Council of the
European Union

Brussels, 26 June 2015
(OR. en)

7587/15
DCL 1

GENVAL 8
CYBER 22

DECLASSIFICATION

of document:	7587/15 RESTREINT UE/EU RESTRICTED
dated:	15 May 2015
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 the Netherlands

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, 15 April 2015
(OR. en)

7587/15

RESTREINT UE/EU RESTRICTED

GENVAL 8
CYBER 22

REPORT

From:	General Secretariat of the Council
To:	Delegations
Subject:	Evaluation report on the seventh round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating Cybercrime" - Report on the Netherlands

EVALUATION REPORT ON THE SEVENTH ROUND OF MUTUAL EVALUATIONS

"The practical implementation and operation of European policies on prevention and combating Cybercrime"

REPORT ON THE NETHERLANDS

Table of Contents

1. EXECUTIVE SUMMARY

The evaluation visit was very well organised and prepared by the Dutch authorities. The selection of authorities visited and participants met was appropriate. The evaluation team particularly appreciated the welcome by the Ministry of Security and Justice and its coordinating role throughout the whole visit. The evaluators were given the opportunity to talk with a large number of professionals from the Dutch central authorities as well as representatives of the judiciary, police and private sector.

The Netherlands is highly digitised, both economically and socially. The Netherlands continues to build the necessary knowledge, capacity and legislation to enhance cyber security and fight cybercrime since this process is not an easy one and requires many resources and the involvement of the most important stakeholders from both the public and private sector.

The Netherlands has set up a strategy and priorities to combat cybercrime which are clearly laid out in the National Cyber Security Strategy (NCSS2). It provides strategic guidance at tactical and operational levels, such as on strengthening national and international legislation, tackling cybercrime, prevention and awareness, improving cooperation with all relevant national and international parties and capacity building. All those aims should be reached while respecting fundamental rights such as freedom of speech and privacy.

There is a consistent legal framework in place in the Netherlands, at both substantive and procedural level. The implementation of Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA is to be finalised in 2015 and should further improve Dutch law.

From a practical point of view, fulfilment of the Dutch strategy on cybercrime is carried out in different fields, including participation in the Virtual Global Task Force, the establishment of a liaison officer at the Interpol Global Complex for Innovation in Singapore, a planned exchange of personnel and knowledge with Europol/EC3, the stationing of two flexible liaison officers in South America and the Philippines to deal with matters relating to online child sexual abuse, and valuable work on the three cyber sub-priorities (online card fraud, online child sexual exploitation and cyber attacks) of the EU Policy Cycle to tackle organised and serious international crime.

These goals are also achieved via public and private partnership as well as through raising public awareness. There are many initiatives worth mentioning. However, The National Cyber Security Centre (NCSC), located within the Ministry of Security and Justice, focuses on the vital sectors of the country and is a flagship in that regard. As a result, its key partners from the private sector are energy companies, and the telecommunications and financial sectors. They will be obliged to notify the NCSC of any cyber breaches that may occur. However, there is no penalty for failing to notify the NCSC, although whether or not a company reported a breach would be taken into account by the relevant authorities looking at the case (data protection supervisor, bank supervisory authority, etc.). Therefore, in the opinion of the evaluators the fact that it is not mandatory to report massive attacks against vital infrastructures run by private companies leaves the power of deciding whether or not to fight criminals and bring them to justice in the hands of the private sector.

The other successful initiative is the ECTF, which was formed to combat digital banking fraud more effectively, specifically phishing and banking malware.

The Netherlands also prioritises the fight against cybercrime and the reaction on attacks on or disruption of information systems by strengthening its current capabilities in investigation and prosecution. The investigation of major cybercrime cases at national level is coordinated by a core triangle consisting of the National High Tech Crime Unit of the National Police, the National Cyber Security Centre (NCSC) and the National Public Prosecutor's Office, which cooperate smoothly and efficiently. Actual investigations into crime are undertaken by the police and the Public Prosecution Service.

The police and the Public Prosecution Service have liaison officers in the NCSC. Investigation of cybercrime at the national level is supplemented by the structure for fighting cybercrime at regional police level. These (teams in regional units of the police), in cooperation with the Dutch Forensic Institute (NFI) and Public Prosecutor's Office, are involved in the majority of cybercrime cases. However, according to the information gathered during the on-site visit, there are discrepancies between the operational means of the different regional authorities. This should be rectified, particularly because cases falling under the competence of regional authorities are those that more closely affect unprotected citizens and are to some extent more visible to the community.

On the other hand, the Dutch practise of combining the possibilities offered by private companies (such as ISPs and social media companies), public entities (e.g. the Ministry of Security and Justice and specialised units dealing exclusively with online child sexual abuse) and campaigns addressed to the general public in order to efficiently combat online child sexual abuse, is in the opinion of the evaluation team worth following.

The Netherlands demonstrates exemplary international cooperation on cybercrime within Europol/EC3 and Eurojust, as well as with Interpol and other third parties. Knowledge of the possibilities resulting from that cooperation seems to be widespread at national level. Nonetheless, the regional police and judiciary need to be further trained. An obligatory cybercrime training programme at least for those dealing with cybercrime cases could cover the gap in communication and mutual understanding between cybercrime investigators, prosecutors and judges (initiatives such as the Expertise Centre on Cybercrime at the Appeal Court of the Hague could be of broader use). A binding and common definition of cybercrime for statistical purposes could also be helpful.

Although the overall assessment of cybercrime in the Netherlands is not comprehensive due to the lack of detailed, standardised and comprehensive statistics on investigations, prosecutions, convictions and reported incidents related to cybercrime, the evaluation team appreciated the way the system works. The strategy in the Netherlands is clearly to make the country unattractive to cyber criminals. Considering the significant role the Netherlands plays in providing infrastructure and hosting services, the level of effort and resources the country is investing in the fight against cybercrime, and the effectiveness of that investment, the opinion of the evaluators is decidedly positive.

2. INTRODUCTION

Following the adoption of Joint Action 97/827/JHA of 5 December 1997[1], a mechanism was established for evaluating the application and implementation at national level of international undertakings in the fight against organised crime. In line with Article 2 of the Joint Action, on 3 October 2013 the Working Party on General Matters including Evaluations (GENVAL) decided that the seventh round of mutual evaluations should be devoted to the practical implementation and operation of the European polices on preventing and combating cybercrime.

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, online child sexual abuse/pornography 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 and replacing Council Framework Decision 2004/68/JHA[2] (transposition deadline 18 December 2013), and Directive 2013/40/EU[3] on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (transposition deadline 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] anticipated the swift ratification of the Council of Europe Convention on Cybercrime (the Budapest Convention)[5] of 23 November 2001 by all Member States and emphasised in their preamble that "the EU does not call for the creation of new international legal instruments for cyber issues". The Convention is supplemented by a Protocol on acts of xenophobia and racism committed through computer systems[6].

Experience from past evaluations shows that Member States will be in different positions regarding the implementation of the relevant legal instruments, and the current evaluation process could also provide useful input to Member States that may not have implemented all aspects of the various instruments. Nonetheless, the evaluation aims to be broad and interdisciplinary and not to focus solely on the implementation of various instruments relating to fighting cybercrime, but also 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 those organisations is channelled to the appropriate police and social services. The evaluation focuses on implementing national policies with regard to the suppression of cyber attacks, fraud and child pornography. The evaluation also covers operational practices in the Member States with regard to international cooperation and the support offered to people who fall victim to cybercrime.

[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 January 2003, entered into force on 1 March 2006.

The order of visits to the Member States was adopted by GENVAL on 1 April 2014. The Netherlands is the second 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 to delegations from the Chairman of GENVAL on 28 January 2014.

The evaluation teams consist of three national experts, supported by two staff from the General Secretariat of the Council and observers. For the seventh round of mutual evaluations, GENVAL agreed with the 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 the Netherlands were Mr Attila Kökényesi-Bartos (Hungary), Mr Wolfgang Bär (Germany) and Mr Ivan Bacigál (Slovakia). The observers were also present: Mr Michele Socco (Commission), Mr Lionel Ferette (ENISA), Mr José Eduardo Guerra (Eurojust) and Mr Philipp Amann (Europol/EC3), together with Mr Francisco Rodríguez Rosales and Mr Sławomir Buczma from the General Secretariat of the Council.

This report was prepared by the expert team with the assistance of the General Secretariat of the Council, based on findings arising from the evaluation visit that took place in the Netherlands between 17 and 21 November 2014, and on the detailed replies from the Dutch to the evaluation questionnaire, together with their detailed answers to ensuing follow-up questions.

3. GENERAL MATTERS AND STRUCTURES

3.1. National cyber security strategy

In 2011 the Dutch Government launched a National Cyber Security Strategy (NCSS), with input from a wide range of public and private parties, knowledge institutions and civil society organisations. On 28 October 2013 the Minister of Security and Justice presented the second edition of the National Cyber Security Strategy ("NCSS2: From awareness to capability").

The intention of the Dutch authorities is to provide safe and reliable ICT and to protect an open, free internet since society's growing dependence on ICT makes it increasingly vulnerable to the misuse and disruption of ICT systems. The ambitions in the NCSS2 are based on strategic objectives that serve as guidelines for the 2014-2016 Action Program. Tackling cybercrime is deemed to be one of these objectives. Cybercrime is considered to be a frequently occurring and increasing threat for all citizens and organisations. In order to offer adequate protection from cybercrime, the NCSS2 prioritises the fight against cybercrime by:

1. updating and strengthening (international) criminal legislation (including the Computer Crime Act III),
2. improving cooperation with Europol/EC3 by exchanging knowledge and personnel,
3. including the strengthening of investigation and prosecution of cybercrime as a subject in the discussion about new national policy objectives for the police in the common security agenda (the current subjects lapsed on 1 January 2015) for the Dutch national police,
4. strengthening the fight against cybercrime in the financial sector through cooperation, including with the private sector,
5. increasing the number of international investigations to 20 in 2014,
6. supervising the link to the investigation and prosecution services in the digitisation of crime,
7. strengthening the intake and registration process for cybercrimes reported to the police.

3.2. National priorities with regard to cybercrime

The National Cyber Security Strategy (NCSS2) describes the overall national priorities for cyber security. Various actions based on the other objectives of the NCSS2, alongside tackling cybercrime, can be regarded as actions aimed at prevention, capacity building in both the public and private domain, and raising public awareness. The following actions are expected to be undertaken:

Prevention

The strategy contains many specific actions to improve the prevention of cybercrime. These actions also reduce vulnerabilities to cybercrime. They include improving resilience to cyber attacks, protecting vital interests (and infrastructure), investment in secure ICT products and services, and investing in knowledge and know-how in the field of cyber security.

Legislation

Updating and strengthening legislation (including the Criminal Code) is vital for the strengthening of an international approach to cybercrime. The Minister of Security and Justice is preparing a new bill of law on cybercrime (The computer Crime Act III) which is expected to be sent to the Parliament in 2015. The new law aims to take measures to address the rapid developments in the field of technology, the internet and cybercrime, in order to undo data encryption, deal with illegal actions on the internet or fight online child pornography. The proposed bill will introduce legislation on the following:

- Remote investigations of the computers of criminals within Dutch jurisdiction by the police and judicial authorities, including where necessary the ability to copy data or make the data inaccessible. It concerns the so-called "investigation into an automated work", which provides investigators with the authority to perform various investigative actions, subject to stringent conditions, when investigating serious offences. This may involve cross-border access to data.

- The possibility of obliging persons suspected of possessing and disseminating child pornography or of terrorist activities to cooperate in opening encrypted files on their computer. The public prosecutor will then issue a so-called decryption order to the suspect. The police and judicial authorities will then obtain access to protected data. However, there are stringent safeguards, including prior court review. Ignoring a decryption order from the public prosecutor will be punishable by a prison sentence.
- The criminalisation of handling stolen computer data. In doing so, the minister intends to prevent third parties from receiving stolen information from hacked computers and subsequently placing it on the internet.
- The criminalisation of repeated fraud in online markets.
- The "grooming" of children, making it possible for such crimes to be investigated by undercover police officers.

In addition, the Netherlands is also in the progress of implementing Directive 2013/40/EU on attacks on information systems.

Capacity building & training

In past years, the Netherlands has invested in building capacity for law enforcement and the criminal courts. At the national level, the police have created a special High Tech Crime Unit for investigating high-end cybercrime. The national support unit will be strengthened by digital experts to support investigations of cybercrimes that are less high tech, and to support the gathering of digital evidence. The regional police units will create digital expert units for the same kind of support at the local level.

Public awareness

Both public and private partners are working on raising awareness and providing information to the public on how to improve cyber security and prevent cybercrime. The National Cyber Security Centre (NCSC) of the Ministry of Security and Justice routinely provides security advice on incidents and specific vulnerabilities (www.ncsc.nl and www.waarschuwingdienst.nl). In a few high-profile cybercrime cases the National Police and the Public Prosecutor's Office have given the public advice on preventing certain types of cybercrime.

The National Hotline for Internet Fraud is a collaboration between the National Police, the Public Prosecutor's Office and the online market www.marktplaats.nl. It provides a facility for internet customers to check whether an internet trader has been reported as unreliable, and to report online trade fraud to the police.

Public and private partners are working together in the Digibewust initiative to improve overall security awareness. Digibewust is a collaboration between the Ministry of Economic Affairs, the European Commission and private partners like KPN, UPC, IBM and the Dutch Banking Association.

Another example of a private initiative was the campaign "Hang op, klik weg, bel uw bank" ("Hang up, click away, call your bank") launched by the Dutch Banking Association (Nederlandse Vereniging van Banken, NVB) to improve online self-defence for customers. It ran until the end of 2014.

International cooperation

The Netherlands actively pursues national and international alliances. Most larger cybercrime cases involve more than one country. The police and Public Prosecutor's Office work together with international partner organisations on a regular basis to handle international cases and to gather evidence. Updating and strengthening (international) criminal legislation (including the Computer Crime Act III) and improving cooperation with Europol/EC3 by exchanging knowledge and personnel are two priorities of the NCSS2. The National Police actively supports Europol/EC3.

The Netherlands also supports the development of the Interpol Global Complex for Innovation in Singapore. The Public Prosecutor's Office, with help from Eurojust and the International Association of Prosecutors, has taken the initiative to strengthen the international cooperation of public prosecutors in cybercrime cases. The Netherlands actively participates in international meetings and related activities, such as the Committee of Contracting States of the Council of Europe's Convention on Cybercrime, the "EU policy cycle on organised crime", and the discussions in the UNODC about a UN treaty in the area of cybercrime. The Netherlands has also invested in knowledge and expertise, and participates in joint investigations.

EU cybercrime priority

The activities to improve the fight against cybercrime largely coincide with the goals of the EU cybercrime priority. For example, online card fraud is one of the issues tackled by cooperation between the financial sector, the National Police and the Public Prosecutor's Office. Together they share information on specific cases and on new criminal activities and methods. Geo-blocking payment cards has reduced online card fraud substantially.

3.3. Statistics on cybercrime

The Ministry of Security and Justice publishes an annual Cyber Security Assessment Netherlands (CSAN) in close collaboration with public and private parties. The CSAN is published for policymakers in government and vital economic sectors, and provides insights into developments and assessments of possible measures for increasing the digital resilience of the Netherlands. The CSAN is produced in cooperation with all ministries, the intelligence and security services, the Defence CERT (DefCERT), the National Police, the Public Prosecutor's Office, the tax service, members of ISACs, scientific institutions and universities, and other cyber security experts. In the new CSAN, cybercrime and cyber espionage are assessed as the largest threats in cyberspace.

The Ministry of Security and Justice also publishes a Threat Assessment on organised crime biannually. The assessment illustrates the great influence of modern ICT on society and thus also on organised crime, where it affects its appearance and methods. This has resulted in an increase in the volume and seriousness of high-tech crimes (hacking, botnets, the spread of malware), as well as the use of ICT in more traditional types of crime, such as fraud.

Furthermore, the Central Bureau for Statistics (CBS) published the yearly Security Monitor in March 2014, focusing on victims of several types of crime. Cybercrime is one of the topics. The Security Monitor uses a very broad definition of cybercrime, including cyber bullying and threats through social media. In 2013, 12% of the inhabitants of the Netherlands over 15 years of age had been victims of some sort of cybercrime. About half of them had been victims of hacking. A quarter

of them had been bullied through the internet and another quarter had been the victims of online trade fraud. Young people, who are relatively active on the internet, are falling victim more often. Of all respondents aged 15-25, almost 20 % had been victims of cybercrime. For respondents aged 25-45, the figure was 15 %. 20 % of all respondents reported having been the victim of a crime in 2013. The document concludes that hacking is the most commonly occurring form of cybercrime, skimming is decreasing and online trade fraud is increasing.

