruments relating to fighting cybercrime only but rather on the operational aspects in the Member States.

Therefore, apart from cooperation with prosecution services, this will also encompass how police authorities cooperate with Eurojust, ENISA and Europol/EC3 and how feedback from the given actors is channelled to the appropriate police and social services. The evaluation focuses on implementing national policies with regard to the suppression of cyber attacks and fraud as well as of child pornography. The evaluation also covers operational practices in the Member States with regard to international cooperation and the support offered to persons who fall victim to cyber crime.

4 12109/13 POLGEN 138 JAI 612 TELECOM 194 PROCIV 88 CSC 69 CIS 14 RELEX 633 JAIEX 55 RECH 338 COMPET 554 IND 204 COTER 85 ENFOPOL 232 DROIPEN 87 CYBER 15 COPS 276 POLMIL 39 COSI 93 DATAPROTECT 94.

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

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

The order of visits to the Member States was adopted by GENVAL on 1 April 2014. Denmark was the 21th Member State to be evaluated during this round of evaluations. In accordance with Article 3 of the Joint Action, a list of experts in the evaluations to be carried out has been drawn up by the Presidency. Member States have nominated experts with substantial practical knowledge in the field pursuant to a written request on 28 January 2014 to delegations made by the Chairman of GENVAL.

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

The experts charged with undertaking the evaluation of Denmark were Mr Gert SEIDL (Austria), Mr Michael GUBBINS (Ireland) and Mr Timothy ZAMMIT (Malta). Mr ZAMMIT declined participation to the on-site visit and did not contribute to the evaluation report. Two observers were present: Mr Reinhard SANTELER (Eurojust), and Mr Tom ROBSON (Europol/EC3), together with Ms Monika KOPCHEVA and Ms Claire ROCHETEAU from the General Secretariat of the Council.

This report was prepared by the expert team with the assistance of the General Secretariat of the Council, based on findings arising from the evaluation visit that took place in Denmark between 15 and 18 March 2016, and on Denmark's detailed replies to the evaluation questionnaire, together with its detailed answers to the ensuing follow-up questions.

3 GENERAL MATTERS AND STRUCTURES

3.1 National cyber security strategy

In December 2014, the Danish Government presented a National Cyber and Information Security Strategy containing a broad range of Government initiatives for 2015-2016. The Danish Government has aimed to strengthen protection against cyber attacks while respecting personal freedom and the rule of law.

The strategy consists of 6 strategic focus areas to be targeted with 27 specific initiatives. Some of the strategic focus areas as regards fighting cyber crime and strengthening cyber security are highlighted below.

The following specific initiatives have been initiated in order to strengthen cyber crime investigations:
- Expansion of the National Cyber Crime Centre (NC3) under the Danish National Police,
- strengthening the cyber capacity and capability of the Danish Security and Intelligence Service (PET),
- establishment of an online platform for reporting cyber crime and
- conducting a study regarding a service providing information on stolen identity documents.

The following specific initiatives have been initiated in order to strengthen cyber security:
- Formation of a cyber threat assessment unit in the Centre for Cyber Security (CFCS) under the Ministry of Defence;
- formation of a unit to investigate major cyber security incidents in the CFCS;
- formation of a SCADA knowledge entity in the CFCS, mandatory inclusion of cyber threats in government institutions' risk management and
- conducting a study regarding the possible concentration of government internet connections.

Link to a presentation of the National Cyber and Information Security Strategy (*In English*):
http://www.fmn.dk/eng/news/Documents/Danish-Cyber-and-Information-Security-Strategy-ENvers.PDF
Link to the National Cyber and Information Security Strategy (*In Danish*): http://www.fmn.dk/nyheder/Documents/National-strategi-for-cyber-og-informationssikkerhed.pdf.

3.2 National priorities with regard to cybercrime

The Danish National Police have adopted an overall strategy for 2016-2020 which both national and local police must adhere to in their work. One of the main targets of the Strategy is to prevent and combat cybercrime.

The Strategy 2016-2020 is complemented by a vision and five strategic objectives for the work carried out by the National Cyber Crime Centre (NC3) under the Danish National Police. The vision is that Denmark is among the ablest countries in the interaction between society and police in the matter of preventing and combating cybercrime. The five strategic objectives cover "the citizen as centre of the effort", "strengthening of the entire Danish police", "collaboration", "quality and competence" and "research-based innovation".

Moreover, in January 2016 NC3 initiated a strategy to work on preventing and combating cybercrime. The strategic work will, in view of the new training programmes , new technology platforms and general strengthening of competencies and capacities, set the direction for the efforts of NC3, and of the police districts, in preventing, disrupting and combating cyber crime, with a focus on how the cases are best handled.

3.3 Statistics on cybercrime

3.3.1 Main trends leading to cybercrime

The Danish National Police have observed an increase in cases regarding computer-related fraud and forgery. Recent figures from a financial infrastructure provider show a significant increase in the abuse of payment cards in relation to online trade. Fraud in relation to online trade between private individuals also shows signs of increasing, although some of the increase may also be due to the growth in the use of online platforms for trading.

During 2015 there have been several ransomware attacks targeting both public institutions, private companies and individual citizens, while from 2014 to 2015 there has been a decrease in the number of cases reported to the police on illegal access to information systems and illegal system interference.

The Danish authorities said, however, that only a small number of the incidents experienced by companies and private persons are reported to the law enforcement authorities (LEA) and with external reports on increased vulnerabilities of systems and Internet of Things (IOT) the decline in the number of reports to the LEA is not viewed as indicative of a general decrease in this type of crime.

Social media platforms play an increasing role as the "setting for" criminal acts, ranging from cases on fraud to cases of unlawful distribution of images and indecent exposure.

In relation to child sexual abuse online, the Danish Police have in recent years processed the first cases of live streaming of abuse. Based on reports from abroad, this type of case is expected to increase in number.

In the Danish statistical system, it is not possible to quantify cybercrime, as opposed to the total crime picture, as cases involving the use of Information and Communications Technology (ICT) are in many instances not recorded separately from cases that do not involve this modus operandi.

3.3.2 Number of registered cases of cyber criminality

As mentioned above, cybercrime cases are in some instances not separated from other cases in the Danish crime statistics as it is a *modus operandi* that cuts across several crime areas. **It is therefore a challenge to draw one national cybercrime figure**.

National statistics on cybercrime published by the Danish National Police are based on police data and are focused on the crime areas that are known to be distinctively related to ICT use. Elaborations on trends in cybercrime compiled by the Danish National Police are, however, based on available statistics and analysis from the private sector and other public sectors institutions.

Statistics provided to the team (see below) were not extensive and were received piecemeal on request during the on-site visit. This was at least partly attributed to an ageing case management system which was not fully fit for purpose. This factor cropped up on each day of the evaluation in reference to different agencies.

N.B. The table below of all cybercrime cases that reach the police is not exhaustive.
Police statistics are primarily structured in accordance with the Penal Code and, as in many Member States, there will be more cases that qualify as cybercrime than are depicted in the official figures. Some instances of attempted grooming may, for example, be registered as indecent exposure while the statistics on indecent exposure also include cases that are not relevant to cybercrime.

Table - Recorded cases, charges and indictments 2014-2015

	2014	2015	2014	2015	2014	2015
	Registered cases		Charges		Indictments	
Distribution of child pornography	71	110	72	118	41	103
Possession of child pornography	106	122	106	127	75	128
Illegitimate access to data information	180	133	110	173	141	75
Illegitimate access to corporate secrets	11	3	19	7	2	1
Illegitimate use of codes for information systems	60	16	8	14	1	17
Data fraud	5628	15399	4992	10808	6770	10109

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

In all areas visited, the budget provided for setting up and operation of the structures to fight cybercrime seemed to be adequate for preventing and combating that phenomenon. In particular, the renewed National Cyber Crime Centre (NC3) under the Danish National Police has dedicated resources at a comfortable level compared to a similar average-sized entity in a Member State.

Denmark benefits from EU funding regarding joint projects with other Member States, e.g. the British KIRAT project on sexual child abuse, but not to tackle specific Danish cybercrime projects.

3.5 Conclusions

- **Denmark would appear to have a strong cyber security strategy in place which is supported at a governmental level;**

- **The Centre for Cyber Security in charge of the cybersecurity of main critical infrastructures has a CERT function that generates responses to cyber-attacks; this Centre is well structured and has demonstrated that it is quite strategic and proactive in its ongoing activities;**

- **There is a specific Cybercrime strategy within Denmark, with all stakeholders well aware of their own area of responsibility;**

- **In the recent years the Danish authorities have allocated substantial funds for the setting up or renewal of structures and tools to better tackle cyber security and cybercrime issues. The evaluation team appreciated this and encourages Denmark to continue to dedicate sufficient resources to keep up with the rapid development of both information technology and its criminal misuse;**

- **Statistics have been provided by Denmark. However, in common with other Member States' recording systems, the police/prosecution recording system would have to be modernised to take better account of the cyber dimension of crimes and its evolution;**

- **As in many Member States LEA, statistics are kept separately from Court statistics; the latter have not been provided to the evaluation team; however, a number of sample court outcomes were provided; Danish authorities qualified the level of sentencing in cybercrime cases as "consistent";**

4 NATIONAL STRUCTURES

4.1 Judiciary (prosecution and courts)

4.1.1 Internal structure

Under Danish law, the Police are in charge of performing criminal investigations. The role of the prosecution is to supervise the investigations and ensure the legality of the investigations. At the local level, there is usually – due to the integrated structure – close cooperation between Police and Prosecution during the investigations.

It is the opinion of the evaluation team that the pairing of the police and prosecution appears to be an overall reflection of the management policy in the fight against crime. Danish practitioners said cases with a chance of producing a positive result were prioritised. The team was also told that the potential for any procedural errors in investigations is minimised, due to the close working relationship with prosecutors and their early involvement in the proceedings. In general, this can be viewed as a best practice model.

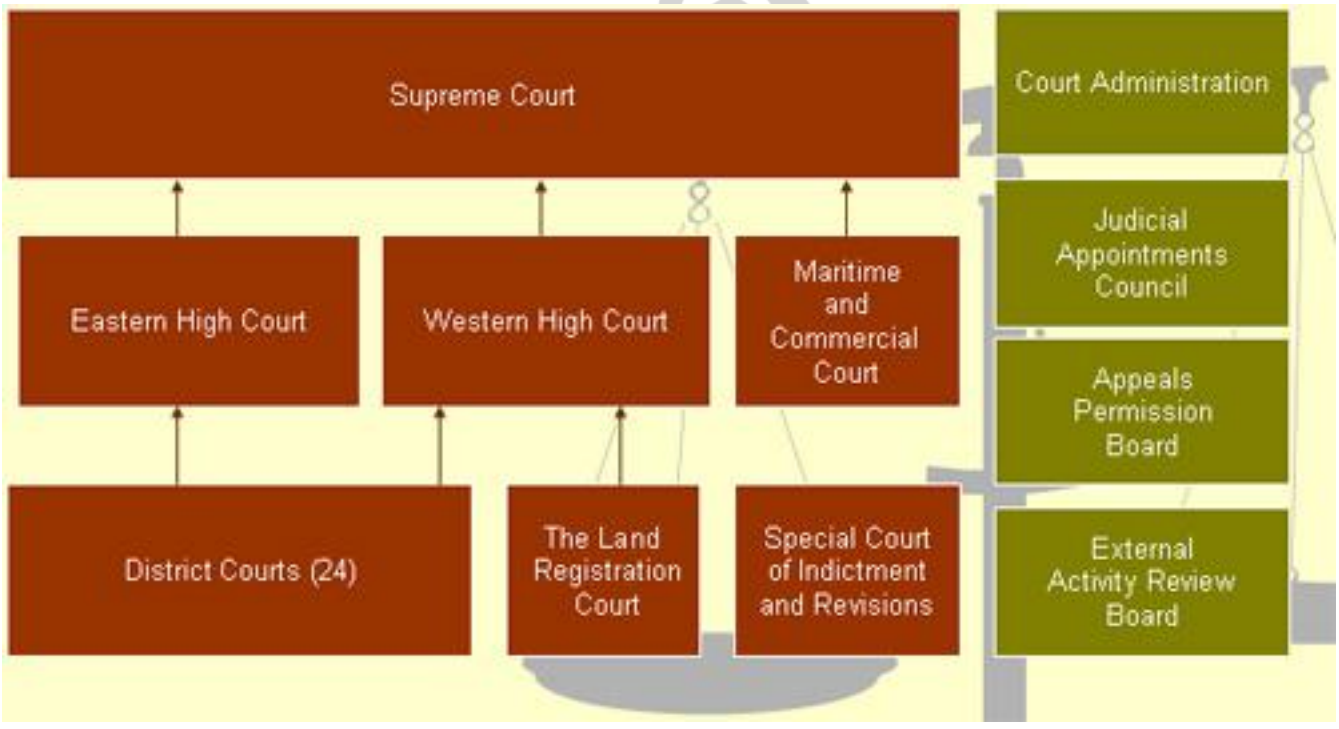
Any investigative steps requiring a court order (coercive measures) need to be decided by the prosecutor who presents the request to the court. Following the investigative phase of the case, the prosecutor assesses the evidence and decides whether or not to prosecute. The prosecutor then presents the case to the court during trial.

