Council of the
European Union

Brussels, 19 May 2017
(OR. en)

7160/1/17
REV 1 DCL 1

GENVAL 21
CYBER 37

DECLASSIFICATION

of document:	7160/1/17 REV 1 RESTREINT UE/EU RESTRICTED
dated:	2 May 2017
new status:	Public
Subject:	Evaluation report on the seventh round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating cybercrime" - Report on Ireland

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

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

Council of the
European Union

Brussels, 2 May 2017
(OR. en)

7160/1/17
REV 1

RESTREINT UE/EU RESTRICTED

GENVAL 21
CYBER 37

REPORT

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

ANNEX

Table of Contents

1. EXECUTIVE SUMMARY

The evaluation of Ireland took place between 27th-30th of June 2016 and included meetings with the relevant actors with responsibilities in the field of prevention and combating cybercrime as well as in the implementation and operation of European policies (Department of Justice and Equality, Department of Communications, Climate Action and Environments, Irish Police Force - An Garda Síochána, Office of the Director of Public Prosecutions).

Furthermore a visit to Criminal Courts Complex was scheduled where the evaluation team had the opportunity to meet with the Judiciary representatives (judges).

During the visit the Irish authorities made efforts to provide the evaluation team with complete information and clarifications on legal and operational aspects of preventing and combating cybercrime, cross-border cooperation and cooperation with EU-agencies, cyber strategy, etc.

Via these meetings the evaluation team had the opportunity to better understand the responses provided in the questionnaire and to fill the gaps where necessary.

There is a good level of Internet access in Ireland both at public and private level. As a consequence Ireland needs to pay an important attention to cyber security.

Many Internet Service Providers/Information Society Service Providers have established a presence in Ireland. In addition some of them hold/store process data in Ireland which makes it an important and vital partner in the fight against cybercrime.

In 2015 the Department of Communications, Climate Action and Environments published the Cyber Security Strategy for 2015-2017 setting out how Ireland will engage with the fast evolving world of digital technology and the Government's approach to facilitating the resilient, safe and secure operation of computer networks and associated infrastructure used both by Irish citizens and businesses. The Strategy identifies the risks posed by cyber-attacks and outlines the possible practices and steps which can be taken to mitigate against such attacks by individuals, corporations and State bodies. According to the strategy all the relevant bodies and institutions should continue to cooperate closely and coordinate with a view to ensuring an effective response to the cyber threats.

A National Cyber Security Centre exists on an administrative basis within the Department of Communications, Climate Action and Environments with responsibilities in three primary areas: government networks, personal and business systems and the protection of critical national infrastructure. This will build on the existing Computer Security Incident Response Team (CSIRT-IE), established in late 2011.

2. INTRODUCTION

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

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

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

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

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

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

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

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

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

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

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

The experts charged with undertaking the evaluation of Ireland were Ms Ioana Albani (Romania), and Mr Darius Zvironas (Lithuania). Two observers were also present: Ms Daniela Buruiana (Eurojust) and Mr Tjabbe Bos (European Commission), together with Ms Monica Kopcheva and Ms Carmen Necula from the General Secretariat of the Council.

This report was prepared by the expert team with the assistance of the General Secretariat of the Council, based on findings arising from the evaluation visit that took place in Ireland between 27 and 30 June 2016, and on Ireland's detailed replies to the evaluation questionnaire together with their detailed answers to ensuing follow-up questions.

3. GENERAL MATTERS AND STRUCTURES

3.1. National cybersecurity strategy

The Department of Communications, Climate Action and Environments (DCENR) published a cybersecurity strategy in 2015.[7] The strategy outlines how the government will 'engage with a dynamic and challenging aspect of developments in digital technology' and its approach to 'facilitating the resilient, safe and secure operation of computer networks and associated infrastructure used by Irish citizens and businesses'. The strategy document follows on from the government's action plan, entitled *New Connections: A strategy to realise the potential of the Information Society* (see Appendix).

The strategy is a comprehensive document which recognises that technology plays a central role in modern society and that it is a target for both industrial and terrorist attack. The document also includes plans to establish a National Cyber Security Centre within the Department of Communications, Climate Action and Environments, which already houses the national CSIRT and works closely with other agencies on identifying, preventing and detecting cybersecurity-related incidents. The strategy identifies the risks that cyber attacks pose to the public, corporate structures and the economy and outlines practices and steps that can help individuals, corporations and state bodies to mitigate against such attacks. It also outlines a number of government initiatives and EU directives which are designed to strengthen internet access and encourage online security in the public domain and other domains.