The police and Public Prosecutor's Office report regularly on the incidence of investigation reports sent to the prosecutor and on prosecutions of cybercrime linked to specific articles of the Dutch Criminal Code. In 2013 the specialised National High Tech Crime Unit of the police conducted nine large investigations and responded to six international assistance requests. Small investigations are not included. Other criminal acts committed with the help of ICT are not counted separately. In previous years, the target for the National High Tech Crime Unit consisted only of large investigations, and therefore only they have been counted.

Having noted that, the evaluation team realised that there are no detailed, standardised and comprehensive statistics at the national level showing all the threats and incidents that have occurred with regard to cyber attacks on a yearly basis. Specifically, it is not known how many incidents in total were not registered due to the application of the principle of opportunity, and as a consequence did not give rise to criminal investigation. Also, there is no figure available for cybercrime as a percentage of overall criminality. The Dutch authorities report that although the Security Monitor provides several figures based on victim reporting, it is difficult to compare these data due to the broad definition of cybercrime used by different people.

In the evaluators' view, the lack of statistics makes it difficult to get a clear view of the progress of cyber criminality on the one hand, and on the other of the effectiveness of combating this phenomenon. Some of the incidents registered may seem small at first glance but turn out to be bigger after a more in-depth evaluation. Therefore, the evaluation team considers that collecting overall statistics could make detailed analysis possible and so help build a clearer picture of the effectiveness of the legal system in protecting the private interests of citizens victimised by cybercrime.

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

The police have a specific capacity for cybercrime and the collection of digital evidence. The specialised National High Tech Crime Unit will have expanded to 119 full-time employees at the end of 2014. National and regional digital support centres are being set up. Moreover, the Minister of Security and Justice provides the police with a dedicated budget of EUR 13.8 million a year for specific improvements in preventing and fighting cybercrime, digitalised crime and the enhancement of digital investigations. The Public Prosecutor's Office has appointed specialist cybercrime prosecutors in every region, and a national public prosecutor for cybercrime.

The Dutch authorities reported two projects currently being run under the ISEC fund:

A. ITOM (Illegal Trade on Online Marketplaces)

- Project ITOM[7] is aimed at combating illegal trade on hidden online marketplaces. The goal is to initiate multidisciplinary initiatives – by law enforcement and other public and private parties – in each of the EU Member States, to share knowledge, expertise, information and intelligence, and to coordinate these interventions where possible. The project is coordinated by the Dutch national Public Prosecutor's Office. The goals of the ITOM project relate to understanding illegal trade on the internet, supporting cooperation between law enforcement agencies, coordinating multidisciplinary intervention(s), evaluating the multidisciplinary intervention(s) and sharing knowledge and expertise.

B. "in-4-mation"

Dutch law enforcement organisations cooperate in the European "in-4-mation" project, in which the participating countries' national databases of confiscated and confirmed child sexual abuse images are connected to each other. This "in-4-mation" database has not been finalised, but the Netherlands is ahead of schedule and currently implementing it.

3.5 Conclusions

- There is a comprehensive national cyber security strategy in place in the Netherlands. In 2011 the Dutch Government launched a National Cyber Security Strategy (NCSS) which was developed by the NCSS2 in 2013.

[7] Supported by the Portuguese Procuradoria-Geral da República, the European Cybercrime Centre (EC3) at Europol, Eurojust, the National Crime Agency, the German Generalstaatsanwaltschaft Frankfurt am Main and Celle, and the Dutch National Police and Prosecutor's Office.

- The NCSS is based on a wide range of public and private parties, knowledge institutions, and civil society organisations. It very comprehensively covers the most important aspects to be taken into account when tackling cybercrime, such as prevention, legislation, capacity building and training, public awareness, international cooperation and the EU cybercrime priority.

- The Netherlands has clearly defined its national priorities with regard to handling cybercrime. They were established in 2011 and are being continuously developed. The recently adopted NCSS2 includes an Action Programme for 2014-2016 which sets out objectives for the coming years, one of which is tackling cybercrime, and comprises a number of actions relating to fighting against cybercrime in the financial sector through cooperation, expanding the number of international investigations and improving cooperation with Europol/EC3 by exchanging knowledge and personnel.

- In the opinion of the evaluators the strategy, along with the defined priorities developed in the Netherlands, is a solid basis on which to fight effectively against cybercrime. Close cooperation between the private sector and public organisations creates a unique opportunity to involve a wide range of entities working together. This should be regarded as best practice.

- One of the main achievements of the NCSS is the Cyber Security Assessment Netherlands (CSAN), which is the main central reporting and information point for IT threats and security incidents.

- Since cybercrime can have lots of forms and is not always the predominant factor in criminal activity, finding a way to have detailed, standardised and comprehensive statistics on cybercrime that would make it possible to check overall cybercrime figures (reported incidents, notifications provided by victims, number of decisions not to investigate certain types of cybercrime, number of investigations carried out, number of prosecutions and convictions related to cybercrime) could make it easier to tackle cybercrime properly and take appropriate follow-up action. Such analysis would also give a clearer picture of the effectiveness of the legal system in protecting the private interests of citizens victimised by cybercrime. This problem may also be related to the lack of a common definition of cybercrime.

- The evaluation team found that the various stakeholders (such as prosecutors or police officers) used different interpretations of cybercrime.

- The Dutch authorities consider cybercrime to be a serious threat to the state and to society. Therefore, there is a wide range of people involved in combating cyber criminality. On the one hand, the public sector is deeply committed to tackling this phenomenon. The Ministry of Security and Justice is involved in providing a comprehensive approach at the central level. Police resources (human and financial) have also been continuously strengthened. On the other hand, cooperation with the private sector seems to be effective and promising.

4. NATIONAL STRUCTURES

4.1. Judiciary (prosecution and courts)

4.1.1 Internal structure

Acts of cybercrime are investigated, prosecuted and adjudicated under the same judicial framework as “other” criminal acts.

The Public Prosecutor’s Office and courts make up the judiciary. The Public Prosecutor’s Office is the only body that can decide to prosecute someone. The public prosecutor recommends an appropriate sentence, after which the court gives its judgment. Convicted persons and public prosecutors are entitled to lodge appeals if they disagree with a district court’s judgment, in which event the Public Prosecutor’s Office at the appeal court prosecutes the case anew. This is its main function. In appeal proceedings, new investigations may be carried out and new witnesses or experts may be heard. The appeal court then hands down a new ruling. In most cases it is possible to contest the court of appeal’s decision by appealing in cassation to the Supreme Court of the Netherlands.

Prosecutors

The Public Prosecution Service decides who has to appear before a court and on what charge. Its field of work is criminal law. The Public Prosecution Service’s main tasks are:

- investigating criminal offences,
- prosecuting offenders,
- supervising the enforcement of sentences.

There are ten districts in the judiciary that coincide with the geographical span of control of the regional units of the police. The Public Prosecution Service has offices – the Public Prosecutor's Office – in every district. Each of the offices is under the authority of a chief public prosecutor, who ensures that the policy of the Public Prosecution Service is implemented in their district. For every district of the Public Prosecutor's Office there is a specialised cybercrime officer and specialised prosecutor's assistants. In total there are eight regional cybercrime officers and ten regional prosecutor's assistants, as well as four cybercrime officers and three prosecutor's assistants at the national level.

In addition to the district offices, there are the National Public Prosecutors' Office (*Landelijk Parket*) and the National Public Prosecutor's Office for serious fraud and environmental crime (*Functioneel Parket*). The National Public Prosecutor's Office focuses on international organised crime and the coordination of efforts to combat terrorism, human trafficking and similar offences. High-tech (cyber) crimes also fall within their remit. The Central Criminal Investigation Division, whose task it is to investigate such offences and that includes the National High Tech Crime Unit, operates under the authority of the National Public Prosecutor's Office. The National Public Prosecutor's Office for serious fraud and environmental crime is responsible for tackling fraud and environmental offences, and handles complex proceeds-of-crime cases.

The Public Prosecutor's Office applies criminal law based on the principle of opportunity, meaning that it chooses whether an investigation is carried out. According to the Dutch authorities, this principle enables the Prosecutor's Office to set priorities for certain types of crime or phenomena. In cases there is a suspect and when there are victims, the prosecutor notifies them if he will not prosecute the case. Article 12 of the Dutch Code of Criminal Procedure (Wetboek van Strafvordering, DCCP) regulates the right of a stakeholder to complain to the court of appeal in case a crime is not prosecuted. The Prosecutor's Office employs an integral approach to fighting crime, together with the police. The subversion approach combines a phenomenon-orientated approach, a subject-orientated approach (targeting specific networks and criminals) and an object-orientated approach (targeting hotspots and safe havens). In every region, integral steering committees are in place to create a common information picture and establish concerted interventions combining penal, fiscal, administrative and other actions. Seizing criminal fortunes is a standard part of the approach.

Judges

The district court is made up of a maximum of five sectors. These always include the administrative sector, civil sector, criminal sector and sub-district sector. Family and juvenile cases are often put into a separate sector. The judges of the criminal law sector deal with all criminal cases which do not come before the sub-district judge. These cases can be heard by a single judge or by full-bench panels with three judges. The full-bench panel deals with more complex cases and all cases in which the prosecution demands a sentence of more than one year's imprisonment.

The courts of appeal deal with civil and criminal cases in which an appeal has been lodged against the judgment passed by the district court. A court of appeal re-examines the facts of the case and reaches its own conclusions.

As the highest court in the fields of civil, criminal and tax law in the Netherlands, the Supreme Court is responsible for hearing appeals in cassation and for a number of specific tasks with which it is charged by law.

4.1.2 Capacity and obstacles for successful prosecution

The Dutch authorities reported that the existing law needs to be updated and it offers insufficient options for undoing data encryption, dealing with illegal actions on the internet or fighting online child pornography.

In addition, according to the Dutch authorities, mutual legal assistance is often found to be difficult and timely assistance is an issue. It takes a while before a request is translated and sent to the requested state. In the digital world time is essential, therefore long procedures can be a crucial negative factor.

Recent developments in the field of cybercrime require demanding actions, for example to counter DDoS attacks or distribution of malware, or where criminals are involved in paralysing vital parts of society by means of botnets. Rendering a botnet harmless requires gaining access to the servers that make up the botnet. Actions in cyberspace can involve making data inaccessible, even when it is located on a server abroad. This can be the case if the actual location of the data cannot be reasonably identified, as is the case in the cloud.

When intercepting communications, the police and judicial authorities are increasingly affected by encryption of electronic data. Special programs for the encryption of data files are available on the internet. Information systems and software are often configured by default for encrypted forms of communication, e.g. Gmail and Twitter. Internet users can transmit information anonymously via certain services. Criminals profit from these developments. Even though providers are obliged to cooperate in disabling encrypted communication, they are sometimes incapable of doing so or are located abroad.

Therefore, the draft law on cybercrime provides for measures that are a better fit for the rapidly developing field of technology, the internet, and computer crime.

4.2 Law enforcement authorities

Police

Investigations are headed by a public prosecutor representing the Public Prosecution Service, which bears final responsibility for investigations. However, investigations are conducted by the police investigators. Police officers seek evidence, interview witnesses and victims, arrest suspects, and record all the information gathered in an official report. Many police stations or basic units have their own criminal investigation section. According to the so called "Organisation plan police" ("Inrichtingsplan politie") a regional unit of the police consists of:

- several districts, each consisting of
- several frontline teams and a District Criminal Investigations Team
- one Regional Criminal Investigations Division, and
- a flex team of investigators to support the district and frontline teams in case of incident peaks or sudden emerging trends.

The Netherlands has been engaged in a comprehensive reform of the national police based on unifying 25 Regional Police Forces and merging them into one national entity. The national unit of the police consists of:

- Central Criminal Investigations Division, amongst others consisting of:
    - The National High Tech Crime Unit (NHTCU);
    - The national team against child pornography and traveling child sexual abuse (TBKK)
- Other central Divisions, like the Central Operations Division and the Central Intelligence Division.

The process entails numerous organisational measures, including adjustments to the mechanisms for coordination among all the stakeholders at regional level (mayors, prosecutors and the police) and with the national level (the Ministry of Security and Justice).

With the advent of cyberspace, the fight against cybercrime, such as internet fraud, is now also part of the local units' workload. These units consist of police employees without specialist knowledge of cybercrime. The police will build digital expert units for support at the local level. At the national level the Netherlands has the Central Criminal Investigation Department for combating very serious, organised and international crime and terrorism.

National High Tech Crime Unit (NHTCU) and digital support

At the national level, the police have set up a special high tech crime unit as part of the National Crime Squad for investigating high-end cybercrime. The national support unit contains digital experts to support investigations of cyber crimes that are less high tech, and to support the gathering of digital evidence. The regional police units will set up digital expert units for the same kind of support at the local level.

Fiscal Information and Investigation Service (Fiscale inlichtingen- en opsporingsdienst, FIOD)

The FIOD is part of the Tax and Customs Administration of the Ministry of Finance and deals with detecting fiscal, economic and financial fraud. The FIOD contributes to the fight against organised crime and terrorism, for example by investigating fraud and mapping out the money flows of criminal and terrorist organisations. The FIOD, in consultation with the Public Prosecution Service, may decide to start a criminal investigation.

The Royal Netherlands Marechaussee

The Royal Netherlands Marechaussee (RNLM) is a gendarmerie corps, i.e. a military personnel with fully fledged police powers. Besides functioning as a military police force the RNLM performs civil police duties at the borders, mainly at airports and seaports. Among the crimes they are confronted with are human trafficking and child sexual abuse, which are both areas of possible cybercrime.

4.3 Other authorities/institutions/public-private partnership

Cooperation between public institutions (mainly law enforcement) in the fight against cybercrime takes the form of public-private information-sharing initiatives. The Electronic Crimes Task Force (ECTF) and the National Cyber Security Centre (NCSC) are a remarkable example of public-private partnership in the field of cyber security.

The Electronic Crimes Taskforce (ECTF) is a joint working group involving the National Prosecutor's Office, the National Police, the major banks in the Netherlands and the Dutch Association of Banks. The main tasks of the ECTF are to share information on specific cases, identify new criminal methods and discuss possible actions to counter them. New payment methods, technologies and possible vulnerabilities are a subject of discussion in the ECTF. The ECTF also produces criminal threat assessments and is able to quickly feed intelligence into law enforcement investigations by proposing concrete action plans. There is a specific focus on financial malware, phishing attacks and other cyber-related incidents directed against the financial sector. The ECTF has been involved in 15 investigations into digital banking fraud. Since the ECTF began its work in 2011, more than 100 suspects have been arrested, including press gangs, money mules and corrupt company employees. According to the Dutch Association of Banks, the damage caused by online banking fraud in 2010 was as high as EUR 9.8 million, whereas in 2009 it was EUR 1.9 million.

The National Cyber Security Centre (NCSC) is another example of a public-private partnership that forges an integrated approach to cyber security in general. It has been operational since 1 January 2012. Its objectives are:

- to contribute to increasing the resilience of Dutch society in the digital domain,
- to help create a safer, more open and stable information society.

The NCSC concentrates mainly on the so-called vital sectors of the country. Therefore, some of its key partners from the private sector are energy companies, and the telecommunications and financial sectors. Participants from the government include the Ministries of Security and Justice, Economic Affairs, Agriculture and Innovation, the Interior and Kingdom Relations, Foreign Affairs, and Defence. The Public Prosecution Service, the General Intelligence and Security Service (AIVD) and the National Police also contribute to the Centre. In the field of financial crime the public-private partnership of the Financial Information Sharing and Analysis Centre (FI-ISAC) is worth mentioning.

The NCSC seems to be well-equipped and well-trained. However, its mandate only covers government and critical infrastructures. Therefore, in the opinion of the evaluators a mechanism should be developed to facilitate assistance to civilian victims of cybercrime.

The above mentioned partnership (FI-ISAC), is a collaboration between the police, the Public Prosecutor's Office and the online market "www.marktplaats.nl". It provides a facility for internet customers to check whether an internet trader has been reported as unreliable, and to report online trade fraud to the police. The financial institutions and government entities share information on cyber attacks..