Cases of cybercrime are investigated in 12 local Police and Prosecution Districts. An exception is cases of violation of IPR rights which may be investigated and prosecuted by the State Prosecutor for Serious Economic and International Crime - who has national jurisdiction.

Cyber attacks. The Danish National Police are also responsible for investigating cyber attacks in order to apprehend and prosecute the perpetrators behind the cyber attacks. In December 2012 **Centre for Cyber Security (CFCS)** was established as a sector in the Danish Defence Intelligence Service (DDIS).

One of the responsibilities of the Centre for Cyber Security (CFCS) is to use its expertise to conduct IT security technical analysis of advanced cyber attacks in order to mitigate the cyber attacks and clarify the method of attack. The Danish National Police/Danish Security and Intelligence Service (PET) and the Centre for Cyber Security (CFCS)/ Danish Defence Intelligence Service (DDIS) cooperate closely, which involves the mutual exchange of information in relation to cyber attacks as well as operational cooperation in connection with specific cyber attacks.

Neither the Danish replies to the GENVAL questionnaire, nor the on-site visit provided the evaluation team with substantial information about the Judiciary. There are no judges specialising in cybercrime. The Judiciary is organised as follows.



4.1.2 Capacity and obstacles for successful prosecution

The National Cyber Crime Centre (NC3) was established (on the basis of two previous entities) under the Danish National Police in 2014. NC3 increases and strengthens the work of the district police on investigative, preventive and research areas related to cybercrime in terms of enhanced qualifications and greater capacity, as well as considerable investments in technology. The NC3 employs approximately 100 persons, including specialised police investigators, IT professionals, analysts, lawyers etc.

IT engineers have also been assigned to the local police districts.

The Prosecution Service. Most simple cases of cybercrime are handled by generalists in the Prosecution Service. However, the Director of Public Prosecutions (DPP) in 2014 decided to enhance the skills of the prosecutors at three levels.

- All prosecutors should be able to handle simple or more common cybercrime cases, e.g. computer-related fraud or forgery.
- In all prosecution offices, cybercrime specialists have been appointed. The specialists should be able to handle larger and more complicated cybercrime cases.
- At national level, four cybercrime experts have been appointed. These experts should be able to handle the most comprehensive and complicated cybercrime cases. They are also involved in training, gathering information and distributing it.

Enhancement of competences and skills in prosecuting cases of cyber crime is implemented through the issuing of standards, guidelines, through training and through the setting up of networks.

The Prosecution Service offers two training courses on cybercrime; Cybercrime I and II.

- The course *"Cybercrime I"* consists of e-learning and is aimed at all prosecutors. Currently, four modules are available online and in spring 2016 more modules will be available. The training course was designed in cooperation with the Danish National Police.
- The course *"Cybercrime II*" is aimed at specialists/experts and is a four-day training course focusing on the national and international legislation and regulations and on technical aspects.

The Director of Public Prosecutions has issued guidelines for the Prosecution Service on cases concerning child pornography etc. and also guidelines covering the entire cybercrime area.

- Guidelines on child pornography
- Guidelines on cybercrime
- Description of the training courses; Cybercrime I and II (page 38 and 41 in catalogue)
- E-learning module: “Offences, prosecution and jurisdiction” (screen prints)
- Letter from the DPP dated December 17th, 2014

A best practice standard on computer-related fraud or forgery is being prepared.
The documents are for internal use only in the Police and the Prosecution Service.

The DPP assesses that the main obstacles regarding the investigation and prosecution of cybercrime are:

- The difficulty in providing an overview of many small offences committed e.g. via the Internet (organised petty crime)
- The technical complexity of many cybercrime cases.

The on-site visit made rather clear that the current structure of the national case management system would have to be reviewed to make it more efficient. Updating case management systems is probably a common issue in many Member States.

Furthermore, providing digital evidence can be an obstacle because of the structure of the Internet and of the volatility of the evidence.

Danish authorities said there is no formalised interaction with judges in order to fully respect their independence. However there is an open dialogue with the court administration and a daily dialogue takes place between local prosecutors and judges.

4.2 Law enforcement authorities

In Denmark there is one single police force, the Danish National Police.
The individual police districts are responsible for the prevention, investigation and prosecution of cybercrime. **The police districts have specially assigned IT investigators and IT engineers to support the investigation**.

At national level, the National Cyber Crime Centre (NC3), has the overall supervision and responsibility for coordination (nationally and internationally) and for instructions regarding the investigation. NC3 also provides assistance to the police districts in cases of cyber attacks, content-related acts facilitated by IT, acts where computers or IT systems are involved as a tool or target and all kinds of cases where digital evidence needs to be secured and analysed.

The Danish National Police said it cannot point to any obstacles to successful investigation of cybercrimes that are unique or especially relevant to Denmark. As such, the main obstacles are, among others, the rapid development of technology, the increasing professionalism and level of expertise of cybercriminals, the fact that cybercrime can easily span the jurisdiction of several countries, the elusiveness of evidence in regard to cybercrime and the wide spread use of encryption, TOR and other means of anonymisation.

The National Centre of Investigation under the Danish National Police operates the Danish Communications Centre 24/7/365 as a Single Point of Contact (SPOC) to the entire Danish police force. This includes requests under the auspices of Europol, Schengen, Baltic Sea Task Force, Frontex, Interpol, the Nordic police cooperation, bilateral cooperation with law enforcement of other countries, cross border surveillance and controlled deliveries. It furthermore handles urgent requests according to the Budapest Convention relating to cybercrime. This means one point of entry to the entire Danish police and no "red tape" in the opening phase of cooperation with other countries. Procedural steps are in place so that requests directed to the SPOC are immediately redirected to the National Cyber Crime Centre (NC3) in order to implement appropriate investigative measures and the involvement of the prosecution service and the judiciary system when needed.

4.3 Other authorities/institutions/Public Private Partnership

The Danish Security and Intelligence Service under the Danish National Police is responsible for preventing, investigating entities and preventing actions that are, or could pose, a danger to Denmark as an independent, democratic and secure society. This also applies to threats targeting information and communication systems, or the use of information and communication systems when the threats also pose a danger to national security.

The Centre for Cyber Security, established in 2012 as part of the Danish Defence Intelligence Service, provide assistance to the authorities and companies essential for the Danish society. The Danish Security and Intelligence Service under the Danish National Police is responsible for preventing, investigating and preventing entities and actions that are, or could pose, a danger to Denmark as an independent, democratic and secure society. This also applies to threats targeting information and communication systems, or the use of information and communication systems when the threats also pose a danger to national security.

In some cyber crime cases, the Centre for Cyber Security provides technical assistance to the National Cyber Crime Centre (NC3). In other cyber crime cases NC3 provides assistance to investigations led by the Danish Security and Intelligence Service.

The Centre for Cyber Security conducts IT security- related technical investigations of cyber attacks against governmental institutions and critical infrastructure in order both to stop the individual attacks and to clarify attack methods and tools so that the protection against similar attacks can be strengthened in society at large. These studies are performed in close collaboration with the authority affected.

For many major cyber attacks both investigations and IT security -related technical studies will be needed. Thus, there is close cooperation both on a strategic and operational level between the Danish Security and Intelligence Service, NC3 and the Centre for Cyber Security.

4.4. Cooperation and coordination at national level

4.4.1 Legal or policy obligations

The private sector is not required to report any kind of cyber crime, including cyber attacks, to the police. However, Danish authorities foster a cooperative relationship with the private sector.

All State authorities, including critical State infrastructure institutions, will report cyber attacks to the Centre for Cyber Security. (*see details in 6.1.2 below*).

4.4.2 Resources allocated to improve cooperation

As co-operation with the private sector is a special focus area in the Strategic Objectives of NC3, resources are allocated and possibilities for further enhancing co-operation are continuously developed.

4.5 Conclusions

- **The Danish Administration has adopted the principles of *Lean management* to add efficiency to their service; this could be regarded as a good practice in building capabilities to prevent and combat cybercrime;**

- **There is evidence of good co-operation between the intelligence services, Law Enforcement and the Centre for Cyber Security;**

- **The close cooperation of prosecutors and police (both placed under the general authority of the same ministry – MoJ) has a clear effect on quality: as the prosecutors know the case from the beginning, they are, systematically, well prepared to present it in court. They also can point out to investigators missing facts or evidence at a very early stage;**

- **As in some other Member States, courts are separated from the prosecution service as "pillars of impartiality", which may result in different levels of awareness of, and general knowledge about cybercrime;**

- **Currently the national case management system does not allow for an overview of all categories of cyber-related crime, or for the early identification of multiple linked cases or parallel investigations and proceedings at national level;**

- **Danish LEA authorities showed examples of effective cooperation with the private sector, based on agreements or Memoranda of Understanding; in particular, NC3 engages with**
  - private partnerships via the so-called *Netfilter programme* aimed at blocking access to material with sexual abuse of children on the internet;
  - Danish banks and private IT companies to combat cyber-enabled bank fraud.

- **The evaluation team was presented with an overview of the judicial system by MoJ. However, the team did not have an opportunity to engage with the Judiciary and to document its experience in relation to cybercrime matters.**

5 LEGAL ASPECTS

5.1 Substantive criminal law pertaining to cybercrime

5.1.1 Council of Europe Convention on cybercrime

Denmark ratified the Convention on Cybercrime (CETS no. 185) on 21 June 2005, and the Convention entered into force on 1 October 2005.

5.1.2 Description of national legislation

General principles relevant to criminal offences in the Danish Criminal Code

In accordance with Section 19 of the Danish Criminal Code, no offences mentioned in the code are punishable due to negligence, unless specifically provided for. This means that only intentional offences are covered by the sections mentioned below, unless otherwise specifically indicated.

Intention in this context covers a range of variations, i.e. explicit intent, intent based on probability and intent as positive acquiescence. Explicit intent is when the action and its result etc., was (explicitly) intended. Intent based on probability is when the perpetrator acted even though the criminalised action and its the result etc., was the most likely outcome. Intent based as positive acquiescence is when the perpetrator achieved a certain result (by perpetrating the action) and accepted this possibility as a part of the risk of the specific action.

Chapter 10 of the Criminal Code sets out the general principles governing sentencing, e.g. terms of imprisonment. Section 81 of the Criminal Code lists a number of non-exhaustive aggravating circumstances. These circumstances are to be considered when determining a sentence for an offence. For instance, prior convictions relevant to the current crime may be considered an aggravating circumstance. Section 82 of the Criminal Code lists a number of non-exhaustive mitigating circumstances when determining the sentence for a criminal offence. For instance, it may be considered a mitigating circumstance if the perpetrator voluntarily reported himself to the authorities and made a full confession.

If several offences have been committed, a concurrent sentence for such offences must be imposed within the limits of the prescribed minimum and maximum penalties pursuant to Section 88. It should be borne in mind that the use of the minimum penalty in the Criminal Code usually means that the possibility to impose a fine as a sentence is absconding, i.e. very few offences have actual requirements for a minimum period of imprisonment (e.g. homicide, cf. Criminal Code Section 237, is punishable with imprisonment for a minimum period of 5 years).