[7] http://www.dcenr.gov.ie/communications/SiteCollectionDocuments/Internet-policy/NationalCyberSecurityStrategy20152017.pdf

As stated in section 5.6 of the strategy, the Department of Communications, Climate Action and Environments will continue to work closely with the Department of Justice and Equality and other relevant agencies, including An Garda Síochána (Ireland's police service), on implementing forthcoming legislation which will allow for the full implementation of the Budapest Convention and the EU Directive on attacks against information systems. This association will be formalised by means of a Memorandum of Understanding setting out the roles and duties of each body.

The Computer Crime Investigation Unit of An Garda Síochána, Ireland's national police service, is tasked with the investigation of all cyber-related crimes and the forensic examination of computer media seized or surrendered in such incidents. The unit is the primary cyber unit within the police service and is staffed by qualified forensic experts and cybercrime investigators.

A review has identified the need to strengthen the resources of the unit and establish an intelligence capability along with a strengthened investigative arm. A revised public information webpage is currently being implemented for both public and corporate information in the areas of cybersecurity and cybercrime. In addition the unit works closely with CSIRT-IE, academia and the cybersecurity unit within the Irish Defence Forces in a collaborative approach to cybercrime and cybersecurity issues. As part of the policing initiative, the unit is currently undergoing review and is upgrading its technology and increasing the capability and numbers of its staff.

All of the CCIU's activities in tackling and investigating cybercrime are carried out in accordance with best practice and recognised standards.

3.2. National priorities with regard to cybercrime

As indicated in the National Cyber Security Strategy 2015-17, the state recognises the substantial risk posed by the threat of cybercrime. That risk is particularly great in light of the significant ICT presence in Ireland, with a large number of multinational technology corporations choosing to base their European headquarters and associated infrastructures there. The National Risk Assessment Report[8] acknowledges the threat of cyber attack and the increasing sophistication of the methods and tools used to carry out such attacks. In addition the national strategy recognises the risks cybercrime poses both nationally and personally to the public. It purports to set out the methods needed to protect and improve the cybersecurity of critical national infrastructure and emergency planning.

The Irish police service, An Garda Síochána, are in the process of drawing up a high-level strategy document which will set out the intended strategy for the future in terms of cybercrime and cybersecurity, the investigation of online crime and attacks on ICT systems, the prevention and public advice processes for cybercrime and cybersecurity issues, communication and cooperation with national and international partner agencies, the provision of training in the area of cybercrime for new and existing personnel, and the continuing review of practices in the light of new trends and methods for online offending. The strategy provides for the setting up of a national unit which will be tasked with developing a coordinated response to the threat of cybercrime by engaging with partner agencies and analysing and reporting threats and trends in offending. The high-level strategy is an ongoing project that has yet to be finalised and is not currently in the public domain.[9]

8 www.taoiseach.gov.ie/eng/publications/publications 2014/National Risk Assessment report 2014.

9 Since the evaluation visit An Garda Siochána has finalised the strategy and an implementation plan is being developed.

In addition, the Computer Crime Investigation Unit has identified critical improvements and investments which will enable it, as the national unit, to prepare for current and potential threats from cyber offending. This includes investment in terms of personnel, training, ICT infrastructure, budgets and intelligence gathering. The proposed restructuring is based on similar units in the United Kingdom, Europol and Denmark and includes a two-stranded approach involving strategic planning and operational activities. The proposal is currently under review.

3.3. Statistics on cybercrime

3.3.1. Main trends leading to cybercrime

Trends in cyber-related crime are constantly in a state of flux with new trends emerging all the time. It was not possible to provide a precise figure for the number of offences or the ratio of each type of offence as this information is not collated centrally. In addition current statistics do not refer to online offending as separate types of offence: attacks on computer systems would be classified as criminal damage and collated with all other damage offences regardless of type. The trends below are based on cases at hand at the Computer Crime Investigation Unit and do not include cases which have been reported to law enforcement but have not involved forensic examination of computer media. The following have been identified as current trends:

- Offences relating to child exploitative material continue to account for approximately 60 % of the cybercrime incidents examined by the Computer Crime Investigation Unit. The cases received at the unit are predominantly those involving allegations of possession of child pornography, and the exploitation of children over online forums and other such social networking platforms. In addition there has been an increase in the incidents of distribution of child exploitative material, the majority of which is sourced online by the sender rather than home-produced.