4.4. Cooperation and coordination at national level

The Minister of Security and Justice plays the key role in providing cooperation and coordination on cyber security and tackling cybercrime at national level. The Ministries of Economic Affairs (with regard to telecommunications and trade), Internal Affairs (with regard to safeguarding the constitution and national security), Defence (with regard to cyber warfare) and Foreign Affairs (with regard to cyber issues in international law) develop and implement the cyber policies within their area of responsibility. The Minister of Security and Justice is responsible for coordinating cyber security issues, and for the policies against cybercrime within the government.

Cooperation with the private sector is well advanced in the Netherlands. The Cyber Security Council established in June 2011 may serve as another example (in addition to those mentioned in point 4.3). The Council consists of high-level representatives of government bodies and business enterprises. The Public Prosecutor's Office and the police are also represented in the Council.

The NCSS2 identifies several actions to intensify the cooperation with private industry, such as improving or developing standards in the international context to promote the security and privacy of ICT products and services.

4.4.1 Legal or policy obligations

Dutch law imposes the following obligations on the private sector to notify public institutions of suspicious incidents:

1. Telecommunications Law – personal data: the notification duty applies to infringement of the technological or organisational security of providers of public electronic communications services where the infringement has adverse effects on the protection of personal data. The notification should be made to the independent Netherlands Authority for Consumers and Markets (ACM). Notification is not required if the data cannot be accessed by the attacker, for example because of encryption.

2. Telecommunications Law – disruption of continuity of services: providers of public electronic communications networks and publicly available electronic communications services should inform the Telecom Agency immediately in case of a breach of security or loss of integrity which disrupted the continuity of the network or service.
3. Law on Financial Supervision – sound operation: on the basis of the Financial Markets Act a number of financial institutions are obliged to notify either the ACM or the Dutch National Bank (DNB) of incidents which affect the sound operation of their institution.

Nonetheless, there are no penalties for failing to notify the NCSC.

In the opinion of the evaluators, mandatory reporting is not an added value in itself, and the risks associated with loss of confidence in service providers must be taken into consideration when assessing this subject. However, it should also be taken into account that the lack of mandatory reporting in case of massive attacks against vital infrastructures run by private companies means the private sector has the power to decide whether or not to fight criminals and bring them to justice according to their own interests and not the public's. It was mentioned during the on-site visit that there had been some reluctance on the part of private companies to pass on information for various reasons.

Nonetheless, the Dutch authorities indicated that new notification duties are currently being prepared for the private sector.

4.4.2 Resources allocated to improve cooperation

The staff of the NCSC (within the Ministry of Security and Justice) coordinates cyber security issues in general among the ministries involved. The Law Enforcement Department of the Ministry of Security and Justice is responsible for policy on criminal law and fighting crime, including cybercrime. The daily coordination and contacts are managed at staff level.

The National High Tech Crime Unit of the police will have grown to 119 full time employees by 2015 and has up-to-date equipment. The Dutch authorities intend to provide the police in every unit with a digital support unit to support the investigation teams. These investments should improve the capacity and knowledge of the regional police units, strengthen the focus of the NHTCU on new and technologically complex crime, and allow for the team to actively share new knowledge with other police units.

During the visit to the premises of the digital centre of the Rotterdam Police the evaluation team was informed that the regional units of the police are not as well-equipped as those at the national level. Although the visit there was promising, in the view of the evaluators there is a discrepancy between the expertise and operational means to fight cyber crimes of the national authorities and the regional authorities (both the police and the Prosecution Services).

4.5 Conclusions

- There is a very coherent territorial allocation in span of control in the Netherlands in terms of law enforcement, the prosecution service and the courts, which is applicable to all authorities involved in combatting crimes. It is followed by a consistent allocation of competences between central and regional units, both at the Public Prosecutor's Office and the police, resulting in good cooperation. In the opinion of the evaluation team, this close cooperation at operational and strategic level allows them to combat cybercrime more effectively.

- The Prosecution Service has developed a specific division for cybercrime consisting of specialist cybercrime officers and prosecutors' assistants, as well as a network of prosecutors handling these cases, which according to the evaluators is a useful method of sharing information and experience.

- The experience at police level seems to be very good, even if the digital centres are still being set up. Therefore, the existence of regional prosecutors specialising in cybercrime could lead to the establishment of similar structures within law enforcement since there is a close relationship between prosecutors and the police on legal and operational aspects.

- Moreover, there are no judges appointed to deal with cybercrime. Therefore, in the opinion of the evaluators raising awareness of this type of crime among judges requires regular training.

- The Ministry of Security and Justice plays a key role in coordinating governmental actions on cyber security alongside the other ministries (Economic Affairs, Internal Affairs and Defence) and chairs meetings held at various levels. The Cyber Security Council has a significant role in that field as well, both as the guarantor of a timely and coordinated response and as the provider of political and strategic guidance to the lower levels of coordination.

- According to the evaluators, public-private partnerships are a very interesting initiative which enables information to be processed informally and alleged crimes and suspects to be discovered using the databases of financial institutions and investigating authorities. It seems that this method of cooperation prevails over the more traditional method based on an official exchange of documentation at the request of law enforcement. The traditional methods of investigating crime apply once law enforcement is convinced that a reasonable suspicion of a crime exists and a crime has been committed.

- Public-private partnerships established in the Netherlands seem to be a very positive step in preventing cyber attacks on vital infrastructures and financial services and ensuring damage control in the event of such attacks (the ECTF and the NCSC). According to the evaluators, cooperation between the public and private sectors brings together a unique set of specific knowledge, information and expertise, substantially improving analysis and intervention capabilities in the context of cybercrime.

- The existence of reliable public-private partnerships is an added value for the prevention of cybercrime and enforcement of cybercrime law. However, in the opinion of the evaluation team these partnerships are also strongly orientated towards protecting the financial markets and the vital infrastructure of the country, with less attention paid to protecting the interests of secondary victims, such as the customers of the main victims and the users of the affected services, particularly when reporting a cyber attack could be detrimental to the image of the corporations involved.

- Dutch law includes obligations to notify public institutions of suspicious incidents, which are set out in the Telecommunications Law (for infringement of the technological or organisational security of providers of public electronic communications services where the infringement has adverse effects on the protection of personal data and on disruption of continuity of services) and in the Law on Financial Supervision (for incidents which affect the sound operation of financial institutions). However, there is no obligation to notify the judiciary or law enforcement of incidents of a criminal nature, including cybercrime, which are not related to the functioning of the public or financial institutions.

- The evaluation team was told that a new law should be passed in 2015 which will include an obligation to report breaches to the NCSC. However, there are no penalties for failing to report, although whether or not a company reported a breach would be taken into account by the relevant authorities looking at the case (data protection supervisor, bank supervisory authority, etc.). Representatives from the NCSC confirmed a general reluctance to report on the part of private-sector organisations. Therefore, in the opinion of the evaluators consideration should be given to establishing a more binding legal framework to govern companies' reporting of cyber attacks.

- In the opinion of the evaluation team, the possibility of employing IT specialists and offering them competitive working conditions may help build capacity to effectively fight cybercrime.

5. LEGAL ASPECTS

5.1. Substantive criminal law pertaining to cybercrime

No legal definition of cybercrime has been developed in Dutch law.

5.1.1 Council of Europe Convention on Cybercrime

The Netherlands signed the Convention on Cybercrime in 2001 and ratified it in 2006.

5.1.2 Description of national legislation

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

Dutch law contains extensive provisions on cybercrime[8]. Council Framework Decision 2005/222/JHA on attacks against information systems has been implemented into Dutch law.

The Netherlands is currently preparing a law which will fully implement Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. The Dutch authorities reported that Dutch law is already largely consistent with this Directive, for example the criminal offences have already been laid down in the Dutch Criminal Code by earlier revisions of Dutch law in 1993 and 2006.

The new legislation will primarily increase the penalties for certain offences. Specifically, the minimum penalties will be increased. The punishment of certain offences with a maximum sentence of two years will be introduced. Moreover, three aggravating circumstances will be added. The sentence will be increased to a maximum of three years if a botnet is used when committing the offence, and to five years if it causes serious damage or is directed against vital infrastructure.

[8] A detailed description has not been inserted into the report for reasons of length. For more information see the annexes attached to the Dutch answers to the questionnaire.

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

In 2014 the Dutch Parliament adopted the draft legislation implementing Directive 2011/93/EU of the European Parliament and of the Council on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (PbEU L 101, 15 April 2011) (hereafter "the Directive"). Since the Netherlands is already legally bound by the Council of Europe's Convention on the protection of children against sexual exploitation and sexual abuse (CETS No 201), the legislative implications of the Directive for Dutch law are relatively minor. According to the Dutch authorities, in comparison with the Council of Europe's Convention and the Directive, the Dutch legislation on child sexual abuse and child pornography is "state of the art".

C. Online card fraud

Cooperation with banks in the Netherlands is not based directly on legal provisions but on private settlements. As an example, law enforcement agencies and the financial sector work together in the Electronic Crimes Task Force (ECTF) to share information on specific cases, identify new criminal methods and discuss possible actions to counter them.

To tackle the problem of skimming, law enforcement agencies and the financial sector worked together in the National Skimming Point. This cooperation resulted in the use of new payment facilities that do not use magnetic strips, together with the standard blocking of debit and credit cards for use outside Europe. This has reduced skimming substantially.

As part of the Financial Information Sharing and Analysis Centre (FI-ISAC), financial institutions and government entities share information on cyber attacks. The NCSC is connected to and supports the FI-ISAC.

As a result of this cooperation the total amount of damages from online banking fraud decreased from EUR 34.8 million in 2012 to EUR 9.6 million in 2013. The total amount of damages from skimming decreased to EUR 6.8 million in 2013.

5.2. Procedural issues

5.2.1 Investigative Techniques

In general, criminal investigations and prosecution procedures are regulated by the Dutch Code of Criminal Procedure. Investigative powers can be used, depending on the invasiveness of the power involved and the seriousness of the offence under investigation. The use of special investigative powers can be triggered by crimes that allow for pre-trial detention, which is generally the case for crimes carrying a maximum of at least four years' imprisonment (Article 67(1)(a) of the DCCP), and by certain specifically mentioned offences (Article 67(1)(b) of the DCCP). Because digital investigative powers may also be required for "simple" cybercrimes, for example hacking without aggravating circumstances, the Computer Crime Act II inserted almost all cybercrimes specifically into Article 67(1)(b) of the DCCP. As a result, for most cybercrimes pre-trial detention is allowed, regardless of their maximum penalty, and most investigative powers can be used to investigate them.

The DCCP describes the following investigative powers for the police in relation to cybercrime: searching premises to secure data on storage devices (Article 125i); acquiring data from other automated works on the searched premises, provided the person(s) present on those premises have

legitimate access to those other automated works (Article 125j); making data inaccessible to stop or prevent a criminal act (Article 125o); acquiring private communications by technical means (Article 126m); ordering a communication service provider to provide data on the user of a communication service and on the communications of that user (Article 126n); ordering a communication service provider to provide personal information on the user of a communication service (Article 126na); identifying the user of a communication service by technical means (Article 126nb); ordering a person who has the relevant data to provide identifying data stored on a suspect (Article 126nc); ordering a person who has access to relevant data to provide that data (Article 126nd-125ng); ordering a person (not a suspect) to help with the decryption of data (Article 126nh); ordering a person (not a suspect) to store relevant data for up to 90 days (Article 126ni).

• *Search and seizure of information system/computer data*

The DCCP contains no specific provisions on searching and seizing computer-related data. The general seizure provisions can be used to seize data storage devices. Data as such cannot be seized, since they are not considered "goods", but they may be copied by law enforcement officers during a search – comparable to taking images of the crime scene or fingerprints, for instance. In addition, the 1996 Data Production Orders Act introduced in Article 125i of the DCCP the power to search in order to preserve data. In the interest of public order or the protection of victims (e.g. children under 18 who have fallen victim to child sexual abuse of which images were made and have been disseminated), merely copying the data may not suffice. In those cases Article 125o of the DCCP allows the prosecutor to order an internet service provider to make the data inaccessible. Article 125j of the DCCP contains the power to conduct a network search if, during a search, relevant data appear to be stored elsewhere on a network. Article 125j of the DCCP allows the person who conducts a search to also search computer networks from computers located at the search premises. The network search may only be conducted to the degree that the network is lawfully accessible to the people who are regularly present on those premises. Under the current interpretation, the network search cannot go beyond Dutch jurisdiction.

Because of decryption technologies it can be difficult for the police to access data. Article 125k of the DCCP enables the investigating officer to order the undoing of a security measure and to order the decryption of, or handing over of a decryption key for, encrypted data. The orders may not be given to suspects.

As general safeguards in the procedures for investigating computers and data, obligations exist to delete retrieved data as soon as they are no longer relevant for the investigation − except if they have to be used for a different case or registered in a serious crime register (Article 125n of the DCCP) − and to inform the persons involved when data have been copied or made inaccessible. The persons to be notified are suspects (unless they are automatically informed through the case file), the controller of the data, and the right-holders of the premises searched, except in cases in which notification is not reasonably possible (Article 125m of the DCCP).

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

Article 126m of the DCCP enables the public prosecutor, with authorisation from a judge, to order the recording of communications that are generated by means of a communications service provider's service. Interception is permitted in cases for which pre-trial detention is allowed and which seriously infringe the rule of law. If the intercepted communications turn out to be encrypted, an order to decrypt may be directed at the person who is likely to know the decryption means, but not at the suspect.

Communications may be intercepted if the interception is necessary for the investigation. The communications of persons with a right to the legal privilege of nondisclosure (lawyers, public notaries, clergy, medical practitioners) cannot be intercepted, unless they are themselves suspects; if, during a regular wiretap, a conversation with such a person on duty is recorded, it must be deleted.

Interception from the Netherlands of the communications of someone located abroad is permitted after the other state has given consent. Also, interception and direct transmission from another state to the Netherlands can be requested, and, conversely, the Netherlands can grant interception and direct transmission from the Netherlands to another state.

Article 126l of the DCCP allows the public prosecutor, with authorisation from the investigating judge, to order an investigating officer to record confidential communications with a technical device, in cases for which pre-trial detention is allowed and that seriously infringe the rule of law. Examples of relevant technical devices are directional microphones, bugs, and keystroke loggers. If necessary, the power includes entering premises to install a device. If the premises entail a private house this can only be done if the crime carries a maximum punishment of at least eight years' imprisonment and the judge has explicitly authorised the measure.

Article 13(1) of the Telecommunications Act (Telecommunicatiewet) requires providers of public telecommunications networks or services to ensure that their networks or services enable interception. This includes internet providers, although not hosting providers.

• *Preservation of computer data*

Article 126ni of the DCCP enables the public prosecutor, in cases of crimes for which pre-trial detention is allowed and which seriously infringe the rule of law, to order someone to preserve data stored on a computer that are particularly vulnerable to loss or change. The preservation can be ordered for a period of at most 90 days (extendible once).

• *Order for stored traffic/content data*

The DCCP provides for powers to order the provision of data. The powers make a distinction between identifying data, "other" data and sensitive data. The orders can be given to persons who process the data in a professional capacity; an order for other stored data and sensitive data can, however, also be directed at persons who process data for personal use. According to Article 126nc of the DCCP, an investigating officer can order identifying data such as names, addresses, postcodes, dates of birth, gender and administrative numbers to be provided in case of a crime (not a misdemeanour).

According to Article 126nd of the DCCP the public prosecutor can order other data to be provided in cases for which pre-trial detention is allowed, including future data and, in urgent cases and with the permission of the investigating judge, the real-time delivery of future data, for an extendible period of four weeks (Article 126ne of the DCCP).

According to Article 126nf of the DCCP the investigating judge can order sensitive data such as religious affiliation, race, political or sexual orientation, health, or trade union membership to be provided in cases involving a crime for which pre-trial detention is allowed and which seriously infringes the rule of law. The provision of data stored with a public telecommunications provider may only be ordered with the consent of a judge (Article 126ng(2) of the DCCP).

• *Order for user information*

In order to obtain user data, Article 126na of the DCCP provides investigating officers with the possibility of ordering a communications service provider to provide user data in the event of a crime. User data includes names, addresses, telecommunications numbers, and types of service. Article 126n of the DCCP, concerning traffic data (see above), also comprises the collection of user data. The provision of other information pertaining to the identity of a person may be ordered under Article 126nc of the DCCP.