Publicly inciting a person to commit a crime is a criminal offence pursuant to Section 136(1) of the Criminal Code. Furthermore, complicity in a criminal offence by incitement or aiding and abetting is a criminal offence pursuant to Section 23 of the Criminal Code. Attempt is punishable pursuant to Section 21.

The criminalisation of those cybercrime -related acts listed in Table 2 of the GENVAL questionnaire is as follows in Denmark.

- Acts unique to information systems

Illegal access to information systems is criminalised in the following sections of the Criminal Code:

- Section 263(2) regarding wrongfully (unjustifiable) gaining of access to any data or programs of another person intended for use in an information system.
- Section 263a regarding the wrongful selling or distribution to a wide group for commercial gain of a code or other means access to a non-public information system protected by a code or other special access protection and disclosure of a larger number of such codes or access means (concerns non-commercial systems).

- Section 301a regarding the wrongful (unjustifiable) acquisition or disclosure of codes or other means of access to information systems where access is reserved for paying members and protected by a code or other special access restriction (concerns commercial systems). The (commercial) information systems in Section 301a of the Criminal Code including, inter alia, so-called on-demand systems and information collections such as newspaper databases where access is reserved for paying members and protected by code, etc. Examples of code or other special access restrictions mentioned in Section 301a are Network User Identification Codes (NUI), decoding cards and calling cards (telephone PIN codes).

Ten or more codes, etc., are generally required to establish the finding of "a larger number" of information system codes or access means as per Section 263a (2) of the Criminal Code. The maximum penalty for violations of Sections 263(2), 263a or 301a of the Criminal Code is 1 year and 6 months. However, if a person commits any act referred to in Section 263(2) with intent to obtain or become acquainted with the business secrets of an enterprise, or if other particularly aggravating circumstances apply, the penalty may be increased to imprisonment for a term not exceeding 6 years. The same penalty is imposed for any of the offences referred to in subsection (2) which are committed in a systematic or organised manner.

If any disclosure, etc., as referred to in the Section 263a of the Criminal Code Section is made in particularly aggravating circumstances, under subsection (4) the penalty is imprisonment for a term not exceeding 6 years. Especially circumstances in which information is disclosed or otherwise widely shared, or the disclosure entails a particular risk of serious harm, are considered particularly aggravating.

If any disclosure, etc., as referred to in Section 301a of the Criminal Code is made in particularly aggravating circumstances, under subsection (2) the penalty is imprisonment for a term not exceeding 6 years. Especially circumstances in which information is disclosed or otherwise distributed for commercial gain to a large group of people or in a manner entailing a particular risk of serious abuse are considered particularly aggravating.

Illegal system interference is criminalised in the following sections of the Criminal Code:

- Section 193(1) regarding the causing of comprehensive interference with the operation of any public transport means, public postal service, telegraph or telephone service, radio or television broadcasting system, information system or service providing public utility supplies of water, gas, electricity or heating.
- Section 291(1) regarding the destruction, damaging or removal of any property belonging to another person.
- Section 293(2) regarding the act of wrongfully preventing another person from disposing of an item in full or in part. Deleting, damaging, deteriorating, altering or suppressing computer data is covered by Section 291 of the Criminal Code. Denial of service attacks that prevent the normal use of or access to data systems by overload or by causing a breakdown is criminalised under Section 293(2).

The term "*comprehensive interference*" in Section 193 of the Criminal Code is used for acts that have the potential to affect the general public in terms of information systems, etc. An example of such an act is the deletion of an internet provider's data system or other hacking causing interference with a critical infrastructure information system.

The maximum penalty for violations of Section 193 of the Criminal Code is 6 years, while the maximum penalty for violations of Section 293(2) is 1 year. However, the sentence under Section 293(2) may increase to imprisonment for 2 years if an offence is committed in a systematic or organised manner or in otherwise particularly aggravating circumstances.

The maximum penalty for violations of the Criminal Code Section 291(1) is 1 year and 6 months. In the case of serious criminal damage or criminal damage in a systematic or organised manner, or if the offender has previously been convicted under this Section 291 or under Section 180, Section 181, Section 183(1) and (2), Section 184(1), Section 193 or Section 194, the sentence may increase to imprisonment for 6 years.

Illegal data interference is criminalised by the same Sections of the Criminal Code as the Sections mentioned with regard to illegal system interference, such as deletion of damage to, etc., computer data.

Illegal interception of computer data is criminalised in Section 263(2) of the Criminal Code) which deals with the wrongful (unjustifiable) gaining of access to any data or programs of another person intended for use in an information system. Reference is made to the comments about Section 263(2) under illegal access to information.

Misuse of devices - production, distribution, procurement for use, import or otherwise making available or possession of computer misuse tools is not criminalised per se. However, the production, procurement etc. of devices or tools with features that can be misused for the purpose of committing criminal offences is punishable as incitement or aiding and abetting an offence (Section 23) or attempting to commit an offence (Section 21). Hence, planning to design a program with the intention to use it for purposes of a cyber attack is punishable as an attempt to commit, inter alia, illegal interference in accordance with Section 293(2).

- Content-related acts, in particular those related to child sexual abuse online and child pornography

Computer-related production of child pornography involving a child below the age sexual of consent is criminalised in the following sections of the Criminal Code:

- Section 216(2) regarding sexual intercourse with a child below 12 years of age (Section 225 if the sexual act concerns sexual activity other than intercourse);
- Section 222 regarding sexual intercourse with a child below the age of sexual consent (Section 225 if the sexual act concerns sexual activity other than intercourse);
- Section 226 regarding production of pornographic photographs, pornographic films or similar recordings of a person under 18 years of age with intent to sell or otherwise distribute the material,
- Section 232 regarding indecency.

Production of computer-generated child pornographic images is criminalised in the following sections of the Criminal Code:

- Section 235(2) regarding possession or viewing, for payment or through the Internet or a similar system for dissemination of information, of pornographic photographs or films or other pornographic visual reproductions or similar recordings of persons under 18 years of age;
- Section 226 regarding production of pornographic photographs, pornographic films or similar recordings of a person under 18 years of age with intent to sell or otherwise distribute the material;
- Computer-related distribution of child pornography is criminalised in Section 235(1) of the Criminal Code regarding distribution of pornographic photographs or films or other pornographic visual reproductions or similar recordings of persons below 18 years of age.

Computer-related possession of child pornography is criminalised in Section 235(2) of the Criminal Code regarding possession or viewing, for payment or through the Internet or a similar system for dissemination of information, of pornographic photographs or films or other pornographic visual reproductions or similar recordings of persons under 18 years of age. However, it follows from Section 235(3) of the Danish Criminal Code that possession of material involving a child who has reached the age of sexual consent, that child having consented to possession, falls outside the scope of Section 235(2).

The term "pornographic photographs, pornographic films or similar recordings of persons below 18 years of age" includes persons appearing to be a child. However, if the depicted person appearing to be a child was in fact 18 years of age or older at the time of depiction the material is not considered as child pornography. The term pornographic visual reproductions or similar recordings of persons under 18 years of age means in particular computer- generated images that do not depict a real person under 18 years, but, apart from the fictional aspect, fully resemble a photograph. The fictional production must therefore appear approximately the same as photographs and so forth.

Criminal liability for the abovementioned offences requires intent (Section 19, cf. Sections 216(2), 222, 226, 232 and 235 of the Criminal Code). However, pursuant to Section 228 of the Criminal Code, criminal liability for violations of Sections 222 and 226 can be incurred despite lack of knowledge of the victim's age if the perpetrator acted negligently with respect to the victim's age. The maximum penalty for violations of Sections 216(2) of the Criminal Code is 12 years.

The maximum penalty for violations of Section 222 is imprisonment for a term not exceeding 8 years. If the perpetrator has used coercion or threats the maximum penalty is imprisonment for a term not exceeding 12 years. The maximum penalty for violations of Section 226 is imprisonment for a term not exceeding 6 years. The maximum penalty for violations of Section 232 is imprisonment for a term not exceeding 4 years if the child is below 15 years and imprisonment for a term not exceeding 2 years if the child is 15 years or older. The maximum penalty for violations of Section 235(1) is imprisonment for a term not exceeding 2 years or in particularly aggravating circumstances imprisonment for a term not exceeding six years. The maximum penalty for violations of Section 235(2) is imprisonment for a term not exceeding 1 year.

Computer-related "grooming" is criminalised as an attempt (Section 21) to commit a sexual offence against a child pursuant to Chapter 24 of the Criminal Code, e.g. an attempt to engage in sexual intercourse with a child who has not reached the legal age for consent or to produce child pornography. Because "grooming" is criminalised as an attempt to commit a sexual offence "grooming" is not defined in the Criminal Code. However, criminal liability for attempt includes in principle any preparatory action irrespective of whether the action itself is harmless or unsuitable as a means to commit the intended crime. Thus, computer-related "grooming" may be punishable from the time the perpetrator first contacts the child with the intent to commit the sexual offence regardless of whether the contact is initiated by means of information and communication technology or whether the perpetrator has proposed to meet the child and taken material steps leading to such a meeting.

The maximum penalty for computer-related "grooming" relates to the offence that the perpetrator attempted to commit. For example,. the maximum penalty for computer-related "grooming" with intent to produce child pornography intended for distribution (Section 21 and Section 226 of the Criminal Code), is the maximum penalty for production of child pornography with intent to distribute the material, which is imprisonment for a term not exceeding 6 years.

In the opinion of the evaluation team the concept of a very early beginning of the stage of attempt certainly covers most cases of grooming, especially if the necessary intent can be proven. This might in many cases not be too difficult, given the special nature of the offence. However, it might be worth keeping in mind that situations can arise, where the intent is difficult to prove or suspects voluntarily abandon their attempt, which would lead to an absence of criminal liability. The fact that grooming is merely considered an attempt might also lower the social stigma of the crime. In many countries such an attempt would even be considered as a mitigating circumstance.

- Acts where computer/IT systems were involved as tool or target:

Computer-related fraud is criminalised in the Section 279a of the Danish Criminal Code regarding data fraud. To ensure the criminalization of cases of fraud where no human person is misled because the treatment of information/data is made by an information system this section was introduced in 1985.

The maximum penalty for violations of Section 279a is imprisonment for 1 year and 6 months. However, if the data fraud is of a particularly aggravating nature, especially because of the methods used, because the offence was committed jointly by several persons or due to the scope of the gain made or intended, or when several offences have been committed, the penalty may increase to imprisonment for a term not exceeding 8 years (Section 286(2)).

Computer-related forgery is criminalised in Section 171, which deals with fraud. The section applies to forgery of electronic data. Hence, the offence covers all electronic data that form a verification, including e-mails, voice-mails etc..

The maximum penalty for violations of Section 171 is 2 years of imprisonment. If the forgery is particularly aggravating or multiple offences of the same nature have been committed, the penalty may increase to imprisonment for a term not exceeding 6 years.

Regarding computer-related identity offences, it should be noted, that identity theft is not separately criminalized. However, because of the broad scope of the rules on attempt and incitement or aiding and abetting, identity theft will often be considered an attempt to commit another offence, e.g. fraud, and will thereby result in criminal liability.

Examples of offences where misuse of identity can be the main modus operandi – other than the above mentioned – are:

- wrongful disclosure of communications or pictures concerning the private affairs of another person (the rightful owner of the identity) under Section 264d, or
- defamation of another person's character (the rightful owner's character) by offensive expressions or acts or by making or propagating allegations of acts likely to reduce the esteem in which such person is held by his fellow citizens (Section 267).

Sending or controlling the sending of spam is not separately criminalised. However, because of the broad scope of the rules on attempt and incitement or aiding and abetting, it will often be considered an attempt to commit another offence and thereby result in criminal liability. If sending spam renders an internet service, e.g. an e-mail account, unavailable, this may be a violation of the Section 293(2) of the Criminal Code, and the act of controlling may then be considered incitement or aiding and abetting commission of the offence. If spam results in any form of damage, deletion, deterioration of data, this may be a violation of the Section 291 (vandalism).