- Attacks on computer systems are recurrent. The number of cases fluctuates, with 2016 seeing a slight increase in website and network intrusions. However, reporting to law enforcement falls far short of the actual number of incidents. This may be for a number of reasons, including reluctance to report that the company's system has been breached in case it results in negative publicity.
- Online fraud, such as CEO fraud, '419 letter' scams and auction fraud, is trending at present with a number of reported incidents involving the successful deception of companies and subsequent payments being redirected to fraudulent accounts.
- Police ransomware, while not as prevalent as before, continues to occur with some regularity and in some cases has resulted in people making voluntary admissions that they were in possession of child exploitative material.
- Ransomware is on the increase and many companies and individuals have become victims of this type of criminal activity in recent months.
- Distributed denial of service attacks and related offences continue to rise. In January 2016 there was a very specific DDoS attack against Irish government networks and some financial institutions. DDoS attacks take a number of forms:
    - attacks by hacktivists where no warning is given or demands made of the victims (Anonymous);
    - DDoS attacks where victims are forewarned and asked to pay a ransom to prevent an attack on their network (DD4BC & Armada Collective);
    - scam DDoS attacks where criminals send an email advising the victim to pay a ransom but do not execute a DDoS attack against the victim company (Lizard Squad).

- Online sexploitation is increasing, with regular reports of individuals being blackmailed as a result of being coerced into performing sexual acts online. These cases can be particularly heinous as the victims are often exposed to their family even after they have cooperated with the demands made of them.
- Cyberbullying continues to present problems.

3.3.2. Number of registered cases of cybercrime

Cybercrime is not classified as a separate offence in Irish law and is often classified under separate parent legislative provisions. As offences are recorded with reference to the legislation, it is not possible to accurately quantify the number or percentage of offences which relate to or involve computer networks or cybercrime as distinct from other types of crime.

National crime figures are based on recorded crimes and do not include those which, for one reason or another, go unreported to law enforcement but may receive media coverage. Figures are recorded nationally by law enforcement (An Garda Síochána) and published by that organisation and government departments. Judicial figures for convictions are recorded by the Courts Service and while the convictions are a matter of public record, they are not the subject of a public statistical record.

The figures given below have been taken from available sources and should not be considered definitive as they are dependent on the modes of recording used and the accuracy of the data supplied by a number of sources. The figures are available from a number of sources and may contain overlap:

Crime type	*Year*	*Recorded at CCIU*	*Recorded by GNPSB*[10]	*Convictions PULSE*
CEM[11] *cases*	*2014*	*117*	*137 investigations*	*23*
Unauthorised access	*2014*	*6*	*Not applicable*	*0*
Harassment	*2014*	*9*	*Not applicable*	*Not available*
CEM cases	*2015*	*176*	*410 investigations*	*18*
Unauthorised access/damage	*2015*	*12*	*Not applicable*	*1*
Harassment	*2015*	*25*	*Not applicable*	*Not available*

10 Garda National Protective Services Bureau. This unit is responsible for investigating sexual offences, including those involving the exploitation of children online.

11 Child exploitation material, i.e. child pornography.

The Computer Crime Investigation Unit records applications to the unit for assistance based on the crime type. While not all the cases are cyber in nature, they do involve computers which require analysis. The following table reports the total number of cyber-related applications to the unit for its services and a breakdown of the case types involved. The total includes cybercrime investigations and non-cybercrime investigations, which are fewer in number.

	2014	*2015*	*2016*[12]
Total cases received	*320*	*446*	*135*

- CCTV requests
- Fraud offences (online)
- Child exploitation
- Harassment (cyberbullying)
- Criminal damage (data)
- Murder/manslaughter (online evidence)
- Data retrieval
- Phishing
- PABX fraud
- Terrorism
- Unauthorised access

[12] 2016 figures are up to 5 May 2016.

A number of significant cases were recorded during the previous year, including some which, while not cyber in nature, contained a significant cyber element in either their facts or their investigation. They illustrate the level of sentences being given in similar cases.

- Case A: The accused was convicted of the murder of a woman that the accused had met online. The primary evidence on which the conviction was secured was the digital evidence from an examination of computers and mobile phones. The Court imposed the mandatory life sentence.
- Case B: Conviction for possession and distribution of child pornography. The accused received a three-year sentence, which is the average sentence handed down for such offences.
- Case C: The accused was convicted for the exploitation of a child and the possession and production of child pornography. The Court imposed a seven-year sentence with the final two years suspended.
- Case D: The accused were prosecuted under section 2 of the Criminal Damage Act for hacking a prominent political party's website. They pleaded guilty at District Court and the Court applied the Probation Act 1901.
- Case E: The accused received a six-and-a-half-year sentence for dealing controlled drugs on the Darknet. The case also involved the seizure of Bitcoin and forfeiture. The severity of the sentence is currently being appealed.