In general, the National Police has learned that the use of investigative powers to acquire digital evidence often works best when combined with more traditional powers. For example, while arresting a suspect it can be important to keep an IP-tap running and/or to prevent the suspect locking the computer or smartphone where possible evidence may be stored.

5.2.2 Forensics and Encryption

Under the DCCP, it is possible to carry out electronic and/or remote forensic examination when conducting a network search. The same applies to placing technical devices such as key loggers.

The rapid developments in ICT mean that investigative powers need to be adapted. This will allow the police and judicial authorities to take adequate action against cybercrime. A significant amount of communications and information, and hence potential investigative information, travels via the internet and computers and is encrypted by default. Examples are conversations via Skype or chats via WhatsApp. The Dutch authorities underlined that the police and judicial authorities can intercept these messages using standard internet interception, but are often unable to decrypt them.

The National High Tech Crime Unit of the police and the forensic experts of the regional police units can secure digital evidence. The Dutch Forensic Institute (NFI) also employs digital forensic experts for that purpose at the national level.

The police also cooperates with other government bodies and with private industry in the NCSC.

Dutch experience shows that encrypted files and communications often remain (partly) inaccessible. The algorithms used by criminals and their implementation are often technologically solid. Therefore, cooperation is essential for a successful investigation. The police, especially the National High Tech Crime Unit, cooperates with the Dutch Forensic Institute and Europol/EC3. Private companies are not involved in decryption in criminal investigations.

The Dutch authorities reported that a new law is being prepared to enable the police to remotely access an automated work under strict conditions. This would create possibilities for capturing data before it is sent out (and encrypted) or after it has been received (and decrypted).

5.2.3 e-Evidence

The DCCP regulates evidence-gathering in general. Article 350 of the DCCP stipulates that the court (usually a panel of three trial judges) discusses whether the alleged criminal acts can be proven and can be attributed to the accused. The judges have to be convinced that the defendant is guilty of the offence, based on the statutory means of evidence (Article 338 of the DCCP). The statutory means of evidence are the judge's own observation, statements in court from the defendant, witnesses and experts, and written documents (Article 339 of the DCCP).

Written documents include various official documents that have evidential value on their own and all "other writings" that count only in relation to the contents of other means of evidence (Article 344(1) of the DCCP). An official report by an investigating officer has special evidential value; it can constitute proof that the defendant committed the alleged acts (Article 344(2) of the DCCP). The "other writings" mentioned in Article 344(1) of the DCCP are independent of a medium and can include electronic documents. Forensic digital evidence can be used in court in various ways: as official documents written by experts, as expert statements made in court, as official reports by investigating officers describing their observations, or as observations by the judge when the evidence is demonstrated on a computer in court.

Electronic evidence is acquired and stored by the National Police. The DCCP and the Police Data Act regulate the acquisition, storage and destruction of electronic evidence. Analyses of electronic evidence are provided to the parties involved in the court proceedings as part of the criminal case file.

There are no additional regulations for electronic evidence acquired outside Dutch jurisdiction. It is handled in court as other evidence, based on full disclosure. However, if investigative procedures set out by the DCCP were not met, the judge may rule the evidence inadmissible. If special conditions are set by the country that helped acquire the evidence, the police and prosecutor will respect those conditions. Nonetheless, this could hinder the ability to use the evidence in court.

5.3 Protection of Human Rights/Fundamental Freedoms

The Dutch Data Protection Act (Wet bescherming persoonsgegevens, Wbp) and the Police Data Act (Wet politiegegevens, Wpg) provide the legal framework for access to personal data and the destruction of data when they are no longer relevant for a criminal investigation. The Dutch Data Protection Agency (College Bescherming Persoonsgegevens, CBP) supervises compliance with acts that regulate the use of personal data. It supervises compliance with and the application of the Dutch Data Protection Act, the Police Data Act and the Municipal Database Act. The Data Protection Agency must be notified of the use of personal data, unless an exemption applies. The framework for performing this task has been set out in the Data Protection Act and other related legislation.

In criminal investigations, when the use of special investigative powers is necessary, law enforcement agencies are bound by the principles of proportionality and subsidiarity. The Public Prosecutor's Office is responsible for ensuring that investigative powers are used in a way which entails the least possible infringement on fundamental rights. Moreover, the infringement cannot go beyond what is strictly necessary for the specific investigation.

Furthermore, the legal system of criminal proceedings provides a hierarchy of competent authorities. Greater infringements on rights require an order of the public prosecutor; for the greatest infringements the prosecutor requires authorisation from a judge. The use of investigative powers is assessed by a judge in court when the suspect is prosecuted. Infringements on universal rights, such as the right to privacy, are only possible if allowed under and in accordance with international treaties, such as Article 8(2) of the Convention for the Protection of Human Rights and Fundamental Freedoms. Fundamental rights and freedoms are guaranteed in the Dutch Constitution.

There is no normative hierarchy indicated by the Constitution: all basic rights are in principle equal in value and importance. Some rights are absolute, most can be limited by parliamentary or "formal" law, and many can be limited by delegation of limiting powers. They include the following:

- Freedom of speech (Article 7 of the Dutch Constitution).
- Right to privacy (Article 10 of the Dutch Constitution), which can be limited by formal law although delegation is allowed only in relation to databases. The Article imposes a duty on the government to protect against a threat to privacy posed by a possible abuse of databases (subarticle 2), and to regulate the right of persons to be informed about the content of such databases concerning their person and the right to correct possible mistakes in such content (subarticle 3).
- Secrecy of communication (Article 13 of the Dutch Constitution), which covers the right to privacy of correspondence and the right to privacy of communication by telephone and telegraph. No delegation is allowed. For most cases the investigative judge is the competent authority.

5.4 Jurisdiction

5.4.1 Principles applied to the investigation of cybercrime

Article 2 of the DCC sets out substantive jurisdiction and states that the Code is applicable to anyone suspected of any offence in the Netherlands. Article 4 of the DCC provides jurisdictional grounds for many specific offences committed outside of the Netherlands. These include forgery, extending to computer forgery, committed abroad by Dutch government employees and computer sabotage or data interference committed against a Dutch national if the act is related to terrorism.

Article 5 of the DCC establishes jurisdiction for certain crimes committed outside of the Netherlands by Dutch nationals. These include publishing corporate secrets acquired by accessing a computer and child pornography. Jurisdiction also extends to child pornography committed by foreigners with a fixed residence in the Netherlands, even when they come to reside in the Netherlands after the crime has been committed. This also includes jurisdiction over almost all cyber crimes when committed by Dutch nationals abroad. Dutch law uses the active nationality principle.

In cybercrime cases it is possible for intereception and observation to be carried out across national borders. The Schengen Treaty and the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union of 29 May 2000 are applicable.

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

The Netherlands resolves conflicts of jurisdiction through consultation with the respective countries, and with Eurojust and Europol. However, the Netherlands has not yet established the mechanism set out in Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings. Nonetheless, the Netherlands takes part in joint investigations under the coordination of Eurojust.

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

The Dutch authorities stressed that the police and judicial authorities have a need to access computers via the internet in order to track serious crimes in the digital era. The increasing storage of data in the cloud causes problems for the police and judicial authorities. Even though a provider can be ordered to supply certain data, this often turns out to be very difficult in practice. There are providers who do not cooperate with the police ("rogue providers"). Sometimes, a provider cannot be found or is established in a country with which the Netherlands maintains a very limited relationship of legal assistance.

Moreover, people are able to conceal the path of their exchange of data to such an extent that they are difficult to trace. Also, cloud storage providers may have trouble locating the actual (territorial) location of data. Because of the technologies used, and because of storage capacity in servers and economies of scale, data move around the globe constantly and may be fragmented in pieces to be put together only upon retrieval. While the police may suspect that information is not located in the Netherlands, it often proves impossible to ascertain this and to pinpoint data to a territorial location. As a result, information and the computers that process it, especially in the cloud, are not easily located and accessed by law enforcement.

The Dutch authorities underlined that it has proven impossible to date to solve this problem adequately. International law provides countries with various possibilities for acting independently or in mutual cooperation (legal assistance), but this has proven limited for investigations in cyberspace. The Council of Europe has concluded conventional law agreements relating to such matters (including with non-member countries such as the United States of America, Canada, Australia, and Japan). Pursuant to the Convention on Cybercrime, cross-border action is only possible in a very limited number of cases, i.e. with the lawful consent of the person who has the

lawful authority to disclose the data, in a case where the jurisdiction is known. In cases where the location of data is not known, these provisions are inadequate. This results in cases where cybercrime will go unpunished, and situations in which people will be victimised over and over again.

5.4.4 Perception of the Netherlands with regard to legal framework to combat cybercrime

The Netherlands does not consider the existing framework sufficient. Therefore, the Minister of Security and Justice is preparing a new bill of law on cybercrime. The Netherlands fully agrees with the findings and recommendations set out in the report prepared by the Cybercrime Convention Committee on trans-border access to data[9]. This report includes a discussion of the applicability of the principle of territoriality in the light of the movement of data in "cyberspace", and of the need to adopt an Additional Protocol to the Budapest Convention as a consequence.

An Additional Protocol could address the following situations between Parties:

- trans-border access with consent but without the limitation to data stored "in another Party";
- trans-border access without consent but with lawfully obtained credentials;
- trans-border access without consent in good faith or in exigent or other circumstances;
- extending a search from the original computer to connected systems without the limitation "in its territory";
- the power of disposal as a connecting legal factor.

9 http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/TCY_2012_3_transborder_rep_V30public_7Dec12.pdf

5.5 Conclusions

- The Netherlands signed and ratified the Convention on Cybercrime. The draft legislation implementing Directive 2013/40/EU on attacks against information systems is currently being prepared. Nonetheless, the Dutch authorities reported that Dutch law is already largely consistent with this Directive.

- Directive 2011/93/EU of the European Parliament and of the Council on combating the sexual abuse and sexual exploitation of children and child pornography was implemented in 2014.

- Combating credit card fraud is based more on cooperation with financial institutions than legislative solutions.

- The existing legislation seems not to provide a binding and common definition of cybercrime. According to the evaluators, this may result in the use of a limited or different concept of cybercrime for statistical purposes. Consequently, stakeholders involved in combating cybercrime may not share a common understanding of or common approach to the same concept.

- In relation to investigative techniques, there are a number of measures for seizing and retaining data for the purpose of gathering evidence (e.g. ordering a person who has access to relevant data to provide that data, or ordering a person to help with decryption of data), but also to prevent a criminal act from being committed (such as making data inaccessible to stop an activity). In the Netherlands, the use of special investigative powers commonly hinges on whether the crime allows for pre-trial detention (for crimes carrying a maximum of at least four years' imprisonment). Investigative powers can also be used depending on the type and seriousness of the offence with regard to specifically mentioned offences (almost all cybercrimes fall under this category).

- The Ministry of Security and Justice is preparing a new bill of law on cybercrime. This legislative reform may address new investigative measures and instruments, such as the ability to enter a computer device secretly and remotely (online), safeguards and conditions (e.g. an order can only be given if it is urgently required in the interest of the investigation or its execution is reserved for designated investigators within the police), decryption by the suspect, enhanced possibilities for criminalising and investigating online grooming of children, the criminalisation of handling stolen computer data, and the criminalisation of repeated fraud in online markets.

- The Dutch authorities reported having difficulties with granting full or partial access to encrypted files and communications. It is specifically problematic when e-evidence is located abroad. Therefore, they stressed the importance of cooperation for a successful investigation. For that purpose the police (especially the National High Tech Crime Unit) cooperate with the Dutch Forensic Institute and Europol/EC3. Private companies are not involved in decryption in criminal investigations.

- The Dutch Data Protection Act and the Police Data Act provide the legal framework for accessing personal data and the destruction of data when they are no longer relevant for a criminal investigation. Human Rights and Fundamental Freedoms are also protected by the Dutch Constitution.

- Dutch law provides for an obligation to investigate crimes committed within Dutch territory. Moreover, the Dutch Criminal Code provides jurisdictional grounds for many specific offences committed outside of the Netherlands. The Dutch Criminal Code establishes jurisdiction over almost all cybercrimes when committed by Dutch nationals abroad. Dutch law uses the active nationality principle.

- Cybercrime committed via the "cloud" was highlighted during the evaluation visit as an area creating issues for investigation and prosecution, particularly in relation to retrieving the actual physical location of data. The method of cloud computing creates a problem not only with regard to national law but also to international legislation which is based on the acknowledgement of states' independence. Nonetheless, in the opinion of the evaluators, it could be useful to consider addressing the existing relevant legal frameworks in place and/or investigative issues in relation to cybercrime committed in the "cloud".

6. OPERATIONAL ASPECTS

6.1. Cyber attacks

6.1.1 Nature of cyber attacks

Every year the Ministry of Security and Justice publishes the Cyber Security Assessment (CSAN) on the developments in the past twelve months. The number of incidents measured includes incidents which are reported to the NCSC on a voluntary basis**.** The primary targets of the NCSC are federal government and critical (private) infrastructure. Therefore not all incidents are reported to the NCSC during the reporting period.

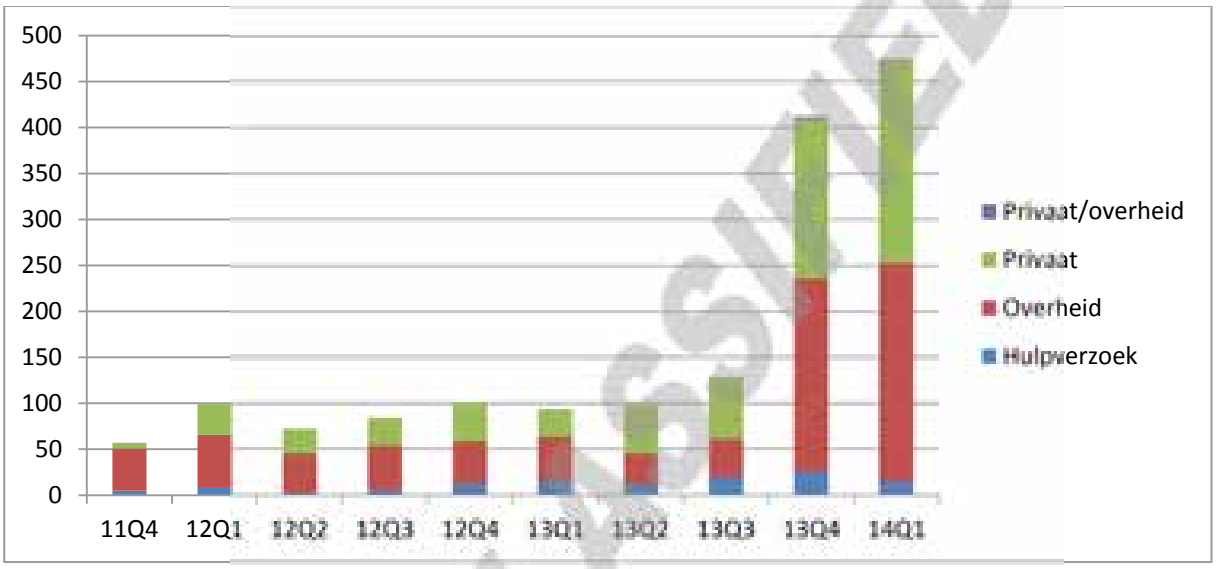

Figure 1: Incidents handled by the NCSC (11Q4-14Q1). [10]

The Dutch authorities explained that the sudden increase in incidents (Q4-2013 and Q1-2014) can primarily be attributed to automated computer controls which started in October 2013. In addition, the number of responsible disclosures to the Dutch government also increased starting from September 2013.

[10] The descriptions given in diagram No 1 should be read in English in the following order: private/public, private, public, request for assistance.

When the incidents registered via automated controls are excluded there is still an increase in incidents reported to the government from 89 in the second quarter of 2013 to 163 in the first quarter of 2014. This surge is possibly explained by certain factors such as changes to the criteria used to define an incident, better-functioning systems and the further professionalisation of the NCSC. Also, the number of incidents reported by the private sector increased during the reporting period.