Legal persons are subject to criminal liability in accordance with Section 306, (cf. Section 25-27) of the Criminal Code, for violating sections in the Criminal Code, including provisions covering criminal acts committed as cybercrime. Legal persons are subject to punishment by fines in accordance with Sections 50 and 51 of the Danish Criminal Code. There is in theory no maximum level for fines imposed under the Criminal Code.

The Criminal Code contains no general criteria on what is to be considered a "major offence". No legal definitions are set either. However, such criteria are typically implemented in the individual sections on the offences and the criteria are then essential when determining which maximum penalty is applicable in a specific case.

For example, a systematic or long-term denial of service attack on a server can be considered as deserving the maximum penalty under Section 293(2). The assessment of whether a series of such attacks are to be considered systematic or long-term is on the whole a matter for the courts to assess.

Minor offences resulting in punishment with a fine can be handled by the police without involving the court on condition that the perpetrator confesses to the offence and is prepared to settle the case with a fine.

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

Denmark has not transposed Directive 2013/40/EU on attacks against information systems as, it is not bound by this Directive in accordance with Articles 1 and 2 of the Protocol (No 22) on the position of Denmark annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union..

However, in relation to a referendum regarding, inter alia, Europol held in Denmark on the 3rd of December 2015, the Ministry of Justice conducted an analysis of Denmark's compliance with the Directive. The MoJ said Danish legislation is largely compliant with the Directive, however:

- with regard to Article 9(3) and 9(4) on minimum requirements to the maximum penalty a minor amendment of Section 291(2) would have to be made to ensure that illegal system interference with a critical infrastructure information caused by deletion, damage, deterioration etc. is punishable by at least five years of imprisonment,
- the same minor amendment would be necessary for Section 293(2), together with a raising of the maximum penalty to at least five years of imprisonment in order to be compliant with Article 9(3) and 9(4). Moreover, rules on the misuse of personal data with the aim of gaining the trust of a third party, thereby causing prejudice to the rightful identity owner as an aggravating circumstance in respect of all the offences relevant to Articles 4 and 5 would have to be set out in the Criminal Code.

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

Denmark has not transposed Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography as Denmark is not bound by the Directive or subject to its application in accordance with Articles 1 and 2 of the Protocol (No 22) on the position of Denmark annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union.

However, by Act No. 633 of 12 June 2013, the Chapter 24 of the Criminal Code on sex crimes was amended. The amendment included raising the maximum penalty for attending pornographic performances involving the participation of a child from a term not exceeding 1 year of imprisonment to a term not exceeding 2 years of imprisonment, thereby bringing Danish legislation into line with Article 4(4) of the Directive. Furthermore, the statute of limitation in cases where a child below the age of sexual consent is incited to witness sexual activity without participating (punishable as indecency under the Danish Criminal Code) was amended so the date from which the statute of limitation is counted at the earliest starts from the day the child turns 21 years of age, thus, enabling prosecution for a sufficient period of time after the victim has reached the age of majority in line with Article 15(2) of the Directive.

In relation to a referendum regarding, inter alia, Europol held in Denmark on 3 December 2015, the Danish Ministry of Justice conducted an analysis of Denmark's compliance with the Directive. The analysis showed that Danish legislation for the most part is in accordance with the Directive.
However, with regard to Article 5(6) regarding the production of child pornography, the maximum term of imprisonment pursuant to the Danish Criminal Code is not in compliance with the Directive in cases where the child is above the legal age of consent (15 years) and the perpetrator does not intend to disseminate the pornography.

C/ Online Card fraud

National Cyber Crime Centre (NC3) hosts a meeting forum in which the largest provider of digital payment solutions, several of the largest banks and the Danish Bankers Association participate.

Within the forum trends and tendencies – e.g. new tools and modus operandi – and countermeasures are shared and discussed.

D/ Other Cybercrime phenomena

The Danish Police are struggling to keep up with cybercriminals who constantly invent and develop new strategies and tools. To mitigate this, the National Cyber Crime Centre (NC3) constantly implements new software, which includes both commercial and its own tools which it develops. In addition, NC3 recently hired highly - skilled IT engineers who are assigned to each of the police districts.

The National Cyber Crime Centre (NC3) participates in the Europol -driven cooperative framework to investigate and prevent payment card fraud. The Danish Bankers Association is cooperating with similar institutions across Europe just as most of the larger Danish banks are part of an international financial institution. Through these networks the Danish financial sector receives and distributes information regarding border-crossing online card fraud.

5.2 Procedural issues

5.2.1 Investigative Techniques

For the purpose of investigating criminal offences, police can subject persons – mainly persons under suspicion – to a number of coercive and provisional measures.

- Search and seizure of information is possible during investigation of a cybercrime offence in accordance with Chapter 73 and 74 of the Administration of Justice Act. Sections 793 to 807 contain general provisions on trace, search, seizure and freezing. Section 793 sets out the scope of application of the rules on search. For investigations into all the offences mentioned under 2.A. permission for a search may be granted on condition that there are reasonable grounds to suspect the person whose property is subject to the search of committing the crime and on condition that the search is presumed to be of substantial importance to the investigation. Search of a third party's (non-suspects') property can be made when there is reason to presume that evidence or items subject to seizure can be found. Rules on the need for a court order on search and the general conditions for a search are found in Sections 796 to 798.

Section 801 lays down the general scope of application of the provisions on seizure and defines the purposes of seizure. The most common cause for seizure pursuant to Section 802 is grounds to presume that the items can serve as evidence or should be confiscated on the basis of reasonable grounds to suspect the owner or the holder. Seizure may also be made of a third party's items and property on the same conditions as for a suspect. Rules on the general conditions for seizure are found in Sections 805-807.

- Gaining access to websites that have blocked public access, inter alia with a password restriction, is in legal terms considered a search in accordance with the Administration of Justice Act. An electronic document is in legal terms considered an item in relation to search and seizure. This means that a website with unlawful content can be seized in accordance with the rules of seizure in the Administration of Justice Act.

- The use of real-time interception of traffic and content data pursuant to Section 791b is restricted to the serious cybercrime offences punishable by six years' imprisonment. Hence, interception is not possible as part of a investigation of a person who illegally prevents another from using or disposing computer data etc., e.g. a denial of service attack, in accordance with Section 293(2) of the Criminal Code. In addition to this basic condition, reasonable grounds to presume that information is being used or passed by a suspect need to be present as well as a presumption that the interception is of essential importance to the investigation.

- Under Section 781 interception of telecommunications (content data) etc. is also permitted in relation to the serious cybercrime offences punishable by at least six years' imprisonment if there are reasonable grounds to presume that information is being used or passed from a suspect and that the interception is presumed to be of essential importance to the investigation. This measure includes disclosure of email-correspondence and other available content. This Section concerns tapping communication through the service provider's facilities, in contrast to interception under Section 791b, which covers "skimming" via computers (or other information systems).

Providers of telecommunications services can be ordered to preserve computer data pursuant to Section 786a. A preservation order obliges the providers to preserve the data for a period not exceeding 90 days. Within this period police authorities can secure the data through a seizure under Sections 801-802.

In addition, a service provider can be ordered to disclose customer information only necessary for dynamic IP addresses in accordance with Section 804 on condition that the order is issued as part of an investigation into an offence and on condition that there is reason to presume, inter alia, that the item or information can serve as evidence.

Police may request information on statistic IP addresses without a court order.

Providers of telecommunications are obliged to store traffic data for at least 1 year in accordance with Section 786(4) and ministerial order no. 988 issued 28th of September 2006. The provisions oblige telecommunications providers to store a wide range of information on telecommunications traffic to permit subsequent disclosure to the police as part of the investigation and subject to a court order. Information on internet traffic data with the exception of basic subscriber information is no longer a requirement under Section 786(4) and the above-mentioned ministerial order.

An order for stored traffic and content data can be issued by a court under Section 783, cf. 781- 782. As with the interception of communications, the disclosure of traffic and content data is restricted to the serious cybercrime offences punishable by at least six years' imprisonment. A specific exemption from six -year prison term is made in relation to the violation of Sections 235 and 263(2) of the Criminal Code, cf. Section 781(2) of the Administration of Justice Act. This Section covers gaining unlawful access to data or programs intended for use in an information system ("traditional hacking"). A similar exemption is made in relation to investigations of data fraud pursuant to Section 279a of the Criminal Code Section, cf. Section 781(3) of the Administration of Justice Act.

In addition to this basic condition, there need to be reasonable grounds to presume that information is used or being passed by a suspect and that the interception is presumed to be of essential importance for the investigation.

Pursuant to Section 781, subsection 1(3) stored traffic data subject to disclosure in accordance with Section 781 is information on telecommunications traffic in relation to a specific telephone number or IP address, and, pursuant to (4), information on all telecommunications traffic within a specified radius of a location. Disclosure of user information can be ordered pursuant to Section 804. In relation to IP addresses a court order for disclosure is only necessary for dynamic IP addresses. Providers of telecommunications are obliged to disclose user information on static IP addresses to the police.

During the on-site visit the evaluation team was informed of the situation as regards traffic data retention for investigation purposes as follows:

Denmark introduced legislative rules on telecommunication and internet traffic data retention in 2002. In 2007 the national law was adapted in accordance with the EU directive. Considering the ECJ ruling in 2014, Denmark came to conclusion that, with regard to legal safeguards in place, the national law on data retention could be upheld. However, rules applicable to the retention of internet traffic data proved to be technically not adapted in practice. Denmark decided to withdraw and entirely reform them, in consultation with service providers and other interest groups including NGOs dealing with fundamental rights. A new legislative proposal is being prepared for adoption in the forthcoming months.

Special investigative techniques in use. The National Cyber Crime Centre (NC3) uses analysis of log/traffic data and malware samples to determine the origin of the attack/malware as well as the destination of any stolen data. NC3 also uses wiretapping to profile the suspect prior to arrests, which could, among other things, disclose whether he/she uses VPS. Finally, NC3 uses human sources and open sources to collect intelligence and evidence.

5.2.2 Forensic and Encryption

Since encryption is default in many applications, the Danish Police often encounter problems with encrypted data. The encryption makes it difficult to get access to content on seized devices.
In regard to wiretapping the police are limited to the traffic data, since the encryption prevents access to the content.

The experience of National Cyber Crime Centre (NC3) is that encryption is used across a wide spectrum of offences. The Centre addresses the challenge through the use of brute force and intelligence gathering, e.g. interrogation of the perpetrator and collection of passwords from his/her other devices.

On a strategic level the different LEA in Denmark discuss the challenges concerning cybercrime e.g. encryption. On an investigative level the different LEA can ask each other for help in specific cases.

NC3 is the forensic centre supporting the local police districts. In Denmark LEA decryption is not carried out in cooperation with private companies. NC3 has yet only had limited success in some cases. NC3 performs electronic forensic examinations using Encase. It is possible to do forensic examinations of a very wide array of devices ranging from USB drives and mobile phones to server arrays.

NC3 can also perform remote forensic examinations both in regard to cloud services and physical servers that can be accessed via the internet. Remote forensic examinations can be executed in a number of ways, for instance through source- based interception or by exploiting a vulnerability on a server to gain access to the file system etc. These methods require the police to
obtain a court order beforehand.

Finally, NC3 has access to an open - source intelligence tool that can be used to harvest data from open sources such as newspapers and public Facebook pages etc., and it can continually monitor such sites.

5. 2.3 E - e v i d e n c e

No legal definitions are laid down in the national law for the terms *computer data, content data, traffic data, order for search/seizure of information system, networks managed or controlled by suspects of cybercrime*.

There is no legal definition of e-evidence in Denmark; however, **Danish courts operate under what is called a "free assessment of evidence".** This means that evidence that is brought before a court of law can be used. The courts will then decide on a case- by- case basis how much value to put on each piece of evidence. Any errors in relation to the obtaining of a piece of evidence or any undocumented steps in the evidence chain will result in that particular piece of evidence having less of an impact on the courts' decision.

The police can obtain "e-evidence" in accordance with the general rules in the Danish Administration of Justice Act. They expressed the opinion that, with regard to cyber cases, it is very important that the evidence chain is well documented, as regards how the evidence was originally obtained, who has handled it and how it was handled – including whether it was altered in any way – all the way up to the point where the evidence is used in a court of law.