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

Funding comes from the overall budgetary allocation from central government for policing and is allocated to the relevant sections within An Garda Síochána for distribution and spending as necessary. An Garda Síochána and the Computer Crime Investigation Unit benefit from EU funded training provided by CEPOL, Europol, OLAF and also ISF funding.

3.5. Conclusions

- In 2015 Ireland published its national cybersecurity strategy for 2015-2017, which followed on from the government's action plan entitled 'New Connections: A strategy to realise the potential of the Information Society'.
- The Department of Communications, Climate Action and Environments was responsible for drafting the strategy and states in Chapter 4 that the objectives are as follows:

  - to improve the resilience and robustness of critical information infrastructure in crucial economic sectors, and particularly in the public sector;

  - to continue to engage with international partners and international organisations to ensure that cyberspace remains open, secure, unitary and free and able to facilitate economic and social development;

  - to raise awareness of the responsibilities of businesses and of private individuals around securing their networks, devices and information and to support them in this by means of information, training and voluntary codes of practice;

  - to ensure that the State has a comprehensive and flexible legal and regulatory framework to combat cyber crime by An Garda Síochána that is robust, proportionate and fair, and that accords due regard to the protection of sensitive or personal data.
- The strategy also aims to ensure that the regulatory framework that applies to the holders of data, personal or otherwise, is robust, proportionate and fair, and to build capacity across public administration and the private sector to engage fully in the emergency management of cyber incidents.

- The development of a cybersecurity strategy is a positive step forward. However, it will be necessary to follow up on and monitor the implementation closely. During the evaluation visit it appeared that not all elements are followed up on, e.g. the Memorandum of Understanding between the Department of Communication and the national police.
- The cybersecurity strategy addresses cybercrime as one of many issues, and rather briefly. Greater attention should be paid to the topic. The national police's recent high-level strategy is welcomed, but cybercrime should receive more focus and be addressed beyond the operational level.
- The team has not been able to consult an action plan implementing the objectives of the strategy but during discussions representatives of the drafters presented some details of the risk analysis which is done every two years (the last is from 2014) and analyses the availability of services in Ireland. A National Cyber Security Centre exists on an administrative basis within the Department of Communications, Climate Action and Environments with responsibilities in three primary areas: government networks, personal and business systems and the protection of critical national infrastructure. This will build on the existing Computer Security Incident Response Team (CSIRT-IE), established in late 2011.
- In Ireland there is no obligation to report incidents of computer attacks and therefore there are no comprehensive statistics available. Nevertheless, the police are informed about incidents when appropriate.
- Statistics are obtained directly through the Central Statistical Office but precise figures are hard to produce due to the fact that cybercrime is not classified as a special crime. There are no statistics regarding adjudications on cybercrime. However, the courts issue an annual report on general crimes.

- During the evaluation visit cybercrime trends were only indicated in a general sense, as it was stressed that there was a lack of reliable statistics on cybercrime at national level. Although in the interviews the authorities noted the dependence on clear substantive definitions, which will be introduced with pending legislation, it is not clear whether there is a comprehensive national approach to the issue. Several of the institutions – national ministries, the national police and the prosecutor's office – noted the issue, and indicated the need to work on clear substantive definitions, as well as the need to implement administrative measures (e.g. for ICT systems), but there were no clear preparations, plans or schedules available. The lack of statistics may hamper prioritisation of issues and appropriate allocation of resources in the fight against cybercrime.
- During the evaluation visit references were made to limited availability of resources at national level e.g. for development and to offer training to law enforcement. It was pointed out that most efforts to develop and offer training to law enforcement are backed by EU funding, including financial support under the Internal Security Fund (ISF) – Police.
- The evaluation team also noted that with regard to the available budget for the prevention of cybercrime, there appears to be a lack of coordination among relevant authorities at the national level.

4. NATIONAL STRUCTURES

4.1. Judiciary (prosecutions and courts)

4.1.1. Internal structure

Ireland is a common law jurisdiction and, as such, statutes are interpreted having regard to the precedents in earlier cases as well as with regard to the pre-existing common law. And, of course, common law is developed by judges through the decisions of the courts.