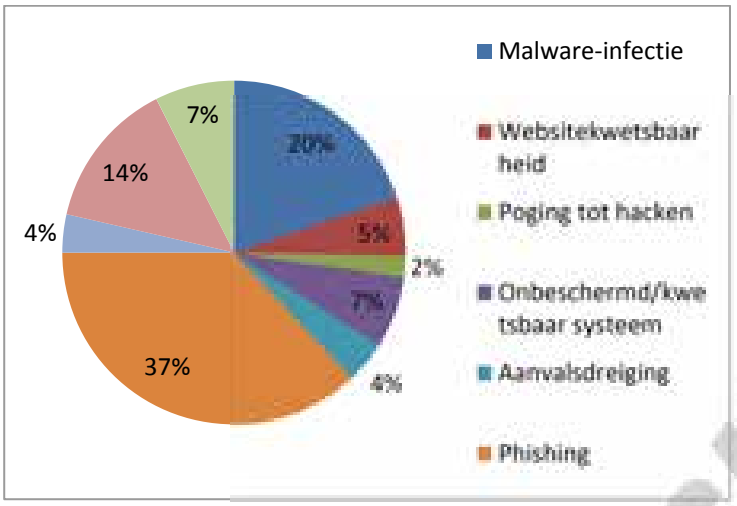

Figure 2: Impact incident notifications related to private parties[11]

The evaluation team realised that the lack of overall cybercrime statistics at the national level, including incidents reported by natural persons victimised by cybercrime, hampers a general assessment of this phenomenon. As a result, the apparent lack of a precise definition of cybercrime – the tendency is to use a limited one similar to that used to define high-tech crimes (*targeting computers using computers*) – and the inability to assess overall figures on cybercrime (as a percentage of overall criminality), make it more difficult to obtain a clear picture of the impact of the cybercrime phenomenon.

[11] The descriptions given in diagram No 2 should be read in English in the following order: malware infection, website vulnerability, attempt to hack, unprotected/vulnerable system, attack threat, phishing.

6.1.2 Mechanism to respond to cyber attacks

The Dutch authorities indicated that increasing Dutch digital resilience cannot be achieved by the government alone. They perceive an important role for the private sector, in particular operators of critical infrastructure and information systems, as the ICT infrastructure itself and knowledge about that infrastructure is largely in the hands of national and international private parties. Therefore, cyber security in the Netherlands is perceived as a joint effort between government bodies, the business community and other organisations and citizens, both at the national and international level. Operators of critical infrastructure have the first responsibility to take measures to guarantee the continuity of their own services. The increased cooperation between different private companies and public organisations within the Information Sharing and Analysis Centres (ISACs) helps to minimise cyber incidents or threats. ISACs are public-private partnerships, organised by sector, where participants exchange information and experience on cyber security.

The Ministry of Security and Justice intends to introduce mandatory reporting of ICT incidents for providers of products or services whose availability and reliability are vital to Dutch society. These are: electricity, gas and water; telecoms; water management; finance; transport (port of Rotterdam and Schiphol Airport); and public authorities. The law should introduce a reporting requirement in case of an infringement on the security of a company or a loss of integrity of electronic information systems in components whereby an infringement might lead directly or indirectly to social disruption. The notification must be made to the Minister of Security and Justice and will be handled by the NCSC. The notification should consist of the following elements:

- the nature and extent of the breach;
- the date of commencement of the ICT infringement;
- the potential impact of the breach;
- an estimation of the recovery;
- the measures to take (or already taken) by the provider;
- the contact details of the official who is responsible for the notification.

The National High Tech Crime Unit and the NCSC have liaisons. These parties exchange information in case of an incident within the confines of the law. If incidents have, or threaten to have, a disruptive effect on society, the NCSC is at the service of the national crisis structure. The NCSC has the task of signalling and initially identifying an ICT threat. The acquisition and sharing of information is coordinated by the NCSC. If necessary the NCSC activates the ICT Response Board (IRB). The IRB is a public-private advisory council responsible for conceptualisation, interpretation and advice in the event of serious ICT incidents. The advice can be used by the national crisis structure of the government, and by the other IRB parties. Those currently represented in the IRB are telecom companies, energy suppliers, banks and governmental organisations such as the police. The National Crisis Centre (NCC), after being advised by the IRB, takes measures to respond to a serious cyber incident. The NCSC then monitors and/or supports the execution of measures taken by the NCC.

In addition, the NCSC coordinated the launch of the National Response Network (NRN) in April 2014. The NRN is a collaboration between public and private organisations aimed at increasing the digital resilience of critical systems in the country. The aim of the NRN is to share information and coordinate responses in the event of major cyber security incidents. The initial participants include the Tax Service, Surfnet, DefCERT, the Information Security Service for municipalities and the NCSC. Through the NRN, the NCSC facilitates the optimisation of the response in case of a serious cyber incident. More public and private partners are expected to join the NRN in the near future.

The government focuses on strengthening cooperation in operational responses between the CERT organisations in Europe as laid down in both the NCSS1 and NCSS2. The Netherlands collaborates mainly in an informal manner, in international networks such as the International Watch and Warning Network (IWWN), FIRST, the European Government Cert network, and TF-CSIRT, as well as through bilateral contacts.

According to NCSS2, citizens are also expected to cooperate with government bodies, business and institutions regarding detected vulnerabilities in their ICT security. However, the impression of the evaluation team is that much more has been done to involve citizens in countering child pornography than other forms of cyber crimes.

6.2 Actions against child pornography and sexual abuse online

The Dutch authorities reported the following numbers related to child sexual abuse in 2013: 3790 reports, 542 suspects prosecuted, 130 victims identified, and five child sex tourism cases.

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

For years the Dutch police have been saving in a database many images of child sexual abuse which have been classified as illegal images according to the Dutch Criminal Code. To enhance the effective use of this database the images have been hash coded.
Dutch law enforcement organisations cooperate in a European "in-4-mation" project, in which the national databases of participating countries are connected to each other. This "in-4-mation" database has not been finalised, but the Netherlands is ahead of schedule and currently implementing it. Dutch law enforcement, especially the police, also actively participates in Interpol's efforts to identify victims. This includes contributing to and making use of the ICSE database.

In 2008 the Minister for Economic Affairs signed a non-legally binding agreement with a large number of internet service providers (ISPs) on a voluntary model of "Notice and take down" of illegal expressions on the internet. Over 95 % of the ISPs are covered by this agreement.

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

According to the Dutch authorities, cyber bullying is on the edge of criminal and non-criminal behaviour. Sexting is also a phenomenon that is on the boundary between legal and illegal behaviour. On the one hand, children are exploring their own sexuality, and on the other hand, they may unwantedly become a victim of sexual abuse. When reports are made, the police respond to them and may open investigations. The main response to cyber bullying and sexting is prevention by making children aware of safety online.

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

The Dutch authorities reported that the approach targeting child sex tourism has been intensified in recent years. In October 2013 the Ministry of Security and Justice sent an Action Plan to combat child sex tourism (or transnational child sex offences) to parliament. The Action Plan includes more focus on the prevention of child sex tourism, improved detection and prosecution, and enhanced national and international collaboration. Among other things, the Dutch police has stationed two flexible liaison officers in Brazil (the stage of the football world cup) and the Philippines (targeted by sex offenders). These officers strengthen the fight against child sex tourism and contribute to international cooperation. Furthermore, a Dutch international certificate of good conduct has been constructed and published, to be used worldwide.

Other actions include the possibility of confiscating the passport of a convicted child abuser, in conjunction with a proposed bill on the oversight of delinquents who have been convicted for violent and sexual abuse. In this way known sex offenders with a high risk of repeat offending will not be able to travel outside Europe to engage in child sex tourism (travelling child sex offending).

Real-time web-based child pornographic performances, for instance in webcam situations, are an emerging threat. In domestic situations this involves grooming of children, where children are gradually lured in, and/or are blackmailed, to pose naked and/or to perform sexual acts. In other countries, mainly countries in which child sexual abuse is very present such as in South East Asia, this leads to sexual abuse of children being watched online. It is hard to find adequate solutions.

Currently Dutch law enforcement is working on methods to enhance the early detection and subsequent investigation and prosecution of online groomers by covert operations in which a police officers present themselves as a child in online chat rooms in order to obtain the identity of the groomer and/or to make an offline appointment to apprehend the groomer. The new bill of law on cybercrime criminalises grooming in order to support this working method.

Media education is a powerful tool for the prevention of child sexual abuse, especially for children and adolescents. Parents and schools are vital in media education. From 2008 onwards the Ministries of Health and of Youth and Family have run a special centre for expertise on media education. This centre (www.mediawijzer.net) aims at enhancing media education for the public, with a special focus on youth (10-14 years). Within the centre many different organisations cooperate and provide education materials, campaigns, etc. Additionally a public-private partnership titled "Digivaardig – Digiveilig" organises and stimulates media education.

The Dutch Ministry of Security and Justice, together with the EU, subsidises a hotline for referral of child sexual abuse which is a member of the international INHOPE network. In addition to receiving actual referrals the hotline also deals with (digital) education of youngsters on the risks of child sexual abuse, such as the risks of grooming (www.helpwanted.nl). Another initiative of this hotline is the introduction of a so-called referral button people can download into their browsers. This button directs users to the hotline's website, where they can report child sexual abuse and find tips to make themselves resilient to child sexual abuse. This website mainly focuses on 11- to 16-year-olds.

The Ministry of Security and Justice has close contacts with social media companies like Twitter. The main goal of this collaboration is to have new child abuse material removed as quickly as possible. In these contacts the method of "PhotoDNA" was discussed, which is a software tool that recognises child abuse material.

The Dutch police hosts a weekly online "Q and A" hour, in which children can chat with police officers (http://www.vraaghetdepolitie.nl). This site is widely promoted and known among a broad public. It is mainly aimed at young people, allowing them to ask questions about their online activity or about special themes such as online abuse.

6.2.4 Actors and measures countering websites containing or disseminating child pornography

Article 125o of the DCCP gives the prosecutor the power to remove the contents of a webpage as a temporary measure if so required in a concrete investigation into child sexual abuse. The removal of content will then be decided upon in a court verdict.

It should be highlighted that the public initiatives such as combating child pornography draw significant involvement from private companies in the Netherlands. A voluntary model of “Notice and take down” of illegal expressions on the internet should be mentioned as an example. For this purpose a uniform time-bound procedure is used in which an ISP investigates a referral of the existence of illegal material on websites to which the ISP in question provides access, and subsequently takes a motivated decision on whether to remove that material. In that case, the person who registered the domain is investigated according to nationality. If the person is Dutch they will be investigated further. This happens once or twice a year. In all other cases the registered person is a foreign national.

In 2009 a public-private partnership of internet service providers, law enforcement agencies and the Ministries of Security and Justice and of Economic Affairs started a working group on internet and security. The group specifically dealt with the (then ongoing) project on DNS blocking of images of child sexual abuse. In this project the ISPs and the Dutch hotline "meld kinderporno op het internet" developed a method to block websites that contained known child sexual abuse images, made available by Dutch police on a DNS level. However, a pilot study led to the conclusion that this DNS blocking method could be applied to such a small number of websites that the results did not justify the cost. The project was ended in 2011.

Another project launched in 2012, in which the uploading of images through a big hosting provider based in the Netherlands was matched with the hash-coded database of known images of child sexual abuse, proved to be of little use for the purposes of investigations. However, the Dutch police realised that it might be useful if the private sector could further investigate the possibilities of creating "whitelisting" tools and applications to prevent private or business networks from spreading known child sexual abuse images.

In addition to this INHOPE hotlines share with each other information on images which they believe originate – at least in terms of where the websites with the images in question are hosted – in one of their countries. The respective hotline will refer those images to the competent law enforcement organisations.

The Dutch police actively participates in Interpol's efforts to identify victims, specifically contributing to and using the ICSE database (for more see point 7.2).

The Dutch police became a member of the Virtual Global Taskforce in 2013. The latest international VGT conference was hosted in and by the Netherlands in November 2014. The theme of this conference was "Transnational Child Sex Offences" and it focused on sex crimes against children with an international component.

There are also specialised units dealing exclusively with child pornography. Since October 2012 the detectives dealing with child pornography and child sex tourism have been operating in a nationally organised uniform entity. The national unit and the 10 regional units have a uniform team for investigations into child pornography and child sex tourism. These units employ 150 detectives and are directed as one organisation. To strengthen their mental resilience the Dutch authorities developed a mental health programme. The police and the prosecutor's office set up a national steering committee to determine a national strategic framework and the national priorities for investigations into child pornography and child sex tourism. The national steering committee also monitors the implementation of the framework and the priorities. In addition to this, a tactical advisory committee guides the implementation and monitors the results of concrete investigations. This tactical committee has been closely watching the focus of investigations shift from downloaders towards victims of child sexual abuse, the actual abuser and the major disseminators. At the national level four prosecutors have been appointed to secure the link between the national approach and regional prosecutions.

6.3 Online card fraud

6.3.l Online reporting

The platform of cooperation between the police, the Public Prosecutor's Office and the online market is the Financial Information Sharing and Analysis Centre (FI-ISAC). It provides a facility for internet customers to check whether an internet trader has been reported as unreliable, and to report online trade fraud to the police.

6.3.2 Role of the private sector

The private sector plays a predominant role in the Dutch system to combat online card fraud. That role has been described in points 4.3 and 5.1.2.

There are many platforms serving to share information on specific cases, identify new criminal methods and discuss possible actions to counter them. Nonetheless, in the opinion of the evaluation team, the Electronic Crimes Task Force (ECTF) merits special attention since it offers a unique opportunity to informally exchange data and information on new payment methods, technologies and possible vulnerabilities that may be further elaborated upon by law enforcement.

6.4 Conclusions

- The Netherlands collects statistics with regard to cybercrime on a yearly basis. The Ministry of Security and Justice publishes the Cyber Security Assessment (CSAN) on developments in the past twelve months.

- Since the statistics involve incidents reported to the NCSC on a voluntary basis, it is difficult to build up a general overview on cyber criminality in the Netherlands detected by the police and private sector. The situation may change in the future since the Dutch authorities aim to broaden the scope of information on incidents that must be reported by the private sector to law enforcement.

- The new draft legislation introduces a reporting requirement in case of an infringement on the security of a company or a loss of integrity of electronic information systems in components whereby an infringement might lead directly or indirectly to social disruption. The notification will be handled by the NCSC.

- The increased cooperation between different private companies and public organisations helps minimise cyber incidents or threats. Nonetheless, in the opinion of the evaluators, those involved in the fight against cybercrime – the Prosecution Service, the National Police and public-private structures – should have a more balanced approach and give more attention to the interests of secondary victims. According to the evaluators, the public-private partnership is too orientated towards protecting the financial markets and the country's infrastructures, with less attention paid to the interests of the secondary victims.

- The Netherlands has established structures and capacities to deal with online child sexual exploitation, including a focus on victims. Law enforcement works with other international entities in this area such as the NCMEC and supports initiatives to tackle the problem of travelling child sex offenders.

- The national programme against child sexual abuse images and transnational child sex offences represents an outstanding initiative to fight against these specific aspects of child sexual exploitation, child sexual abuse and child pornography. The voluntary approach mechanism called "Notice and take down" seems to be very effective due to the number of internet service providers involved. However, the question remains whether, to achieve its full potential, it might require greater involvement on the part of the administration, which would probably need to be supported by legal measures.

- The public campaigns on child pornography along with work of the specialised units dealing exclusively with child pornography and child sex tourism deserve special attention. Also, close cooperation with Europol and Eurojust and international cooperation with partners outside of Europe is having an effect with regard to the growing detection of child pornography. The posting of liaison officers by the Dutch police in countries affected by sex tourism contributes to countering child pornography.

- The Dutch mental health programme for law enforcement officers dealing with CSE is noteworthy. The mental resilience of officers working on cases that involve child sexual abuse images, identifying victims and finding connections, requires special attention, so they can stay healthy despite performing this demanding work.

- In the opinion of the evaluators, continued actions to raise the awareness of society and local investigators and prosecutors of how to deal with child pornography and how to gather evidence should strengthen this approach.

- The Electronic Crime Task Force (ECTF) provides a very good example of police and financial cooperation based on sharing relevant information to deal efficiently with online fraud on a daily basis on the same premises. This cooperation is having a promising effect since statistics show a falling trend in online card fraud in the Netherlands.

- The success of the public-private partnership should be regarded as best practice to explore how to get the best out of close cooperation between the public sector (the police and Public Prosecution Service) and private sector (i.e. internet service providers, social networks online, NGOs, hotline services, etc.).

7. INTERNATIONAL COOPERATION

7.1. Cooperation with EU agencies

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

The Dutch authorities underlined that improving cooperation with Europol/EC3 is a priority of the NCSS2. The Dutch police actively supports Europol/EC3. This should also help the fight against online child exploitation.

The Public Prosecutor's Office, with help from Eurojust, has taken the initiative of strengthening the international cooperation of public prosecutors in cybercrime cases.