The main outstanding legal issues relate to the legal status of the retention by service providers and use by LEA of Internet traffic data. As described in point 5.2.1 above a legal decision is awaited on this - which is, for now, leaving LEA with an uncomfortable degree of uncertainty.

5.3 Protection of Human Rights/Fundamental Freedoms

In Denmark the Commutations Service Providers (CSP) are obliged to retain data regarding telecommunications as well as subscriber information for a period of 12 months. The Danish Police can access and use the retained data only after having obtained the relevant court order from the Danish Courts. However it should be noted that such Court order would not be necessary if the data subject provides his/her consent.

The National Cyber Crime Centre (NC3) has drawn up an internal policy regarding all its databases and registers containing personal identification data. This internal policy contains rules regarding security measures, access to the data in the databases etc. as well as rules regarding deletion of data.

Pursuant to Section 263, Subsection 2, it is illegal to obtain without permission access to someone else's information or programs used in an information system. This may cover the Internet.

Furthermore, the Danish Act on Processing of Personal Data regulates the administration of personal data in information systems under the authority of the Danish Data Protection Agency. The latter may make decisions on whether certain processing is in accordance with the rules laid down in the Act on Processing of Personal Data.

If the Danish Data Protection Agency discovers punishable violations of the Act on Processing of Personal Data in connection with handling a complaint or an inspection, the Danish Data Protection Agency is authorised to issue a ban or enforcement notice or report the violation to the police.

Investigations performed by the Danish Police are conducted in accordance with the Danish Administration of Justice Act.

5.4 Jurisdiction

5.4.1 Principles applied to investigate cybercrime

The Danish jurisdiction rules in Sections 6-9 in the Criminal Code provide for jurisdiction with regard to, inter alia, cybercrime acts committed partially or entirely outside Denmark.

Section 6 of the Criminal Code provides: "Acts falling within Danish criminal jurisdiction are acts committed –

(i) within the Danish state;

(ii) on board a Danish vessel or aircraft located within the territory of another state by a person belonging to or travelling on the vessel or aircraft; or

(iii) on board a Danish vessel or aircraft located outside the territory of any state."

Reference is made to Section 9(2) of the Criminal Code.

In Section 9 it is stated:

"(1) Acts are deemed to have been committed at the place where the offender was when the act was committed. As regards legal persons, acts are deemed to have been committed at the place where the act(s) making the relevant legal person liable were committed.

(2) If the criminality of an act depends on or is influenced by an actual or intended consequence, the act is also deemed to have been committed at the place where the effect occurred, or where the offender intended the effect to occur.

(3) Attempts or acts of complicity are deemed to have been committed within the Danish state if the offender was in Denmark when the act was committed, irrespective of whether the offence was completed or intended to be completed outside the Danish state.

(4) Where part of an offence was committed within the Danish state, the full offence is deemed to have been committed in Denmark."

Section 7 of the Criminal Code concerns the active personality principle. Section 7 states:

"(1) Acts committed within the territory of another state by a person who was a Danish national or has his abode or similar habitual residence within the Danish state at the date of the provisional charge are subject to Danish criminal jurisdiction, if –

(i) the act is also a criminal offence under the legislation of the country in which the act was committed (dual criminality); or

(ii) the offender had the aforesaid attachment to Denmark when committing the act and such act

- (a) comprises sexual abuse of children, human trafficking or female circumcision; or
- (b) is aimed at someone having the aforesaid attachment to Denmark when the act was committed.

(2) Acts committed outside the territory of any state by a person having such attachment to Denmark as referred to in subsection (1) at the date of the provisional charge are also subject to Danish criminal jurisdiction, provided that acts of the kind described may carry a sentence of imprisonment for a term exceeding four months.

(3) Subsections (1)(i) and (2) apply, with the necessary modifications, to acts committed by a person who is a national of or has his abode in Finland, Iceland, Norway or Sweden at the date of the provisional charge, and who is staying in Denmark."

With regard to the passive personality principle reference is made to Section 7a of the Criminal Code. In Section 7a it is stated:

"(1) Acts committed within the territory of another state and aimed at a person who was a Danish national or had his abode or similar habitual residence within the Danish state when the act was committed are subject to Danish criminal jurisdiction if any such act is also a criminal offence under the legislation of the country in which the act was committed (dual criminality) and may carry a sentence under Danish legislation of imprisonment for at least six years.

(2) Danish criminal jurisdiction under subsection (1) only applies to the acts of –

(i) murder;

(ii) aggravated assault, deprivation of liberty or robbery;

(iii) offences likely to endanger life or cause serious injury to property;

(iv) sexual offences or incest; or

(v) female circumcision.

(3) Acts committed outside the territory of any state, but aimed at someone having such attachment to Denmark as referred to in subsection (1) when the act was committed are also subject to Danish criminal jurisdiction, provided that acts of the kind described may carry a sentence of imprisonment for a term exceeding four months."

Regarding legal persons, reference is made to Section 7b of the Criminal Code:
"Where the application of Danish criminal jurisdiction to a legal person is subject to dual criminality, the criminal liability of legal persons need not be prescribed by the legislation of the country in which the act was committed."

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

In Denmark, there is no law concerning the conflicts of jurisdiction in the case of two or more Member states investigating and prosecuting the same perpetrator. The Danish authorities said, however, that the Prosecutor's Office's decision to prosecute or not to prosecute certain cases resolves such questions. The decision is based, inter alia, on the legal doctrine on the *Ne bis in idem* principle.

The Director of Public Prosecutions (DPP) has no information on whether Denmark has experienced conflicting jurisdiction in cases involving cyber crime. In connection with the entry into force of Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings, the Danish Ministry of Justice considered that the principles expressed in the framework decision were already used by the Danish Prosecution Service when dealing with cases of conflicts of jurisdiction.

However, in order to make sure that the framework decision can be considered correctly and fully implemented in Danish law, the Ministry of Justice has instructed the Director of Public Prosecutions to issue an instruction to the Prosecution Service that cases of conflicting jurisdiction should be dealt with in accordance with the framework decision.
The DPP is in the process of drafting this instruction.

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

On 10 May 2012, the Danish Supreme Court delivered a decision in a case regarding data acquisition of a Facebook and a Messenger profile belonging to a suspect in a criminal investigation. The Supreme Court decided that the Danish Police were allowed to gain access to the Facebook and the Messenger profiles via the internet using the correct codes for the profiles that had been obtained through other investigative measures. The reasoning behind this was that the crime that was being investigated was subject to Danish criminal jurisdiction and that access to the profiles could be achieved via the internet without having to involve foreign authorities.

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

On page 69 of the reply to the GENVAL questionnaire, Denmark acknowledged in general terms the need for further legislative progress. *Danish authorities are invited by the evaluation team to provide more details about the current thinking and working progress on this issue.*

Concerning the assessment of and suggestions from Denmark with regard to EU law, see point 9.5 below.

5.5 Conclusions

- **The Danish criminal code is, in general, well adapted to the whole area of cybercrime investigation; Danish authorities may exercise coercive powers, intercepts etc. in accordance with legislation which protects the rights of the Danish citizen;**

- **It is worth mentioning that, when Denmark does not participate in EU legislation in criminal matters, the Ministry of Justice systematically screens this legislation and seeks to align, as far as possible, the domestic legislation with EU requirements; some gaps may be filled through instructions to prosecutors;**

- **Legislation for the mandatory retention of traffic telecommunication data is in place; however, rules on Internet traffic data are missing and under preparation (deadline parliamentary year 2016-2017);**

- **Like many other Member States Denmark lacks clear rules for resolving conflicts of jurisdiction in cyberspace with other countries; however an instruction from DPP directed at the Prosecution Service is under preparation.**

6 OPERATIONAL ASPECTS

6.1 Cyber attacks

6.1.1 Nature of cyber attacks

Cyber attacks on critical infrastructure of Danish public and private institutions essential for the society are monitored by the Centre for Cyber Security. A recent threat assessment from the Centre for Cyber Security points to espionage and crime in terms of fraud and extortion (e.g. ransomware) as the most serious threats to Danish authorities and private companies.

The Danish National Police do not, however, possess statistics on the number of attacks.
In regard to espionage, there have been state- sponsored attacks on Danish authorities and the private sector. A recent attack targeting the Danish Ministry of Foreign Affairs lasted approximately seven months and consisted of 47 e-mails to 9 different accounts within the Ministry. The e-mails originated from 21 addresses. The attacks were well made but did not succeed because they were either blocked by the mail-scanner of the Ministry or the security system blocked communication between the malware and the external actor. The lesson learned from this attack, and attacks similar to this, is that an effective defence takes both the leadership level and the staff level into consideration along with a prioritization of the adequate technical solutions. The sophistication of social engineering techniques in use in cyber attacks is increasing, and awareness of security among all staff members is therefore imperative.

In regard to cybercrime the number of fraud and extortion cases are increasing. During 2015 there has been several “waves” of ransomware attacks that have reached private individuals, companies and public institutions. The Danish National Police furthermore deal with an increasing number of cases related to payment card fraud.

Threats from politically motivated actors are assessed as a medium -scale threat by the Centre for Cyber Security. There have not been many serious cases of this kind but the capacity and willingness to attack a company or business that attracts negative attention are there.

6.1.2 Mechanism to respond to cyber attacks

The Danish Government has decided that all State authorities must report all significant cyber attacks to the Centre for Cyber Security (CFCS) in order to ensure situational awareness and the best possible national overview of the current security situation. If Denmark is subject to or threatened by a cyber attack with major consequences for sectors of society, the crisis management organisation under the auspices of the Prime Minister´s Office is activated using the general procedures described in the national contingency plan.

The purpose of Centre for Cyber Security (CFCS) is to contribute to the protection of Denmark against cyber threats. One of its primary tasks is to detect, give notification of and counter cyber attacks aimed at Denmark's national security and Danish interests.

The Danish Centre for Cybersecurity takes the lead on cyber attack matters and appears to be well equipped to carry out this function. It works in partnership with the intelligence and security agencies as well as NC3; the Centre for Cybersecurity assesses the information it receives prior to dissemination to the relevant party. The National Operating Staff (NOST) is a coordinated multidisciplinary mechanism which can be activated in order to respond to a serious cyber attack. The Danish National Police, Danish Security and Intelligence Service (PET) and the Centre for Cyber Security (CFCS)/Danish Defence Intelligence Service (DDIS) are permanent members of the National Operating Staff (NOST).

6.2 Actions against child pornography and sexual abuse online

The National Cyber Crime Centre (NC3) has a unit of 15 employees dealing with child sexual exploitation only: 9 IT forensic investigators, 2 on - line investigators, 2 proactive investigators, 1 victim ID specialist and 1 team leader.

NC3 deals with CSE investigations on a national and coordinating level, and the jurisdiction in each investigation lies with the local police district.
This means that arrests, house searches, interrogations etc. are the responsibility of the police districts. NC3 therefore carries out investigation in cooperation with the 12 police districts in Denmark.

All forensic examination of seized digital equipment is performed by NC3.

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

To identify victims in Denmark, the National Cyber Crime Centre (NC3) uses its own database and the Interpol's ICSE database. Moreover, NC3 has developed a “look-a-like” software as technical back-up to the identification effort.

To avoid re-victimisation, the National Cyber Crime Centre (NC3) has good experiences with the blocking of internet sites with illegal content of sexual child abuse.

NC3 cooperates with the NGO "*Save the Children*" and the majority of the Danish internet providers on the so-called "*Netfilter*" cooperation. The purpose of the "*Netfilter*" cooperation is, on a voluntary basis, to block access to material with sexual abuse of children on the internet. In this respect, NC3 on a regular basis provides websites to the internet providers that NC3 assesses as containing material covered by the Criminal Code provisions on child pornography. It is then the internet providers that block pages according to the terms of the internet provider. This cooperation has proven useful and effective in a number of cases relating to online child sexual abuse, especially in cases with servers located abroad.

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

On a regular basis, "Save the Children-Denmark" and the **Danish child helpline *Børns Vilkår***, publishes campaigns targeting children, youth and parents aimed at the prevention of children and youth to become victims of sexual child exploitation.