The courts system in Ireland has its origins in the Constitution. The structure of the court system comprises a court of final appeal, the Supreme Court, and courts of first instance, which include a High Court with full jurisdiction in all criminal and civil matters, and courts of limited jurisdiction, the Circuit Court and the District Court. Other courts in operation are the Special Criminal Courts (Special Criminal Court No. 1 and Special Criminal Court No. 2) and the Court of Appeal. The judiciary are completely independent in the performance of their functions.

An Garda Síochána is the national police service of Ireland. It has responsibility for carrying out all policing duties in the Irish state. In addition, it provides state security services and carries out all criminal and traffic law enforcement. The general management and control of the service is the responsibility of the Garda Commissioner who is appointed by the government. The Commissioner is responsible to the government through the Minister for Justice and Equality.

The investigation and prosecution of offences are separate and distinct functions within the Irish criminal justice system. The Director of Public Prosecutions (DPP), as a general rule, has no investigative function and no power to direct An Garda Síochána or other agencies in their investigations. The director may advise investigators in relation to the sufficiency of evidence to support nominated charges and the appropriateness of charges or in relation to legal issues arising in the course of investigation.

Cybercrime is dealt with by the ordinary criminal courts which consist of a lower court of summary trial (District Court) and a higher court of trial on indictment (Circuit Court). The courts are located in the respective district and can try cases within that district. Trials for significant offences may be heard before the Central Criminal Court, which has the same precedence as the High Court. However, where required due to the nature of the crime, such as the persons involved or the potential for witnesses to be interfered with, the case can be submitted to a non-jury Special Criminal Court for trial. This has not happened to date in the area of a cybercrime prosecution. There are no special powers allocated to the courts to deal with cybercrime trials.

4.1.2. Capacity and obstacles for successful prosecution

Prosecutors and members of the Office of the Director of Public Prosecutions have been given specialist training in the area of cybercrimes and cybercrime investigations. In addition they have participated, in tandem with forensic computer examiners from the Computer Crime Investigation Unit, in forums hosted by Europol, EC3 and the EPA on online crime and cybercrime prosecutions.
A draft proposal to increase and restructure the Computer Crime Investigation Unit is currently being considered by management within An Garda Síochána.

Prosecutors in the Office of the Director of Public Prosecutions have attended specialist cybercrime training, including events organised by the ERA, GPEN and an internal cybercrime course designed specifically for prosecutors.

Some issues of technical understanding of the nature of cybercrimes may arise during the course of criminal proceedings.

The existing legislation can be a challenge as the courts are called upon to interpret legislation which was introduced before significant advances in computers and online offending had occurred.

Delays in investigating and prosecuting cybercrime occur because of resources, technical demands and difficulties in obtaining information from outside or multijurisdictional sources.

4.2. Law enforcement authorities

The investigation and prevention of cybercrime is the primary responsibility of the Computer Crime Investigation Unit (CCIU). The unit is a separate section of the Garda National Economic Crime Bureau and is staffed by qualified forensic computer experts who have expertise in the area of cybercrime investigations and computer forensics. However, uniform and detective officers are mandated to investigate all types of crime, including cybercrime. The advice and assistance of the CCIU is available to all members of law enforcement when needed.

The unit provides intelligence and training briefings to partner agencies, including the Irish Banking Federation, government departments and industry. It works in conjunction with academia, including the Centre for Cybersecurity and Cybercrime Investigation at University College Dublin, and CSIRT-IE at the Department of Communications, Climate, Action and Environment and the Defence Forces cybercrime unit. In addition it regularly updates the public on cybercrime trends via its internet presence, the media and press releases.

The investigation of cybercrime is complex, primarily due to the international and online nature of the offending. In some cases it can be time consuming to obtain a statement of complaint from a witness or victim where they are located outside the jurisdiction or in another part of the country. In other cases, the exchange of information between law enforcement and industry can be a challenge. In addition the growing use of encryption and online storage or anonymous internet access continues to present obstacles.

The Computer Crime Investigation Unit provides a 24/7 service to members of An Garda Síochána in the area of cybercrime. Outside office hours a member of the unit at management rank is available through the senior management structure, at superintendent rank or similar, or on request from the Communications Centre.

All urgent requests are prioritised on identified facts and risk factors and where deemed urgent, a forensic examiner/investigator is assigned to assist the local officer. A prosecutor is available to police members of senior rank for consultation in terms of charges and potential prosecutions in all areas, including cybercrime.