The Netherlands has also invested in knowledge and expertise, and participates in joint investigations.

However, the evaluation team noticed at the local level that district prosecutors and regional units of the police seem to have a vague and insufficient knowledge of the possibilities offered by Eurojust and, therefore, do not use them as often as might be necessary to facilitate judicial cooperation or to provide support where coordination is needed.

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

According to the Dutch authorities, the value of Europol and Eurojust is in connecting countries in specific investigations and coordination. Therefore, Eurojust could keep its focus on the overall strategy in the law enforcement approach to possible criminal investigations.

When applicable, contact with ENISA is established through the NCSC of the Ministry of Security and Justice.

7.1.3. Operational performance of JITs and cyber patrols

In the opinion of the Dutch authorities, a joint investigation team (JIT) may contribute to good cooperation with Europol and Eurojust. The board of procurators-general issued an Instruction for the Public Prosecution Offices on 11 February 2008 to develop a common policy on the use of JITs. It establishes rules for the setup, scope, composition and powers of international JITs.

The Dutch experience with regard to working with JITs is positive. Recently two JITs have been operational with regard to cybercrime in which the Netherlands was involved. Europol and Eurojust were central in this. The most recent investigation is the so-called Operation Blackshades. EU funding was allocated to facilitate this cooperation but limited to a travel budget to meet JIT partner countries.

According to the Dutch authorities, using open sources is a method used in the national crime squad.

The team leader of the Dutch High Tech Crime unit takes part in the European Union Strategic Group of the Heads of National High Tech Crime Units at Europol. The Dutch police are also active in the project on child sexual abuse in the EMPACT programme, and where appropriate in the European Financial Coalition against child sexual abuse.

7.2 Cooperation between the Dutch authorities and Interpol

The Dutch police actively participates in Interpol's efforts to identify victims. This includes contributing to and using the ICSE database. Moreover, a new environment called "Baslinelist" in the Interpol ICSE database has been created and is used to speed up image analyses. Specific criteria have been developed, in close collaboration with Dutch law enforcement, to make the content of this "Baselinelist" internationally exchangeable. The baseline is those materials which are punishable under criminal law in every participating country. This part of ICSE is not ready yet, but Dutch law enforcement is set up to start uploading to this database.

In addition, the Netherlands expressed its support for the development of the Interpol Global Complex for Innovation (IGCI) in Singapore. The National High Tech Crime Unit of the police supports the realisation of the IGCI. A liaison from the police and a seconded expert from the team will be placed at the IGCI to share experiences and expertise.

The government focuses on strengthening cooperation in operational responses between the CERT organisations in Europe as laid down in both the NCSS1 and NCSS2. The Netherlands collaborates mainly in an informal manner, in international networks such as the International Watch and Warning Network (IWWN), FIRST, the European Government CERT network, and TF-CSIRT, as well as through bilateral contacts.

7.3 Cooperation with third states

The Dutch authorities stressed that they work on developing cyber security capability in third countries through bilateral or regional initiatives. At the national and international level scarce capabilities have to be deployed among vulnerable sectors and groups. In addition to governments, an important role can be played by private sector parties and social organisations. The Netherlands is promoting this approach internationally – at the United Nations, during international cyberspace conferences such as the ones held in London, Budapest and Seoul and the upcoming Global Cyber Space Conference in the Netherlands in April 2015, as well as in other multi-stakeholder settings like the Internet Governance Forum – by promoting the principles of cyber security as published by the World Economic Forum, and in developing trust-inspiring measures between states, such as the Organisation for Security and Cooperation in Europe (OSCE).

During the on-site visit the evaluation team was informed that an agreement between the USA and the Netherlands is in place which empowers Dutch authorities to send direct legal assistance requests to US companies. In the opinion of the evaluation team, this should be considered as an appropriate tool to speed up investigations.

The Dutch authorities consider that cooperation with Europol/EC3 and Eurojust has brought an added value to cases related to third countries. As an example, they have contributed to successes in investigations into cybercrime, such as:

- Investigation into child sexual abuse: the joint Operation Atlantic, conducted by the US Federal Bureau of Investigation (FBI) and several EU Member States, was finalised in 2011 under the coordination of Europol. After more than a year of investigations in Member States, 37 child sex offenders were identified. Among these offenders, 17 were arrested for child sexual molestation and production of illegal content. Moreover, eight victims were identified.

- The Blackshades investigation: during two days of operations in 16 countries worldwide, coordinated by Eurojust and supported by Europol/EC3, creators, sellers and users of BlackShades malware were targeted by judicial and law enforcement authorities in May 2014.

7.4 Cooperation with the private sector

Dutch law provides for the liability of internet service providers for illegal content on the internet via their systems if they are fully aware of this fact, in accordance with EU law. However, the Dutch authorities reported that many ISPs merely provide a conduit and that situation derogates from the liability of ISPs.

In order to facilitate removal of illegal expressions from the internet, the voluntary model of "Notice and take down" has been introduced to stimulate self-regulation in the industry (for more see points 6.2.1 and 6.2.4).

Furthermore, the public prosecutor has the power to order an organisation to remove content from the internet (Article 125o of the DCCP). Moreover, the DCCP specifies several powers to issue orders for the collection of evidence by search and seizure of information system/computer data, the preservation of computer data, stored traffic/content data, and user information. Private companies may be subject to those orders if they have their main headquarters in a third state. ISPs residing abroad can be approached directly to cooperate with requests/orders on a voluntary basis, provided the government of the country where a company resides consents. The Netherlands claims to have had many good experiences with this working method in practice.

In 2010, the Dutch NHTCU started a public-private partnership to combat botnets. With members of the CERT community, industry, and internet infrastructure they devised a three-stage approach, consisting of intelligence, intervention, and investigation. All partners combined their botnet information and all botnets were tracked in real time using a university-developed tool. The goal was a notice and takedown for most of the botnets and a deeper investigation into some of them. Then one of the partners, a large internet service provider, found a botnet command and control server in their infrastructure. The partners started investigating and found a cluster of 143 malicious servers, seven of which were directly related to a botnet called Bredolab. At that point, Bredolab had been able to infect 30 million unique IP addresses. In a ten-week period the partners were able to draw a picture of the botnet infrastructure. They were also able to identify the suspected operator of the network, an Armenian who planned to come to the Netherlands for a dance party. The network was set to be dismantled on the day the Armenian was to arrive at Amsterdam airport. The Armenian was to be arrested on arrival but due to visa problems he never showed up. Instead, he noticed someone attacking his botnet, assumed it was a competitor and fought back. After trying several backdoors, he decided to DDoS what was left of his own botnet. Due to good international cooperation, the command and control server of the DDoS botnet was quickly dismantled. An Interpol red notice led to the arrest of the suspect the following day at Yerevan airport. He was convicted in Armenia and sentenced to four years' imprisonment.

7.5 Tools of international cooperation

International cooperation in cybercrime cases is based on the same rules applicable to mutual legal assistance, mutual recognition, surrender and extradition in the Netherlands.

7.5.1 Mutual Legal Assistance

The Netherlands receives a large part of its requests for mutual legal assistance (MLA) or for mutual recognition from other EU Member States. Both these categories of requests can be sent directly to (regional) public prosecutor's offices – the offices for international legal assistance in criminal matters (IRCs). They are responsible for the efficient and speedy execution of requests. The establishment of the IRCs in 2003 significantly improved the efficiency with which MLA requests were handled, as IRC staff are now fully devoted to the issue of MLA, whereas before prosecutors dealt with the provision of MLA as part of their regular jobs. The IRCs also function as knowledge and expertise centres for international assistance. Judicial authorities in other Member States may approach their counterparts in the Netherlands directly, but they would then involve the competent IRC. The IRCs have been set up in the Netherlands exclusively to register, deal with and coordinate the execution of MLA requests in criminal matters.

For countries outside the EU, the Minister of Security and Justice in the Netherlands is the central authority in international judicial cooperation in criminal matters and receives all requests for MLA either directly or through diplomatic channels. Upon receipt of a request, the Ministry of Security and Justice, represented by the Office for International Legal Assistance in Criminal Matters (Afdeling Internationale Rechtshulp in Strafzaken, AIRS) verifies that all legal requirements under Dutch law, such as (if necessary) dual criminality and the existence of a treaty basis, are met. Requests that fall within the competence of the regional prosecutor are forwarded to the relevant regional IRC for execution. Cases falling within the competence of the National Public Prosecutor's Office are dealt with by the national IRC (LIRC).

In addition to formal MLA, police-to-police cooperation may occur. If information on data is shared before a formal request for transfer is received, the information may be shared on a police-to-police basis with the consent of prosecutor, and with the note that the information may only be used for investigative purposes. However, the requesting country must send a formal MLA request for transfer to be able to use the information as evidence in criminal proceedings. In some specific cases countries including the Netherlands send information spontaneously to other states.

The 24/7 contact point for urgent requests is incorporated into the National High Tech Crime Unit (NHTCU), which liaises closely with the national prosecutor on high-tech crime. The National Prosecutor's Office assesses the request and decides, with the National High Tech Crime Unit of the police, whether the request should be executed by the National High Tech Crime Unit or by the regional units of the police. If the latter is the case, the National Prosecutor's Office will forward the request to a local IRC office.

The police authorities indicated that one of the most difficult aspects of cooperation is to find the location of data in the cloud. Even though a provider can be ordered to supply certain data, this often turns out to be very difficult in practice. There are providers who do not cooperate with the police ("rogue providers"). Sometimes, a provider cannot be found or is established in a country with which the Netherlands maintains a very limited relationship of legal assistance.

The following statistics comprise formal MLA and police-to-police information:

INCOMING

Searched terminology	**2012**	**2013**
• computer crime • cybercrime • EAW ICT criminality • internet fraud • child pornography	1111	1270

OUTGOING

Searched terminology	**2012**	**2013**
• computer crime • cybercrime • EAW ICT criminality • internet fraud • child pornography	103	226

On average a first response is given within 24 hours. This may be an indication of the actual time needed for the required assistance.

The following actions may be requested via MLA in respect to cybercrime:

- Ordering of data (126na as well as 126nc, 126nd, 126nf of the DCCP)
- Preservation of computer data (126ni of the DCCP)
- Search and seizure of information system/computer data (inter alia 125i of the DCCP)
- Real-time interception/collection of traffic and content data (126m of the DCCP)

7.5.2 Mutual recognition instruments

No specific statistics have been provided with regard to the application of various mutual recognition instruments.

7.5.3 Surrender/Extradition

No specific statistics have been provided with regard to surrender/extradition cases focused solely on cybercrime.

7.6 Conclusions

- The Dutch police cooperates closely with Europol/EC3. This is also regarded as a priority of the NCSS2. The priorities defined at European level (EMPACT in particular) are reflected in the police priorities. The Dutch authorities also appreciate cooperation with Eurojust, actively supporting actions undertaken with the involvement of the Netherlands.

- The evaluation team realised that there is good cooperation with Eurojust and Europol/EC3 at the national level provided by the National Public Prosecutor's Office and the National Police. However, the representatives of the local level authorities met during the on-site visit seemed not to be well informed on the possibilities offered specifically by Eurojust or ENISA. This leaves some room for improvement.

- The Netherlands declares that it actively pursues national and international alliances and engages in international cooperation on the investigation of cybercrimes on bilateral terms, and if needed by creating JITs.

- The Dutch authorities work on developing cyber security capability in third countries through bilateral or regional initiatives specifically to protect the most vulnerable sectors and groups. The Netherlands is promoting this approach internationally, e.g. at the United Nations or during international cyberspace conferences. The decision to organise the Global Cyber Space Conference in 2015 highlights the international involvement of the Netherlands with regard to cyber issues.

- The agreement between the USA and the Netherlands that empowers Dutch authorities to send direct legal assistance requests to US companies should be considered as an appropriate tool to speed up investigations.

- Cooperation with Interpol seems to be good. The Netherlands has developed a model cooperation with the private sector. This approach helps the fight against online child exploitation and other cyber phenomena, e.g. botnets. The voluntary model of "Notice and take down" may also serve as best practice to stimulate self-regulation in the industry and thus to remove illegal content from their websites.

- MLA requests from EU Member States may be sent directly to competent IRCs which are a part of the Public Prosecutor's Office. IRC staff consists of both law enforcement officers and public prosecutors. According to the evaluators, the experience of the National Public Prosecutor's Office as a centre of expertise to take care of investigations on high-tech cybercrime or to deal with more complex MLA requests in this area and to coordinate and provide support to the district prosecutors in other investigations or MLA requests dealing with digital evidence seems to be effective and thus worth considering.

- Requests sent from non-EU countries are dealt with by the Ministry of Security and Justice, represented by the Office for International Legal Assistance in Criminal Matters (AIRS), which verifies that all legal requirements under Dutch law, such as (if necessary) dual criminality and the existence of a treaty basis, are met.

- In addition to formal MLA, police-to-police cooperation may be available. If information on data is shared before a formal request for transfer is received, the information may be shared on a police-to-police basis with the consent of prosecutor, and with the note that the information may only be used for investigative purposes.

- The Dutch authorities declared that close cooperation and information exchange between the various entities involved in international cooperation is of the utmost importance. The statistics from 2012 and 2013 show a growing trend in the number of incoming and outgoing cyber-related MLA requests.

8. TRAINING, AWARENESS-RAISING AND PREVENTION

8.1. Specific training

The training and study centre for the judiciary (Studiecentrum Rechtspleging; SSR) provides initial training programs and offers advanced education for judges, public prosecutors and legal staff, based on the principle that learning and continuing education remain essential throughout careers in the judiciary. SSR offers practical programs, courses, training, coaching and management development programs, including a dedicated module on digital investigation (comprising an interception course and a basic cybercrime course).

Moreover, the judiciary has invested in additional training on cybercrime. The courts have set up an Expertise Centre on Cybercrime at the Appeal Court of the Hague which employs two judges and a clerk. The Expertise Centre on Cybercrime publishes and distributes a newsletter which includes news on cyber-related issues such as recent publications, conferences, seminars and their outcomes, basic information on ongoing criminal cases involving cybercrime, case law, legislation and regulations applied, and explanations of basic terms relating to cybercrime.

The Public Prosecutor's Office has appointed dedicated prosecutors in the districts and in the National Public Prosecutor's Office. An internal network has also been established to raise prosecutors' awareness on cybercrime issues. Also several investigating judges have specialised in cybercrime. Although in theory every public prosecutor and judge is able to work on cybercrime cases, the opinion expressed by the practitioners met by the evaluation team clearly showed a need for additional advanced training on cybercrime.

The police provides custom training courses of an average of four days per course. Provision is made for digital experts to receive four weeks' additional training a year to keep their knowledge and skills up to date. For 2014 the training costs were estimated at EUR 300 000. Especially for proper training of digital investigators, a substantially larger amount would result in more capacity and expertise. This would help with investigations into cybercrime and the acquisition of digital evidence. However, it should be mentioned that a part of the budget of EUR 13.8 million allocated by the Minister of Security and Justice to the police is dedicated to education of the police with regard to cybercrime.

8.2. Awareness-raising

In the opinion of the Dutch authorities, raising awareness of cyber issues is a continuous challenge, and therefore needs special periodic attention. Since 2012 the Ministry of Security and Justice has organised a yearly campaign week for raising awareness on cyber security. The week is called Alert Online and is organised with the help of several ministries and private partners. Alert Online focuses on creating awareness among government parties, business and citizens. In 2014 the programme spanned over almost two weeks. It was connected to the annual European Cyber Security Month. The programme for the week consisted of contributions by public and private organisations.

Awareness of risks and knowledge of possible actions that can be taken to reduce them are key for cyber security. In 2013 various campaigns and initiatives were launched, such as:

- Cyber Security Month (October 2013, ENISA);
- Alert Online (28 October - 5 November 2013);
- Safe online banking (NVB);
- Safer Internet Day 83 (February 2014, DigiBewust).

The education taskforce is one of the central themes in the NCSS2. In order to enlarge the pool of cyber security experts and enhance users' proficiency with cyber security, the business community and the government have joined forces to improve the quality and breadth of ICT education at all academic levels (primary, secondary and professional education). A public-private partnership taskforce on cyber security education has been set up. It will focus on giving advice about the cyber security curriculum, in relation to the certification of information security experts and the further development of learning modules. Connections are being sought with current initiatives regarding information sciences education and the Technology Pact 2020.