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

Save the Children-Denmark and the Danish child helpline *Børns Vilkår* operate hotlines where they provide guidance to children, youth and parents on how to act in the event of sexual child abuse or behaviour on the internet and chat counselling and also, e.g., how to file a report to the police.

On the website of the Danish National Police the National Cyber Crime Centre (NC3) has published information guides for children and parents/adults with responsibility for children, respectively, on how to behave on the internet, information on internet-related criminal activity, how to report to the police and what citizens can do by them themselves to avoid becoming a victim of online sexual abuse and stop the further distribution of such material.

6.2.4 Actors and measures counterfeiting websites containing or disseminating child pornography

In cases where illegal content is found on a server in Denmark, the Danish Police may obtain a court order that allows them to seize the server and/or the domain that the server's content is placed on.

As mentioned above, the Danish *Netfilter blocking system* aims to block access to websites that offer child abuse material. Participation in the scheme is voluntary for the internet providers, and each internet provider has to sign and abide by a contract. The administration of the *Netfilter* is taken care of by NC3. Staff from NC3 assess and add websites to the filter. The actual blocking is dealt with by the CSPs, where the filtering is done. The blocking is a DNS blocking which means that it is the actual URL that is blocked. The site is not removed from the internet, and can still be accessed via the IP address.

Each day staff at National Cyber Crime Centre (NC3) is evaluating potential illegal websites to decide whether the site should be blocked or not. If a site is deemed illegal, it is added to the "*Netfilter*" database. Each hour the "*Netfilter*" database automatically generates a list of sites to be blocked by the internet providers. Once a day the internet providers download the list and use it to block access to illegal sites.

There are four ways NC3 obtains knowledge of websites for further assessment:

1. When there is an attempt to a blocked site, a log file is created at the internet provider with information about where the user came from when he/she ended up on the blocked site. These logs are sent to NC3 once a day. The log file is anonymous and contains no data that can identify the user, but only data on what site the viewer had accessed before meeting the blocked page. These pages are then evaluated.
2. Reviews from citizens and *Save the Children-Denmark*.
3. Websites surfaced during the investigation of cases.
4. International cooperative links, including Interpol and Europol.

Cooperation with the Danish internet providers for blocking access to illegal websites has just celebrated its tenth anniversary and it is running smoothly. In cases where the server is located outside Denmark, NC3 looks for coordination through Interpol and the "Worst of list".

Denmark uses the Interpol CSE database frequently for victim ID issues. Furthermore, Denmark has been involved in the development of the Interpol ICSE-project since the very beginning. The Danish National Police are using ICSE through their own direct VPN connection.

The National Cyber Crime Centre (NC3) participates in the European Union Strategic Group of the Heads of National High-Tech Crime Units at Europol and as far as possible also in other strategic as well as operational cooperative forums.

6.3 Online card fraud

The Danish Agency for Digitisation offers Danish citizens and foreigners residing in Denmark NemID, which is a secure login on the Internet. It consists of a user ID, a password and a code card containing one-time passwords. Today, most telecommunication providers, finance companies and other Danish internet dealers demand NemID as authentication.

In addition, online payments are protected by companies that specialise in powering digital payments. These companies connect banks, businesses and consumers via an international network facilitating digital payments across the Nordic region, providing a broad range of card services, account services, and payment solutions for merchants.

6.3.l Online card fraud reporting

Danish authorities said the degree of reporting online card fraud to law enforcement authorities is assessed as very high since in most cases the filing of the criminal complaint is a condition imposed by the insurance companies.

6.3.2 Role of private sector

In the area of online bank fraud, the National Cyber Crime Centre (NC3) hosts a meeting forum with participation by the largest provider of digital payment solutions, several of the largest banks and the Danish Bankers Association. Within the forum trends and tendencies are shared – e.g. new tools and modus operandi – and countermeasures are discussed.

6.4 Other cybercrime phenomena

The Danish Police are struggling to keep up with cybercriminals who constantly invent and develop new strategies and tools. To mitigate this, the National Cyber Crime Centre (NC3) constantly implements new software, which includes both commercial and own developed tools. In addition, NC3 recently hired highly skilled IT engineers that are assigned to each of the police districts.

6.5 Conclusions

- **The ability of the Danish Centre for Cybersecurity to act as a "clearing house" for information between itself, the police (NC3) and the intelligence services could be promoted as a mechanism for good practice;**

- **NC3 takes the lead in relation to the investigation of child sexual abuse material online and also maintains the national hash set with regard to child abuse images;**

- **The investigators in NC3 are supported in their work by an "innovation unit" composed of civilian IT experts who provide technical support and constantly seek ways to improve the efficiency and capability of NC3;**

- **All Danish organisations visited accept that there is a need to have a blend of both sworn and civilian staff employed in this area; however, they recognise that there is an issue around employee retention and to counter that have tried to create a "best in the class" working environment;**

- **NC3 carries out its duties in conjunction with NGOs and ISPs; one specific and valuable mechanism used in cooperation with the latter is the *Netfilter* project whereby if users try access a website blocked due to illegal content, this will be recorded. From this, the website they previously visited is communicated to NC3. If this website is of a similar character, it will be blocked also. However, the log file is anonymised and contains no data that can identify the user.**

7 INTERNATIONAL COOPERATION

7.1 Cooperation with EU agencies

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

The referendum of 3 December 2015 ended in a "no" to the replacement of the "opt-out model". The Danish government now seeks to strike a parallel agreement to allow the continued participation of Denmark in Europol/EC3 activities.

Cooperation with the national desk at Eurojust is not regulated by any formal requirements or specific procedures. In implementing the Eurojust Decision, Denmark encouraged local police and prosecutors to take maximum advantage of the assistance provided by Eurojust. This has been promoted by informal ways of contact and cooperation.

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

Europol/EC3. In cases with international connections the National Cyber Crime Centre (NC3) sends reports and, e.g., malware samples to Europol/EC3. In a number of cases EC3 has been used as a hub to coordinate distribution of information among several Member States. NC3 participates in the EMPACT cooperation and the derived operations.

The assessment of NC3 is that EC3 has created a framework and foundation for trust and close cooperation between Member States, which is essential in regard to combating international cybercrime. According to Danish authorities EC3's coordination, data collection, malware analysis etc. has had and will continue a significant impact on combating international cybercrime.

Eurojust. The national desk at Eurojust assisted Danish authorities in a number of cases. The following examples can be mentioned:

- A major case of cyber attack committed by a Swedish national. The national desk assisted in obtaining information on case law from other EU member states;
- A case regarding child pornography. The national desk assisted in obtaining information from Romania on an attempted purchase of a child for sexual purposes;
- A number of cases regarding online fraud and credit card fraud. The national desk has assisted in several ways, also by attending and organising coordination meetings.

In some cases, the Prosecution Service also receives assistance from the national unit at Europol.

The Danish national member of Eurojust has mentioned that information gathered by Europol/EC3, in some types of cases, could be used more systematically to ensure coordinated investigation and prosecution as this information may provide a better overview than what is possible from looking at single cases.

7.1.3 Operational performance of JITs and cyber patrols

JITs. The National Cyber Crime Centre (NC3) has not participated in official JITs, but NC3 has several times participated in joint operations and investigations with a number of other Member States.

The national desk at Eurojust has reported that Denmark has participated in a JIT with Germany regarding online fraud committed in Germany and aimed at customers in Denmark. At the moment, Denmark is also involved in a JIT regarding trafficking in human beings where the crime has taken place also via the use of internet services, and electronic identities and signatures.
Denmark is seeking the possible funding from Eurojust in all cases where JITs are set up.

Cyber patrols. The National Cyber Crime Centre (NC3) participates in different Europol coordinated actions against e.g. end users of Crime As a Service. Moreover, NC3 uses virtual agents to infiltrate paedophile networks on the Internet.

The Danish National Police find that the coordinated actions through arrests, press releases and awareness have an impact on the recruitment base, thus fewer persons will become cyber criminals in the future. Their experiences with infiltrating paedophile networks using virtual agents are mediocre, since they - because they are forbidden to upload paedophile material – have difficulties acting as paedophiles do.

7.2 Cooperation between the Danish authorities and Interpol

The National Cyber Crime Centre (NC3) is working well together with Interpol particularly in the area of sexual abuse of children. NC3 seems to be very active in the development of Interpol´s ICSE database.

7.3 Cooperation with third states

The National Cyber Crime Centre (NC3) cooperates with third countries on cybercrime investigations. There are special rules in the Danish Act on Processing of Personal Data that regulate the transfer of personal data to third countries.

It is the experience of the National Cyber Crime Centre (NC3) that Europol is a very efficient information conduit because of the organisation's ability to quickly distribute relevant information between Member States in relation to ongoing investigations. The ability to perform cross-checks in the Europol databases is of value to investigations - also in the area of cybercrime.

The above -mentioned points all came together in a case regarding the sexual abuse of children that is known in Danish as "*Randers sagen*", which involved perpetrators in Denmark, Sweden and the Netherlands (and outside the EU also in Australia).

However, the US have stationed a cyber crime prosecutor at Eurojust which will for sure enable a close contact with the US, should this be needed. Also cooperation with Switzerland and Norway is facilitated by their cooperation agreements with Eurojust.

7.4 Cooperation with private sector

- The Danish rules on data retention obliges the Danish CSPs to retain data regarding phone calls and text messages as well as subscriber information for a period of 12 months. Furthermore, the Danish CSPs are obliged by the Danish Administration of Justice Act to assist the police in setting up legal intercepts and to comply with court orders regarding disclosure of, for example, subscriber information.

- Danish hosting companies are required to comply with court orders regarding seizure of internet domains and *DK Hostmaster*, the company responsible for all .dk domains, is obliged to comply with court orders regarding disclosure of .dk domains. This gives the Danish Police the opportunity to take control over domains that are being used for criminal activities.

- If an international company has a local branch that is located in Denmark, this local branch is subject to the Danish rules on legal measures such as searches, seizes, intercepts and disclosure. There have been cases where a local branch of an international company has been subject to such legal measures. As a main rule, all assistance from public authorities or private companies of a foreign jurisdiction will be requested within the framework of mutual legal assistance.

However, with regard to some private service providers such as Facebook and Google, please refer to the answer under point 7.A.5.

In regard to the blocking of access, reference should also be made to the description of the *"Netfilter"- agreement* between the National Cyber Crime Centre (NC3), *Save the Children-Denmark* and most CSPs. Currently this arrangement does not cover any kind of illegal material other than the sexual abuse of children. However, NC3 in cooperation with the State Prosecutor for Serious Economic and International Crime intends to negotiate with the CSPs on extending this agreement to other kinds of illegal material.

Internet service providers are required to assist the Danish Police with the interception of communications, including the interception of telephone conversations, etc. (Section 786, Danish Administration of Justice Act). Furthermore, Internet service providers are required to assist the Danish Police with expedited preservation of computer data, including traffic data (Section 786a, Danish Administration of Justice Act).

The National Cyber Crime Centre (NC3) participates in the Europol - driven cooperation to investigate and prevent payment card fraud. The Danish Bankers Association is cooperating with similar institutions across Europe just as most of the larger Danish banks are part of an international financial institution. Through these networks the Danish financial sector receives and distributes information regarding border-crossing online card fraud.

7.5 Tools of international cooperation

7.5.1 Mutual Legal Assistance

Generally speaking, the Danish Police and Prosecution Service are well aware of the possibilities of receiving assistance from countries outside EU through mutual legal assistance.

The Danish Police said it makes use of MLA in relevant cases. Utilising this procedure requires the police to involve the Danish Prosecution Service as well.

In a case involving a phishing attack against the Danish banks in 2015 it was established that the attacks were carried out from a computer in another Member State. The investigation showed, however, that the computer in question was being remotely controlled from another computer located in a third Member State. The Danish Prosecution Service subsequently went to court and obtained relevant court orders in relation to the computer in the latter. A request for MLA was sent to the country in question, so far without result.

Also, Denmark receives requests for assistance from third countries. As an example, a case from Midt and Vestjyllands Police and Prosecution can be mentioned: the case concerned a DOS attack on Sea World in Florida where the alleged perpetrator was a Danish citizen. FBI asked for mutual legal assistance which was provided.

7.5.2 Mutual recognition instruments

Denmark did not provide information on the use of EU mutual recognition instruments in relation to prevention, investigation and prosecution of cybercrimes.

The Public Prosecution Service does not collate related figures. However, it is the impression of the latter that the instruments are used only rarely, if ever.

Denmark is not party to the European protection order.

7.5.3 Surrender/Extradition

The "computer-related crime" category referred to in the Framework Decision on the European arrest warrant is not defined in Danish law. Therefore, it is for the law enforcement authorities to assess whether the offence in question falls into this category.

The question of extradition is determined pursuant to the Danish Act on Extradition of Offenders, consolidated act no. 833 of 25 August 2005 with later amendments (the Extradition Act). Extradition is not conditional upon the existence of a treaty. Extradition is thus possible also where no agreement on extradition has been made between Denmark and the relevant foreign country.

Extradition of non-Danish nationals to countries outside the EU under the Extradition Act can take place if the offence is punishable under Danish law with imprisonment of one year or more (Extradition Act, art. 2 a). This requirement is satisfied in cybercrime cases, i.e. the acts mentioned in table 2 of the GENVAL questionnaire. If the extradition concerns enforcement of a judgment, the person must have been sentenced to four months' imprisonment or more in the requesting country or have been committed to a mental institution for a minimum of four months (Extradition Act, art. 3(2)).

A Danish national can be extradited to countries outside the EU if, for the last two years prior to the criminal act, he has had his residence in the country to which extradition is desired, and an act corresponding to the offence for which extradition is sought carries a maximum penalty of at least one year under Danish law, or the criminal act may entail a more severe penalty than imprisonment for 4 years under Danish law (Extradition Act, art. 2). The extradition must normally be based on an agreement with the other country, but if there is no such agreement the Director of Public Prosecutions may, anyhow, decide to extradite a Danish national based on the same requirements.

Special provisions apply within the EU in order for Denmark to comply with the Council Framework Decision on the European arrest warrant. The provisions in the Extradition Act concerning extradition from Denmark to another EU Member State on a European arrest warrant differ in several ways, e.g.:

- Dual criminality is not required in the case of extradition for a large number of offences specified in the "positive list", including child pornography and computer-related crime (Extradition Act, art. 10 a, no. 4 and 11).
- Danish nationals are basically extraditable in the same way as foreign nationals.
- Extradition cannot be refused on the grounds that the offences involved are political or that there is insufficient evidence to support the charge or conviction for an act for which extradition is sought.
- The issue of a European arrest warrant will in itself provide the basis on which to secure a person's arrest and extradition for prosecution or service of sentence.
- A European arrest warrant has to be dealt with within short time limits and the Act includes deadlines for processing a decision on extradition and for any judicial review of that decision.

Finally, special provisions apply with regard to extradition to Nordic countries. Extradition from Denmark to Finland, Iceland, Norway and Sweden for the purpose of criminal prosecution or execution of a sentence can take place on basis of a Nordic Arrest Warrant (NAW) that entered into force in October 2012. The competent authorities for issuing and executing an NAW are the local prosecution districts. Statistical information on the use of the NAW is not available. No districts have reported using the NAW in cybercrime cases.

Decisions on and requests for extradition are made by the Director of Public Prosecutions with regard to extradition to and from EU Member States and third countries (Extradition Act, art. 15 and 18b). The initiative to request extradition or to issue a European Arrest Warrant, will however, come from the Danish law enforcement authorities.

Decisions on and requests for extradition to the Nordic countries, i.e. Finland, Iceland, Norway or Sweden, based on a Nordic Arrest Warrant, are made by the Police Commissioner and handled by the relevant police district (Extradition Act, art. 18h). However, in cases where a request for extradition based on a Nordic Arrest Warrant and a request from a non-Nordic country are submitted at the same time, the Director of Public Prosecutions whether extradition can be granted.

European Arrest Warrants issued by the Director of Public Prosecutions are sent to the relevant Danish police and transmitted directly to the competent authorities within the EU through Interpol, and – to third countries – also through diplomatic channels.

Extradition cases are not separately registered on the basis of the type of offence. Therefore, the Director of Public Prosecutions is unable to provide statistics on the number of requests sent/received etc. as regards cybercrime acts.

Once a request for extradition is received by the Ministry of Justice, the Ministry makes a preliminary assessment of the request. Unless the request can be refused without further investigation, the Director of Public Prosecutions forwards the request to the competent police district for further investigation, which includes an interrogation of the wanted person. Once the investigation has finished, the police district forwards its findings to the Ministry of Justice. Based on the request for extradition and the findings of the police, the Ministry of Justice decides whether or not extradition can be granted.

Requests for extradition under the NAW are handled solely by the relevant police district.

Surrender must as a general rule take place as soon as possible. However, the person subject to a decision to extradite has the right to bring this decision before the courts within 3 days (Extradition Act, art. 17, 18e, 18i). Therefore, surrender cannot take place before the end of these 3 days unless the person concerned has renounced this right.

The Director of Public Prosecutions has issued guidelines on how to deal with requests for extradition. Requests for extradition must contain information on the time, place and nature of the act committed as well as on the applicable penalty clauses and information on whether an order for arrest or detention has been issued or whether a judgment has been passed (Extradition Act, art. 11, 18 a, and 18 g).

Provisional arrests in extradition cases can take place under the same conditions as in a national criminal case.

7.6 Conclusions

- **Denmark's membership of EUROPOL is in doubt and needs to be resolved as a matter of urgency; currently Denmark, while not a member of JCAT, does significantly contribute to EC3 and does engage with the various working groups at EC3 (EUCTF, ECTEG & EMPACT etc.);**

- **Cooperation of NC3 with EC3 is near flawless. All three operational focal points at EC3 (CSE, Cyber attacks and payment card fraud) reported excellent cooperation with NC3, as did NC3 itself;**

- **In relation to all types of serious crime, the assistance of the national desk and of Eurojust as such is highly appreciated by local authorities and considered as a substantial added value.**

- **Denmark uses the MLAT process and has encountered difficulties similar to those encountered other countries when using this process for investigative and evidential purposes; practitioners apparently don't use the mutual recognition instruments;**

- **The regional police North Zealand police are currently involved in a JIT with the Spanish authorities which indicates that Denmark is willing to engage in the JIT process and work with its international law enforcement partners in the fight against cybercrime.**

8 TRAINING, AWARENESS RAISING AND PREVENTION

8.1 Specific training

Law enforcement authorities

Cybercrime training is offered to different target groups.

The Danish Police College has overall responsibility for the provision of training to the Danish police, whereas the Director of Public Prosecutions is responsible for competence development within the prosecution service. However, the National Cyber Crime Centre (NC3) has a central role in the provision of cybercrime training for both police and the prosecution service. Close cooperation between the Director of Public Prosecutions, the Danish Police College, representatives from police districts and NC3 resulted in the "National Cybercrime Programme-level 1 and 2."

In December 2015, the "**National Cyber Crime programme – level 1**" was launched. It is a blended learning programme which consists of 7 hours of **e-learning** and 1½ days of case- based training. The objective of the programme is to give staff a basic technical understanding and knowledge of cybercrime and enable them to assess which information is relevant for the purpose of registering and handling reports of cybercrime correctly.

Furthermore, the programme's objective is to enable staff to make an initial assessment as to whether a reported cybercrime is a criminal offence and if initial and urgent investigative measures are needed in order to secure digital evidence.

Subjects covered are:

- Cybercrime and legal framework
- Digital items and evidence
- Basic networking and evidence
- Social media and communication
- Cybercrime prevention
- Case registration and management

The full programme is targeted at "front end" staff in districts and all "front end" staff are expected to complete the programme during 2016.

The 4 e-learning modules of the programme provide basic cybercrime training and will be compulsory in the basic curriculum of the Danish Police College, and will also be offered to investigators and prosecutors in general in 2016.

A "**National Cyber Crime Programme – level 2**" targeted at investigators and the Prosecution Service is under development and will be launched in October 2016. One- week "**Cyber Crime 2 specialist training**" was already offered to cybercrime specialists of the Prosecution Service in 2015.

The Danish Police College has since 2007 offered an "**IT investigator programme**" targeted at cybercrime specialist investigators in the districts. The programme is offered once or twice a year depending on demand. The programme consists of one e-learning module of 5 ECTS and two campuses, each of one week.

NC3 offers approximately once a year internal update courses in IT forensic tools (X-Ways, ENCASE, XRY, CellBright) for NC3 employees. NC3 has an ongoing focus on quality assurance in IT forensic methods, reporting, chain of custody etc.

Since 2010 the Danish Police College and the National Cyber Crime Centre (NC3) has cooperated with the Norwegian and Swedish Police on the **Nordic Computer Forensic Programme** (30 ECTS) offered by the Norwegian Police University College in Oslo. The programme is a combination of e-learning and campuses. It is a requirement for national IT forensic specialists of NC3 to complete the programme, and the programme has since 2014 been offered to specialists in the districts too.
This programme is offered twice a year.

Moreover, specific programmes on the sexual abuse of children are offered both to investigators in the districts and to the Prosecution Service approximately once a year.

ECTEG modules are generally regarded as specialist educational modules targeted at national specialists who have already completed the "NCFI programme" of the Norwegian Police University College. EGTEC modules are offered to specialists at NC3 and a few have completed a full master's programme at University College Dublin, which is partly based on ECTEG modules. NC3 has also contributed to the review and development of ECTEG modules.

CEPOL courses are disseminated through the Danish Police College and cybercrime-relevant courses are announced to NC3 employees and are regarded as supplementary courses.

Employees may complete, on an annual basis, external courses, seminars or conferences in accordance with individual competence development plans.

Centre of Excellence. The National Cyber Crime Centre (NC3) has a central role both in the curricula and concept development and provision of cybercrime training and can be compared to that of an external department of the Danish Police College.

NC3 has in close cooperation with the Danish Police College and the Director of Public Prosecutions developed "The National Cybercrime Programme "initially targeted at police districts. NC3 provides trainers for several other programmes offered by the Police College or the Director of Public Prosecution such as; the "IT investigator programme", "Sexual Abuse of Children" programmes, "Cyber Crime 2" for specialists in the judiciary and "First responds" as part of core curricula for police students.

Judges and Courts

It can be noted that the Danish Court Administration since 2010 has offered courses on various topics to judges on a voluntary basis, including courses in "Cybercrime".

Furthermore, the Prosecution Service and the National Cyber Crime Center (NC3) are considering which of the "Cyber Crime I" e-learning modules that are relevant to the courts and whether it is technically feasible to provide these modules to the judges. The Prosecution Service will invite judges to the course "Cyber Crime II" provided that the judges can access and have already completed the relevant "Cyber Crime I" e-learning modules which is a usual requirement for participating in "Cyber Crime II".

8.2 Awareness raising

The Danish National Police publish warnings about current cybercrime threats and trends on the Danish National Police's official Facebook and Twitter pages.

The National Cyber Crime Centre (NC3) offers lectures on different aspects of cybercrime, legal framework and crime prevention at the Danish Technical University.

NC3 also frequently raises awareness of current threats through Facebook and Twitter.

NC3 also participates in relevant television productions to raise awareness of certain types of cybercrime like *sextortion* and online fraud.

In cooperation with the Copenhagen district police, the Danish National Police have launched a co-creation project with numerous private partners e.g. to raise awareness of IT -related economic crime.

8.3 Prevention

8.3.1 National legislation/policy and other measures

NC3 has recently launched an initiative that aims to strengthen the cooperation between the Danish Police and the Danish business community. The initiative is loosely modelled on the FBI's *Infragard* programme.

The Danish Police are also working closely together with the NGO *Save the Children-Denmark* on the prevention of sexual abuse of children and the spreading of material containing such abuse.

The Danish "*Netfilter*" project is an example of a prevention activity that involves both the Danish Police and the Danish service providers.

8.3.2 Public Private Partnership (PPP)

Danish authorities underlined that National Cyber Crime Centre (NC3) has participated in public-private partnerships before it even had a name.

Co-operation with *Save the Children-Denmark* and the internet providers on DNS blocking of material on the internet of sexual abuse of children is the oldest example of this.