8.3. Prevention

In the opinion of the Dutch authorities, private individuals are expected to apply basic security measures and to take a certain amount of personal responsibility. For their part, the government and the business community facilitate this by improving their digital skills and by emphasising their duty of care with respect to their clients. This also includes offering secure ICT products and services. The government plays a more active role in the digital domain. On the one hand, by increasing investments in the security of its own networks and services and, on the other hand, by bringing parties together and by taking action if the security of companies and private individuals or the latter's privacy come under threat. Where necessary, the government has established frameworks and standards, for instance with regard to the security requirements of vital services and processes.

The National Cyber Security Strategy has a strong focus on research and innovation. This is set out through:

- maintaining relations with science and research institutes;
- initiating and coordinating research;
- participating in research;
- promoting cooperation at national and international level and between the private sector and research institutions.

As mentioned above, the taskforce on cyber security education is one of the main actions to fulfil the objectives of the strategy in the NCSS2. Another central theme in the NCSS2 is innovation. There is a need for more coordination of supply and demand, which can be achieved by linking innovation initiatives to leading sector policy. In addition, the government, the business community and the world of academia will launch a cyber security innovation platform where start-ups, established companies, students and researchers can connect, inspire one another and attune research supply and demand with regard to general themes such as security-by-design and privacy-by-design.

In order to raise security and trust among citizens and the security and trustworthiness of infrastructure, the National Cyber Security Research Agenda (NSCRA) has been established.
The objectives of the NCSRA are:

- to improve the security and trustworthiness of the ICT infrastructure and ICT services;
- to prepare the Netherlands for the security challenges of the next 6-12 years;
- to stimulate the Dutch security economy and promote innovation in this sector;
- to strengthen and broaden Dutch security research by fostering cooperation between knowledge institutions and relevant public and private organisations.

8.4. Conclusions

- It seems that the Netherlands has established an easily accessible training programme for judges and prosecutors with regard to cybercrime. Training sessions are offered on a regular basis at national level at the training and study centre for the judiciary.

- In addition, the judiciary has invested in setting up an Expertise Centre on Cybercrime at the Appeal Court of the Hague which provides judges with specialised training on cybercrime according to their needs and periodically publishes a newsletter to raise judges' awareness and knowledge of the latest trends, legislation and events related to cybercrime.

- The Prosecution Service has established an internal network for prosecutors, from which every prosecutor assigned to a cybercrime case may get knowledge on cybercrime-related issues. The police also provides training specifically for digital investigators.

- In the opinion of the evaluators, both initiatives such as the Expertise Centre on Cybercrime and the internal network within the Prosecution Service serve well to increase knowledge of the practitioners with regard to cybercrime. Therefore, they should be considered as an example of best practice.

- Although training in this field is available to all stakeholders involved in handling cybercrime cases, participation is still voluntary. The evaluation team was informed that most judges do not deal on a daily basis with cybercrime cases since not many cases are sent to courts. General training could help avoid conflicting court decisions, as referred to during the on-site visit. Therefore, more mandatory participation could also be considered at least for those judges and prosecutors who are likely to deal with cyber criminality and mutual assistance related thereto.

- In addition, in the opinion of the evaluators further training should be offered to personnel who do intake of reports, as well as assistance of them by a support unit for digital investigations. During the on-site visit some opinions were presented that sometimes police officers are not properly prepared to handle these situations on their own. The current method includes only the regional support units to help at local level, not direct and useful preparation to handle the situation. Also, the regional support unit may have capacity problems if the number of complaints rises unexpectedly.

- Prevention and awareness-raising as well as training and capacity building are some of the main pillars of the strategy, in addition to legislation and cooperation. Since the individual is often the weakest link when it comes to cyber security, effective prevention and awareness-raising measures can go a long way. There are a number of practical examples where the Netherlands has already implemented such measures (e.g. the "Hang op, klik weg, bel uw bank" campaign by the Dutch Banking Association). This also means that the strategy is being actively used and implemented.

- The evaluation team realised that the Netherlands has invested lots of recourses in awareness-raising campaigns. The target is to create awareness among government parties, business and citizens. However, it was not clear if a comprehensive communication strategy has been developed to reach all citizens in relation to situations in which they might be potentially endangered by cybercrime.

9. FINAL REMARKS AND RECOMMENDATIONS

9.1. Suggestions from the Netherlands

From the Dutch perspective three issues need to be strengthened to raise the capacity to fight against cyber criminality:

- improving international agreement on jurisdiction in cyberspace;
- improving international cooperation in cybercrime cases, for example through Europol/EC3 and Interpol;
- providing capacity building in countries that are targets and/or origins of cybercrime, to ensure their capacity and enhance joint prevention efforts and investigations.

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 the Netherlands was able to satisfactorily review the system in the Netherlands.

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

The evaluation team thought it fit to make a number of suggestions for the attention of the Dutch authorities. Furthermore, based on the various good practices, related recommendations to the EU, its institutions and agencies, Eurojust, Europol and ENISA, are also put forward.

9.2.1 Recommendations to the Netherlands

1. The Netherlands should develop a mechanism to provide detailed, standardised and comprehensive statistics on investigations, prosecutions and convictions and reported incidents related to cybercrime making it possible to check overall cybercrime figures at the national level; (cf. 3.3 and 3.5)

2. The Netherlands should consider extending the obligation of private companies, such as internet providers, to report cyber incidents of a criminal nature to law enforcement or other public institutions and make it more mandatory; (cf. 4.4.1, and 4.5)

3. The Netherlands should be encouraged to finish the reform of the police at the regional level to strengthen their capacity to fight cybercrime and to ensure that they are sufficiently trained and funded; (cf. 4.4.2, 4.5 and 6.4)

4. The Netherlands should consider developing a common definition of cybercrime for statistical purposes to be applied as a basis for a broad common understanding of the same concept among those involved in fighting cyber criminality, such as law enforcement, the Prosecution Service and courts; (cf. 5.1 and 5.5)

5. The Netherlands should explore the possibilities for establishing a more balanced approach between the protection of governmental institutions and critical national infrastructures and the protection of citizens, in order to improve citizens' resilience to cybercrime; (cf. 6.1.2 and 6.4)

6. The Netherlands should look into further improving the public communication strategy, such as the one applied to combat online child abuse, to cover citizens who may be affected by different forms of cybercrime; (cf. 6.1.2 and 6.4)

7. The Netherlands should develop a comprehensive programme of training on cybercrime issues for all stakeholders involved in fighting cybercrime and on the possibilities offered by Eurojust, Europol and ENISA in that regard, including police officers, prosecutors and judges; (cf. 4.5, 7.1.1, 7.6, 8.1 and 8.4)

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

1. The Member States are encouraged to develop a consistent definition of cybercrime to be applied by all stakeholders involved in fighting cyber criminality in order to be able to provide detailed, standardised and comprehensive statistics on cybercrime figures at the national level; (cf. 3.3, 3.5, 5.1 and 5.5)

2. The Member States should consider developing useful tools to assist and facilitate the work of prosecutors and judges dealing with cyber criminality, such as specialised units dealing with cybercrime and/or a network of prosecutors handling these cases within the Prosecution Service or an Expertise Centre on Cybercrime at the Appeal Court of the Hague; (cf. 4.1.1, 4.5 and 8.1)

3. The Member States should seek to set up solutions to cover the gap resulting from the lack of legal measures allowing data in the cloud to be located and accessed; (cf. 4.1.2, 5.4.3, 5.5 and 7.5.1)

4. The Member States should consider exploring the benefits and feasibility of applying the successful example of the ECTF in the Netherlands in combating digital banking fraud more effectively, specifically phishing and banking malware; (cf. 4.3, 5.1.2 and 6.4)

5. The Member States should consider setting up a form of cooperation with the private sector aimed at protecting their country's vital sectors (energy companies, and the telecommunications and financial sectors), such as the NCSC in the Netherlands; (cf. 4.3, 4.4.2, 4.5 and 6.1.2)

6. The Member States should consider the Dutch practise of combining the possibilities offered by private companies (such as ISPs and social media companies), public entities (e.g. the Ministry of Security and Justice and specialised units dealing exclusively with combating online child abuse) and public campaigns to efficiently combat online child sexual abuse, as an example of best practise; (cf. 6.2.1 - 6.2.4 and 6.4)

7. The Member States should provide their practitioners with practical guidelines aimed at raising the awareness of local-level authorities (specifically law enforcement and the Prosecution Service) on the powers and the services of Eurojust, Europol and ENISA with regard to cybercrime; (cf. 4.5, 7.1.1, 7.6, 8.1 and 8.4)

8. The European institutions should secure and increase the provision of EU funding to help combat cybercrime, for example for setting up JITs through Eurojust; (cf. 3.4 and 7.1.3)

9.2.3 Recommendations to Eurojust/Europol/ENISA

1. Eurojust, Europol and ENISA should consider raising awareness of the services and possibilities for cooperation that they offer with regard to cybercrime; (cf. 7.3 and 7.6)

2. Eurojust, Europol and ENISA should consider actively supporting events that strengthen international cooperation with regard to combating cybercrime, such as the Global Cyber Space Conference; (cf. 7.3 and 7.6)

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

7th Round of Mutual Evaluations - The Netherlands – 17-21 NOVEMBER 2014

Monday 17-11 Den Haag

- PM arrival GENVAL experts in Den Haag (expected in the afternoon)
- Between 17.30 – 19.00 Informal meeting and introductions in hotel bar.

Tuesday 18-11 Den Haag

- 9.00 – 9.30 Reception at Ministry of Security and Justice (Turfmarkt 147)
- 9.30 – 10.00 Welcoming speech and introduction by Mr. Arie Ijzerman, deputy Director general, Director Law Enforcement Department (DGRR)
- 10.00 -11.00 Dutch criminal law system; introduction and overview (Erik Planken from DGRR/DRC en Frans van de Doelen / Pim Albers from DGRR/DRB)
- 11.00-11.15 Coffee Break
- 11.15-11.30 translocate to the National Cyber Security Center (in the same building)
- 11.30-13.00 Visit National CyberSecurityCentre (NCSC): information on policies and operational tasks (Michel van Leeuwen/Aart Jochem)
- 13.00-14.30 Lunche at the Ministry
- 14.30-15.30 Law Enforcement in the Netherlands (policies towards and the governing of police and prosecution service (Jacos van Zelst from Directorate General Police en Erik Planken from DGRR/DRC)
- 15.30-15.45 Coffee / Tea Break
- 15.45 -16.45 Information on Dutch judicial framework and on the draft legistative proposal to enhance law enforcement powers (Luut Mol Lous from the legislative department)
- 17.00-17.30 Closing

Woensdag 19-11 Driebergen (national police, national unit; national crime squad, Team High Tech Crime, National program against child sexual abuse)

- 08.30- 10.00 travel to Driebergen (transport will be provided)
- 10.00- 10.30 Welcome and introduction by Mr. Wilbert Paulissen (Head of the Central Criminal Investigation Department of the national unit of the national police)
- 10.30- 12.00 visit to the electronic crimes taskforce (ECTF) and introduction to the national crime squad by Eric van Schilt (project leader (ECTF) en Michel Zandbergen (ABNAMRO banc)
- 12.00 – 13.30 Luncheon with Mr. Wilbert Paulissen and teamleads THTC
- 13.30-14.30 Introduction of the High Tech Crime Unit ((THTU): organisation, growth, tasks and working processes by outreach officers THTC (Peter Zinn THTU)
- 14.30 – 16.00 Visit of workstations THTC and information on practice, working processes, international cooperation and cases)
- 16.00 – 16.00 Information on the Dutch approach of child sexual abuse, online and offline, as well in other countries by Mr. Ben van Mierlo (National Program child abuse ,NPKK)
- 17.00 -18.00 travel to Den Haag (transport will be provided)
- 19.30- 22.00 Dinner with presence of Mr. Jan Willem Schaper (Director Police Department of the ministry of Security and Justice)

Donderdag 20-11 Rotterdam (National prosecution's service, Dutch judiciary and the Rotterdam regional unit of the national police)

- 09.00- 10.00 travel to Rotterdam (transport will be provided)
- 10.00 -10.30 Welcome and introduction by Mr. Fred Westerbeke , Chief prosecutor of the national crime unit of the Dutch prosecution service
- 10.30 – 11.45 Information by Mr. Lodewijk van Zwieten, national coordinating prosecutor for cyber crimes on de Dutch practice, prosecution dilemmas, mutual legal assistance and international cooperation

11.45 – 12.00 Coffee Break

- 12.00 – 13.15 Information by Mr. Christiaan Baardmans, Judge in the Court of Appeal Den Haag and in the Dutch Expertise Centre on Cybercrime
- 13.15 – 14.30 Luncheon in the building of the national crime unit of the Dutch prosecution service
- 15.00 – 17.30 Visit to the Rotterdam regional unit of the National police: information on practice, working processes, international cooperation and cases (Erik Venema Police)
- 17.30 – 18.00 Closing, inventory of possible follow up interviews on Friday 21
- 18.00- 19.00 travel to Den Haag (transport will be provided)

Vrijdag 21-11 Den Haag

- 09.30 – 10.00 Start up with coffee
- 10.00 - 12.30 closed session for Genval experts and, or, possibility for extra exchange of views, interviews, etc.
- PM 12.30 – 13.00 Closing with light luncheon

-/-

ANNEX B: PERSONS INTERVIEWED/MET

Meetings 18 November 2014

Venue: Ministry of Security and Justice, The Hague

Person interviewed/met	Organisation represented
Arie Ijzerman	Ministry of Security and Justice
Erik Planken	Ministry of Security and Justice
Michel van Leeuwen	National Cyber Security Centre
Aart Jochem	National Cyber Security Centre
Joost Raeven	Ministry of Security and Justice
Barbara Perels	Ministry of Security and Justice

Venue: Directorate General Police, the Hague

Person interviewed/met	Organisation represented
Jacos van Zelst	Directorate General Police
Erik Planken	Ministry of Security and Justice
Luut Mol Lous	Ministry of Security and Justice

Meetings 19 November 2014

Venue: Police, Central Criminal Investigation Department, Driebergen

Person interviewed/met	Organisation represented
Inge Philips	Central Criminal Investigation Department
Eric van der Schild	Electronic Crimes Taskforce
Michel Zandbergen	ABN AMRO Bank
Roelandt van Zeijst	High Tech Crime Unit
Marjin Schuurbiers	Central Criminal Investigation Department
Peter Zinn	National High Tech Crime Unit
Ben van Mierloo	National Programme against Child Abuse

Meetings 20 November 2014

Venue: National Prosecution Service, Rotterdam

Person interviewed/met	Organisation represented
Sander de Haas	Public Prosecution Office
Lodewijk van Zwieten	Public Prosecution Office
Lisanne van Dijk	Public Prosecution Office
Odette Zonneveld	Public Prosecution Office
Christiaan Baardmans	Court of Appeal, The Hague

Venue: Regional Unit of the National Police, Rotterdam

Person interviewed/met	Organisation represented
Rob Hokke	National Police
Erik Venema	National Police
Erik Planken	Ministry of Security and Justice

Meetings 21 November 2014

Venue: Ministry of Security and Justice, The Hague

Person interviewed/met	Organisation represented
Erik Planken	Ministry of Security and Justice
Joost Raeven	Ministry of Security and Justice

-//-

ANNEX C: LIST OF ABBREVIATIONS/GLOSSARY OF TERMS

LIST OF ACRONYMS, ABBREVIATIONS AND TERMS	DUTCH OR ACRONYM IN ORIGINAL LANGUAGE	DUTCH OR ACRONYM IN ORIGINAL LANGUAGE	ENGLISH
ACM	*ACM*		Netherlands Authority for Consumers and Markets
AIRS	*AIRS*	*Afdeling Internationale Rechtshulp in Strafzaken*	Office for International Legal Assistance in Criminal Matters
AIVD	*AIVD*		Public Prosecution Service, General Intelligence and Security Service
CBS	*CBS*		Central Bureau for Statistics
CBP	*CBP*	*College Bescherming Persoonsgegevens*	The Dutch Data Protection Agency
CSAN	*CSAN*		Cyber Security Assessment Netherlands
DCCP	*DCCP*	*Wetboek van Strafvordering*	Dutch Code of Criminal Procedure
DefCERT	*DefCERT*		Defense CERT
DNB	*DNB*		Dutch National Bank
FIOD	*FIOD*	*Fiscale inlichtingen- en opsporingsdienst*	Fiscal Information and Investigation Service
GovCert	*GovCert*		Dutch Government Computer Emergency Response Team