NC3 works closely together with the Danish Bankers Association and a private IT security company to combat bank fraud etc. Recently, NC3 has explored opportunities to engage in cooperation with a private credit risk information company to remedy the effects of identity theft in the form of online "fraud alerts" to let potential creditors and others know that a person has been a victim of identity theft. This has however - given the prerequisites - not proven to be a possibility since the co-operation had to be open to other private competitors in the market too.

NC3 has also initiated a public-private partnership "NC3skyt" with private companies to prepare society to prevent and respond to the exploitation of security vulnerabilities through confidential exchange of information among members and education of infrastructure stakeholders. **The initiative is inspired by FBI´s *INFRAGARD***.

8.4 Conclusions

- **The overall structure of Danish cybercrime awareness raising and training to LEA practitioners is to be considered as a very good practice;**

- **In particular, the e-learning modules developed by Danish authorities for police and prosecution practitioners is an excellent format which may inspire other Member States; even at national level, this material could be offered to the Danish Judiciary for awareness and training purposes;**

- **The competent Danish authorities in general, the Centre for Cybersecurity and NC3 in particular, are well involved in public-private partnerships;**

- **Other awareness and prevention initiatives appear valuable also;**

- **Cybercrime training was offered to judges on a voluntary basis in contrast to other parties. Training should be strongly encouraged, even if not mandatory for them as it is for policemen and prosecutors;**

9 FINAL REMARKS AND RECOMMENDATIONS

9.1. Suggestions from Denmark

As regards the situation at national level the Danish authorities identified further needs regarding training of personnel in the police districts, innovation both in new technologies and investigative measures, and legislation. A plan for further developments is however in place and some of it has already been implemented.

As regards the situation in the European Union:
In the light of the technological progress, in particular in transmission and storage of data and secure distribution, the Danish National Police do not consider the existing EU legal framework sufficient for the investigation and prosecution of cybercrime. The sophistication of some of the more extensive cases is increasing, thus demanding highly specialised technical investigative skills as well as effective and smooth international legislative cooperation.

Therefore, **the Danish National Police support streamlining of the European regulation in the areas of**
(i) **harmonisation of the regulation of investigative measures**
(ii) **harmonisation of cybercrime laws to introduce criminal sanctions at the same level** in order to ensure the enforcement of mutual legal assistance, which will enable Member States to enforce most requests on mutual legal assistance in this area.

The competent Danish authorities said that the prerequisite for being able to request a certain investigative measure though mutual legal assistance is very often **access to information on data retention** (which IP address was connected to which IP address, when, for how long, and where was the IP address located). If this information is not available, most investigations stop here, and law enforcement authorities need, more than ever, to be able to access these data **not only nationally but also in other Member States**.

The Danish National Police also believe that the **EU needs to rethink investigative jurisdiction when it comes to searches on the internet**. The physical positions of the servers are irrelevant to the users, and we need to accept cyberspace as a place on its own, but at the same time part of the investigative jurisdiction of one Member State, but not necessarily also two or more Member States.

The mutual recognition of results of searches (examination of servers or cloud accounts without relying on the service provider) in cybercrime cases, which can be conducted from the investigating state without technical assistance from the state where the server is located, will also provide law enforcement with a very effective tool, thereby avoiding the loss of volatile evidence.

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 Denmark was able to satisfactorily review the system in this Member State.

Denmark should conduct a follow-up to 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 fit to make a number of suggestions for the attention of the Danish 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 Denmark

1. **Denmark should consider adapting its current statistical approach in a suitable way to better reflect the current and future cybercrime situation (see also Rec. n. 12);**

2. **Denmark should consider improving the efficiency and consistency of its case management system, which would include not only the names of suspects and victims, but also some operational information and investigative leads (e.g. phone numbers, IP addresses, IBAN numbers, DNA profiles special *modus operandi* etc.) and would provide for the early and automated detection of parallel proceedings;**

3. **Denmark should consider the creation of a real-time sharing of information and intelligence sharing with the Danish Bankers Association;**

4. **Danish authorities are encouraged to take the necessary steps to allow the continued participation of Denmark in Europol/EC3 activities – including considering seconding a full-time resource to the JCAT;**

5. **While fully respecting the independence of courts and judges, the training material developed for the Prosecution Service and NC3 should be made available to the Administration of the Judiciary for training purposes;**

6. **Denmark should continue to promote "*best in class*" management practices to continue attracting and retain appropriately qualified employees in the respective competent services;**

7. Danish authorities should continue and expand the exchange of knowledge, experience and tools with EUROPOL/EC3 (e.g. via SPACE) and other relevant entities;

8. The current situation of Denmark with regard to traffic data retention requires swift resolution to overcome legal uncertainty for practitioners; Denmark should swiftly adopt and implement the new legislation in preparation.

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

9. The European Union and its institutions should more actively promote the identification and expansion of Member States' best practices, including toolsets utilised in the fight against cybercrime;

10. Inspired by the Danish case management system (common to the police and prosecution service), the European Union and its institutions are advised to consider whether Member States would benefit from Eurojust and Europol developing a case management system allowing for the capture of common fields;

11. The European Union and its institutions should proactively encourage the use of open-source tools and material by Member States competent authorities with a view to facilitate the sharing of knowledge;

12. Member States should develop well-designed statistics reflecting correctly the reality of the cybercrime phenomenon; this would be important for checking the effectiveness of legal and investigative measures in place and for responding in a more agile and efficient manner;

13. **Member States should examine several areas of good practice in Denmark which could potentially be a source of inspiration, including:**
    - **the Danish management approach, (a long-term approach that seeks to achieve small, incremental changes in processes in order to improve efficiency and quality, and to regularly review progress) - which seems to be of great value for law enforcement authorities;**
    - **The NC3 "Innovation team", using skilled software expertise to utilise open-source software and build bespoke tools;**
    - **NC3's recruitment model as a whole, consisting of a 50 / 50 mix of police investigators and civilian IT engineers, thereby ensuring an optimal mix of technical and investigation skills for tackling cybercrime;**
    - **The active ongoing cooperation between the various competent entities; as a good example of that, the Danish Centre for Cybersecurity providing on request specific technical support for NC3 investigations;**
    - **The investigation procedure "flow" as practised in the police district of North Zealand, composed of a front-end office (collecting, documenting and sorting reports coming from all sources) and a visitation centre (reviewing all reports and identifying those which will be investigated at the local police stations);**

9.2.3 Recommendations to Eurojust/Europol/ENISA and other agencies/bodies

14. **Europol should consider the possibilities for facilitating the sharing of forensic knowledge and tools at NC3 with EC3 and the forensic capabilities of other Member States;**

15. **EUROPOL should encourage and facilitate the setting up of a framework under which tools can be exchanged or jointly used by Member States' competent authorities;**

16. **Both CEPOL and EJTN should examine the e-learning approach developed by the Danish authorities for the spreading of basic cybercrime awareness and knowledge to competent practitioners throughout the Member States;**

17. **EUROJUST should, with the support of EC3 on the one hand and the JIT Network on the other, proactively identify suitable cases where a JIT would be of assistance in the area of cybercrime; in particular, it should encourage those Member States that haven't used JIT before to make use of this process;**

18. **ENISA should consider ways to promote/expand the CERT model as employed in Denmark.**

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

The Danish Authorities are invited to check and complete the following:

Tuesday 15 March 2016

10.00-11.00 Ministry of Justice – "Welcome and introductory meeting" - *Slotsholmsgade 10, Copenhagen*

13.00-16.00 Director of Public Prosecutions - *Rigsadvokaten, Frederiksholms Kanal 16, Copenhagen*

Wednesday 16 March 2016

9.30-16.00 The Danish National Police, National Cyber Crime Center (NC3)*, Ejby Industrivej 125-135, Glostrup*

Thursday 17 March 2016

9.30-12.00 North Zealand Police - *Prøvestensvej 1, Elsinore*

14.00-16.00 Danish Defence Intelligence Service, Centre for Cyber Security - *Kastellet 30, Copenhagen*

Friday 18 March 2016

9.30-11.00 Ministry of Justice – "Debriefing meeting"

ANNEX B: PERSONS INTERVIEWED/MET

(The Danish Authorities are invited to check and complete the following list of attendees)

Ministry of Justice

Deputy Permanent Secretary Pernille Breinholdt Mikkelsen
Deputy Head of Division Michael de Thurah
Deputy Head of Division Nicolai Winther
Head of Section Michael Schaumburg-Müller
Head of Section Mark Orberg

The Director of Public Prosecutions

Assistant Deputy Director Alessandra Giraldi
Assistant Deputy Director Pernille Langermann

Deputy Chief Prosecutor Karina Nørgaard

Chief of Training and Development Holger Smith
Prosecutor Henriette Reinholdt

The Danish National Police, National Cyber Crime Center

Head of National Cyber Crime Center Kim Aarenstrup
Head of Innovation and Technology Karsten Brinkmann Pedersen

General Counsel Kate Jacquerot

Legal Adviser Jesper Hagen

Superintendent Flemming Kjærside
Superintendent Sonny Olesen

Senior Consultant Susan Varmer

North Zealand Police

Senior Chief Prosecutor Ida Sørensen

Centre for Cyber Security

Head of Policy Department Thomas Kristmar

Chief Legal Advisor Jørgen Breddam
Training and Exercise Peter Knøster

ANNEX C: LIST OF ABBREVIATIONS/GLOSSARY OF TERMS

LIST OF ACRONYMS, ABBREVIATIONS AND TERMS	ACRONYM IN DANISH OR OTHER ORIGINAL LANGUAGE	FULL NAME IN DANISH OR ORIGINAL LANGUAGE	ENGLISH
CEPOL			European Police College
CERT			Computer Emergency Response Team
CFCS			Centre for Cyber Security under the Danish Ministry of Defence
CMS			Case Management System
CoE			Council of Europe
CSA			Child Sexual Exploitation
DDIS			Danish Defence Intelligence Service
DPP		*Rigsadvokaten*	Director of Public Prosecution
ECJ			European Union's Court of Justice
EC3			European Cybercrime Centre
EGTEC			European Cybercrime Training and Education Group
EJN			European Judicial Network
EJTN			European Judicial Training Network
EMPACT			European Multidisciplinary Platform Against Criminal Threats
ENISA			European Union Agency for Network and Information Security
EUCTF			European Union Cybercrime Task Force
EUROJUST			European Unit Judicial Cooperation Unit

LIST OF ACRONYMS, ABBREVIATIONS AND TERMS	ACRONYM IN DANISH OR OTHER ORIGINAL LANGUAGE	FULL NAME IN DANISH OR ORIGINAL LANGUAGE	ENGLISH
EUROPOL			European Police Office
FBI			United States Federal Bureau of Investigations
GENVAL			Working Party on General Matters including Evaluations
ICSE			Interpol's International Child Sexual Exploitation Database
ICT			Information and Communications Technology
INTERPOL			International Criminal Police Organization
IOCTA			Internet Organised Crime Threat Assessment
IOT			Internet of Things
IP			Internet Protocol
IPR			Intellectual Property Rights
IT			Information Technology
J-CAT			Joint Cybercrime Action Task Force
JIT			Joint Investigation Team
JHA			Justice and Home Affairs
LEA			Law Enforcement Authorities
MLA			Mutual Legal Assistance
MLAT			Mutual Legal Assistance Treaty
MoJ		*Justitsministeriet*	Ministry of Justice
NAW			Nordic Arrest Warrant
NC3		*Nationalt Cyber Crime Center*	Danish National Cybercrime Center
NGO			Non-Governmental Organisation

LIST OF ACRONYMS, ABBREVIATIONS AND TERMS	ACRONYM IN DANISH OR OTHER ORIGINAL LANGUAGE	FULL NAME IN DANISH OR ORIGINAL LANGUAGE	ENGLISH
PET	PET		Danish Security and Intelligence Service
NOST			National Operating Staff - Danish coordinated multidisciplinary mechanism for serious cyberattacks
PPP			Public Private Partnership
SCADA			Supervisory Control and Data Acquisition
SPACE			EC3's restricted virtual platform
SPOC			Single Point of Contact
TOR			The Onion Router
VPN			Virtual Private Network
VPS			Virtual Private Server