IGCI	*IGCI*		Interpol Global Complex for Innovation
ISP	*ISP*		Internet service providers
ITOM	*ITOM*		Illegal Trade on Online Marketplaces
NCC	*NCC*		National Crisis Centre
NCSC	*NCSC*		National Cyber Security Centre
NCTV	*NCTV*		National Coordinator for Security and Counterterrorism
NHTCU	*NHTCU*		National High Tech Crime Unit
NFI	*NFI*		Dutch Forensic Institute
NRN	*NRN*		National Response Network
NVB	*NVB*	*Nederlandse Vereniging van Banken*	Dutch Banking Association
RNLM	*RNLM*		Royal Netherlands Marechaussee
SSR	*SSR*	*Studiecentrum Rechtspleging*	Training and study centre for the judiciary
Wbp	*Wbp*	*Wet bescherming persoonsgegevens*	The Dutch Data Protection Act
Wpg	*Wpg*	Wet politiegegevens	the Police Data Act
WWN	*WWN*		Watch and Warning Network

ANNEX D: DUTCH CRIMINAL CODE AND CYBER CRIMES

Illegal access to information system = computervredebreuk		
Art. 2 Cybercrime Convention	Art. 3 EU Dir 2013/40	Art. 138ab, par 1, Dutch Criminal Code
Definition used	Any person who intentionally and unlawfully gains entry to a computerised device or system or a part thereof shall be guilty of computer trespass: Unlawful entry shall be deemed to have been committed if access to the computerised device or system is gained: a. by breaching a security measure, b. by a technical intervention, c. by means of false signals or a false key, or d. by assuming a false identity.	
Intent/recklessness	-	
Aggravating/mitigating	Aggravating= 1. if the offender subsequently copies the data stored, processed or transferred by means of the computerised device or system, which he has unlawfully accessed, and copies, intercepts or records such data for his own use or that of another. 2. Computer trespass committed via a public telecommunication network, if the offender subsequently: a. with the intention of benefitting himself or another unlawfully, uses processing capacity of a computerised device or system; b. accesses the computerised device or system of a third party via the computerised device or system to which he has unlawfully gained entry.	
Minimum/maximum penalty	Max: a term of imprisonment not exceeding one year or a fine of the fourth category (to be raised to two years) Max: aggr 1 / 2 : a term of imprisonment not exceeding four years or a fine of the fourth category	
Multiple crimes/ recidivism	See general rules	
Incitement, aiding, abetting, and attempt	See general rules	

Illegal system interference = stoornis in een geautomatiseerd werk veroorzaken		
Art. 5 Cybercrime Convention	Art. 4 EU Dir 2013/40	Art. 138b, art. 350a Dutch Criminal Code, and art. I, par G, draft proposal for national implementation directive
Definition used	(Section 138b) Any person who intentionally and unlawfully hinders the access to or use of a computerised device or system by offering or sending data to it (Section 350a) 1. Any person who intentionally and unlawfully alters, erases, renders unusable or disables data stored, processed or transferred by means of a computerised device or system or by means of telecommunication, or adds other data thereto G draft proposal for national implementation directive Na artikel 350b worden twee artikelen ingevoegd, luidende: (Artikel 350c) 1. Hij die opzettelijk enig geautomatiseerd werk of enig werk voor telecommunicatie vernielt, beschadigt of onbruikbaar maakt, stoornis in de gang of in de werking van zodanig werk veroorzaakt, of een ten opzichte van zodanig werk genomen veiligheidsmaatregel verijdelt, indien daardoor wederrechtelijk verhindering of bemoeilijking van de opslag, verwerking of overdracht van gegevens of stoornis in een telecommunicatienetwerk of in de uitvoering van een telecommunicatiedienst, ontstaat. 2. Artikel 138b, tweede en derde lid, is van overeenkomstige toepassing.	
Intent/recklessness	- intent is presumed	
Aggravating/mitigating	Aggravating= 1. Any person who commits the offence defined in subsection (1) after having unlawfully gained access and causes serious damage to such data 2. who intentionally and unlawfully makes available or disseminates data that is intended to cause damage Mitigating = Any person who commits the offence defined in subsection (3) with the intention of limiting the damage resulting from such data	

Minimum/maximum penalty	Max: in case of interference = a term of imprisonment not exceeding one year or a fine of the fourth category (to be raised to two years) In case of altering, deleting, etc: , a term of imprisonment not exceeding two years or a fine of the fourth category. Max: aggr 1 / 2 : a term of imprisonment not exceeding four years or a fine of the fourth category Mitigating = shall not be criminally liable
Multiple crimes/ recidivism	See general rules
Incitement, aiding, abetting, and attempt	See general rules and Current art. 139d, par 2 Any person who: a. manufactures, sells, obtains, imports, distributes or otherwise makes available or has in his possession a technical device that has been primarily adapted or designed for the commission of such serious offence, or b. sells, obtains, distributes or otherwise makes available or has in his possession a computer password, access code or similar data that can be used for accessing a computerised device or system or a part thereof; with the intention of using it in the commission of a serious offence, as referred to in section 138ab(1), 138b or 139c, shall be liable to a term of imprisonment not exceeding one year or a fine of the fourth category. G draft proposal for national implementation directive (Artikel 350d) hij die, met het oogmerk dat daarmee een misdrijf als bedoeld in artikel 350a, eerste lid, of 350c wordt gepleegd: a. een technisch hulpmiddel dat hoofdzakelijk geschikt gemaakt of ontworpen is tot het plegen van een zodanig misdrijf, vervaardigt, verkoopt, verwerft, invoert, verspreidt of anderszins ter beschikking stelt of voorhanden heeft, of b. een computerwachtwoord, toegangscode of daarmee vergelijkbaar gegeven waardoor toegang kan worden verkregen tot een geautomatiseerd werk of een deel daarvan, vervaardigt, verkoopt, verwerft, invoert, verspreidt of anderszins ter beschikking stelt of voorhanden heeft.

Illegal data interference = opzettelijk vernielen, verstoren of onbruikbaar maken van computers of computernetwerken		
Art. 4 Cybercrime Convention	Art. 5 EU Dir 2013/40	Art. 350a Dutch Criminal Code (NB hoe zit het met 350b???)
Definition used	(Section 350a) 1. Any person who intentionally and unlawfully alters, erases, renders unusable or disables data stored, processed or transferred by means of a computerised device or system or by means of telecommunication, or adds other data thereto (section 350b) 1Any person who, through negligence, causes data stored, processed or transferred by means of a computerised device or system to be altered, erased, rendered unusable or disabled, or causes other data to be added thereto, if this causes serious damage to that data, 2Any person who, through negligence, causes data stored, processed or transferred by means of a computerised device or system to be altered, erased, rendered unusable or disabled, or causes other data to be added thereto, shall, if this causes serious damage to that data, G draft proposal for national implementation directive Na artikel 350b worden twee artikelen ingevoegd, luidende: (Artikel 350c) 1. Hij die opzettelijk enig geautomatiseerd werk of enig werk voor telecommunicatie vernielt, beschadigt of onbruikbaar maakt, stoornis in de gang of in de werking van zodanig werk veroorzaakt, of een ten opzichte van zodanig werk genomen veiligheidsmaatregel verijdelt, indien daardoor wederrechtelijk verhindering of bemoeilijking van de opslag, verwerking of overdracht van gegevens of stoornis in een telecommunicatienetwerk of in de uitvoering van een telecommunicatiedienst, ontstaat. 2. Artikel 138b, tweede en derde lid, is van overeenkomstige toepassing.	
Intent/recklessness	- Intent is presumed in 350a - Neglect is presumed in 350b	
Aggravating/mitigating	Aggravating= 1. Any person who commits the offence defined in subsection (1) after having unlawfully gained access and causes serious damage to such data 2. who intentionally and unlawfully makes available or disseminates data that is intended to cause damage. Mitigating = Any person who commits the offence defined in subsection (3) with the intention of limiting the damage resulting from such data	

Minimum/maximum penalty	350a Max: a term of imprisonment not exceeding two years or a fine of the fourth category Max: aggr 1 / 2 : a term of imprisonment not exceeding four years or a fine of the fourth category Mitigating = shall not be criminally liable 350b Max: a term of imprisonment not exceeding two years or a fine of the fourth category
Multiple crimes/ recidivism	See general rules
Incitement, aiding, abetting, and attempt	See general rules and 350a par 3 Any person who intentionally and unlawfully makes available or disseminates data that is intended to cause damage in a computerised device or system, shall be liable to a term of imprisonment not exceeding four years or a fine of the fifth category.

Illegal interception of computerdata = onrechtmatige onderschepping / gegevensdiefstal		
Art. 3 Cybercrime Convention	Art. 6 EU Dir 2013/40	Art. 139c, 139d Dutch Criminal Code
Definition used	(139c) Any person who intentionally and unlawfully intercepts or records by means of a technical device data which is not intended for him and is processed or transferred by means of telecommunication or by means of a computerised device or system. No liability in the following cases: • data received via a radio receiver • by or on the instructions of the person entitled to use the telecommunication connection • for the purpose of a good operation of a public telecommunication network, for the purpose of criminal proceedings, or for the purpose of implementation of the Intelligence and Security Services Act 2002. (139d par 1)Any person who has a technical device installed in a particular place with the intention of unlawfully using it to eavesdrop on, intercept or record a conversation, telecommunications or other type of data transfer or data processing by a computerised device or system	
Intent/recklessness	Intent is presumed	
Aggravating/mitigating	-	
Minimum/maximum penalty	Max: a term of imprisonment not exceeding one year or a fine of the fourth category (to be raised to two years)	
Multiple crimes/ recidivism	See general rules	
Incitement, aiding, abetting, and attempt	See general rules	

Misuse of devices = instrumenten voor het plegen van strafbare feiten / voorbereidingshandelingen onderschepping		
Art. 6 Cybercrime Convention	Art. 7 EU Dir 2013/40	Art. 139d Dutch Criminal Code
Definition used	(139d par 2) Any person who: a. manufactures, sells, obtains, imports, distributes or otherwise makes available or has in his possession a technical device that has been primarily adapted or designed for the commission of such serious offence, or b. sells, obtains, distributes or otherwise makes available or has in his possession a computer password, access code or similar data that can be used for accessing a computerised device or system or a part thereof;	
Intent/recklessness	Intent is presumed	
Aggravating/mitigating	Any person who commits the offence referred (1) with the intention of using it in the commission of a serious offence, as referred to in section 138ab(1), 138b or 139c (2) with a view to the commission of a serious offence as referred to in section 138a(2) or (3).	
Minimum/maximum penalty	Max: a term of imprisonment not exceeding one year or a fine of the fourth category (to be raised to two years) Aggr. 1: same penalty as in section 138ab(1), 138b or 139c = : a term of imprisonment not exceeding four years or a fine of the fourth category Aggr. 2: shall be liable to a term of imprisonment not exceeding four years or a fine of the fourth category.	
Multiple crimes/ recidivism	See general rules	
Incitement, aiding, abetting, and attempt	See general rules	

Computer-related production, distribution or possession of child pornography = kinderporno		
Art. 9 Cybercrime Convention	Art. 5 EU Dir 2011/92	Art. 240b Dutch Criminal Code
Definition used	Any person who distributes, offers, publicly displays, produces, imports, conveys in transit, exports, obtains, possesses or accesses by means of a computerised device or system or by use of a communication service an image - or a data carrier that contains an image - of a sexual act involving or seemingly involving a person who is manifestly under the age of eighteen years	
Intent/recklessness	-	
Aggravating/mitigating	Aggravating= Any person who makes a profession or habit of committing any of the serious offences defined in subsection (1	
Minimum/maximum penalty	Max: a term of imprisonment not exceeding four years or a fine of the fifth category Max: aggr 1: a term of imprisonment not exceeding eight years or a fine of the fifth category	
Multiple crimes/ recidivism	See general rules	
Incitement, aiding, abetting, and attempt	See general rules	

Computer-related solicitation or grooming of children = grooming / kinderlokken on line		
Art. 23 Lanzarote Convention	Art. 6 EU Dir 2011/92	Art. 248e Dutch Criminal Code
Definition used	The person who proposes to arrange a meeting, by means of an automated work or by making use of a communication service, to a person of whom he knows, or should reasonably assume, that such person has not yet reached the age of sixteen, with the intention of committing indecent acts with this person or of creating an image of a sexual act in which this person is involved, will be punished with a term of imprisonment of at most two years or a fine of the fourth category, if he undertakes any action intended to realise that meeting	
Intent/recklessness	-	
Aggravating/mitigating	-	
Minimum/maximum penalty	Max: a term of imprisonment of at most two years or a fine of the fourth category	
Multiple crimes/ recidivism	See general rules	
Incitement, aiding, abetting, and attempt	See general rules	

Computer-related fraud or forgery = computergerelateerde fraude en oplichting		
Art. 7, 8 Cybercrime Convention		Artt. 326/225 (phishing, fraud on online markets, advance fee fraud, "click" fraud), 232 (skimming), 310 (theft of virtual goods) 317/318/285 (embezzlement, / blackmail), 334 (market manipulation), 139e (fencing) Dutch Criminal Code
Definition used	(326) Any person who, with the intention of benefitting himself or another person unlawfully, either by assuming a false name or a false capacity, or by cunning manoeuvres, or by a tissue of lies, induces a person to hand over any property, to render a service, to make available data, to incur a debt or relinquish a claim; (232) • Any person who intentionally makes a false cash card, a stored value card, any other card available to the public or an identity data carrier available to the public that is intended for making or obtaining automated payments or other services, or falsifies such card or carrier, with the intention of benefiting himself or another, • Any person who intentionally uses the false or falsified pass or card as if it were genuine and unfalsified or intentionally delivers, possesses, receives, obtains, transports, sells or transfers such pass or card, while he knows or has reasonable cause to suspect that the pass or card is destined for such use (310) Any person who takes any property belonging in whole or in part to another person with the intention of unlawfully appropriating	
Intent/recklessness	Intent is presumed	
Aggravating/mitigating	(326) If the offence is committed with the intention of preparing or facilitating a terrorist offence	
Minimum/maximum penalty	Max: (326) a term of imprisonment not exceeding four years or a fine of the fifth category Aggr: term of imprisonment prescribed for the offence shall be increased by one third (232) a term of imprisonment not exceeding six years or a fine of the fifth category (310) a term of imprisonment not exceeding four years or a fine of the fifth category	
Multiple crimes/ recidivism	See general rules	
Incitement, aiding, abetting, and attempt	See general rules	

Controlling or sending spam = spam		
Art. 7, 8 Cybercrime Convention		art. 11 pr. 7 Telecommunications Act)
Definition used	NB strafbaarstelling Tw opzoeken (contact met OPTA???)	
Intent/recklessness	Intent is presumed	
Aggravating/mitigating	(225) If the offence is committed with the intention of preparing or facilitating a terrorist offence	
Minimum/maximum penalty	Max: (225) a term of imprisonment not exceeding four years or a fine of the fifth category Aggr: term of imprisonment prescribed for the offence shall be increased by one third	
Multiple crimes/ recidivism	See general rules	
Incitement, aiding, abetting, and attempt	See general rules	

Computer-related identity fraud = identiteitsfraude		
Art. 7, 8 Cybercrime Convention		Artt. 326/225 (phishing, fraud on online markets, advance fee fraud, "click" fraud
Definition used	(225) • Any person who makes a false document or falsifies a document that is intended to be used as evidence of any fact, with the intention that he or others shall use it as if it were genuine and unfalsified • Any person who intentionally uses such a false or falsified document as if it were genuine and unfalsified or intentionally delivers or possesses such a document, while he knows or has reasonable cause to suspect that this document is destined for such use (326) Any person who, with the intention of benefitting himself or another person unlawfully, either by assuming a false name or a false capacity, or by cunning manoeuvres, or by a tissue of lies, induces a person to hand over any property, to render a service, to make available data, to incur a debt or relinquish a claim; There is no specific article on identity fraud by means of useing credentials that are connected to another person. In those cases 326 is used.	
Intent/recklessness	Intent is presumed	
Aggravating/mitigating	(225) If the offence is committed with the intention of preparing or facilitating a terrorist offence	
Minimum/maximum penalty	Max: (225) a term of imprisonment not exceeding four years or a fine of the fifth category Aggr: term of imprisonment prescribed for the offence shall be increased by one third .	
Multiple crimes/ recidivism	See general rules	
Incitement, aiding, abetting, and attempt	See general rules	