4.3. Other authorities/institutions/public-private partnership

The Garda Press Office and the Garda Crime Prevention Office of the Community Relations Section also fulfil a preventative role and provide crime prevention advice and releases to the public and to private or public industry.

In addition, the National Cyber Security Centre (NCSC) in the Department of Communications, Climate Action and Environments has a role with regard to advising and supporting a range of organisations on cyber security.

As the national police force, An Garda Síochána has sole responsibility for investigating criminal offences, including those of a cybercrime nature. A culture of cooperation exists between the oversight authorities, CSIRT-IE and the Defence Forces cybersecurity section, and in cases of identified offences these authorities may provide intelligence or technical support for the investigative role played by the Computer Crime Investigation Unit.

An Garda Síochána has both an investigative and preventative role in the area of cybercrime. It also provides an intelligence response in the area of all criminal activity, including cybercrime.

The Computer Crime Investigation Unit (CCIU) within An Garda Síochána is the primary police unit tasked with the prevention and investigation of cyber-related offending. It has a number of distinct roles which are both forensic and collaborative in nature.

- It is tasked with the investigation of major offences involving:
  - computer network intrusions or attacks against corporate, private or government-owned systems
  - the investigation of complex cyber-related offences.
- It carries out the forensic examination of computer media seized or surrendered in all types of offences, including those which are cyber-related.
- It acts as a liaison and advice centre for police personnel in locally conducted investigations into cyber-related crimes.
- It is the single point of contact (SPOC) for international agencies and partners in the area of cybersecurity and cybercrime, e.g. EC3, Europol, Eurojust, Interpol, the NCA, and the FBI.
- It provides training and advice to the police, partner agencies such as government departments and the Defence Forces, the public, and corporate partners, including the Banking Federation, in the area of cybersecurity and cybercrime prevention.
- It provides training, in conjunction with academia and external agencies such as OLAF and the IACIS (International Association of Computer Investigative Specialists), to other law enforcement personnel on request.

The unit works closely with CSIRT-IE on preventing attacks on national infrastructure systems and training key personnel in the prevention of such attacks and mitigation initiatives. It also actively engages with private academia, in particular with University College Dublin, in the training of industry professionals, prosecutors and law enforcement personnel in cybercrime and cybersecurity initiatives and measures.

Uniform and detective units within An Garda Síochána are also tasked with the investigation and prevention of online crime and where necessary work with the assistance of the CCIU.

While there is nothing in law to prevent public-private partnerships in the fight against cybercrime, An Garda Síochána do not currently engage with PPP in that respect. However, the organisation does use the technical services of a number of private companies in the forensic examination of damaged or corrupt media. In addition a number of private companies, as well as academia, have provided training to law enforcement authorities (LEAs) in the area of cybercrime and this has proved both successful and beneficial.

CSIRT-IE is responsible for the security and protection of government infrastructures and systems. It responds to threats and attacks on critical infrastructure and engages with departments on security, training, reporting mechanisms and investigations. It liaises with the Computer Crime Investigation Unit of An Garda Síochána in the investigation of criminal offences committed against or over governmental systems and reports to the Minister for Communications, Climate Change and Natural Resources. A member of An Garda Síochána with computer expertise is permanently seconded to CSIRT-IE.

The Defence Forces maintain a cybersecurity unit which has an investigative role in terms of protecting its own networks and investigating military offences committed against or across their networks. Where a criminal offence is identified on the Defence Forces network, they will immediately liaise and coordinate with civilian law enforcement in the investigation and potential prosecution of that offence.

The Department of Justice and Equality is responsible for the development of criminal justice legislation relating to cybercrime. In addition, the Office for Internet Safety, an executive office of the Department of Justice and Equality, was established to take lead responsibility for internet safety in Ireland, primarily as it relates to children.

The role of the Office for Internet Safety was examined as part of a broader exercise which examined the existing national regulatory and legislative frameworks around electronic communications, internet governance and the sharing and accessing of content online[13]. Work flowing from this exercise is ongoing.

Office for Internet Safety

In Ireland the Office for Internet Safety (OIS) is an executive office within the Department of Justice and Equality.

The responsibilities of the OIS are as follows:

- internet safety, particularly in relation to combating child pornography
- the internet hotline (www.hotline.ie), the system for dealing with reports of illegal content on the internet
- internet safety awareness campaigns
- monitoring compliance with the internet service provider industry code of practice.

[13] https://rcsi.ie/files/newsevents/docs/20140702102657_InternetContentGovernanceAdvis.pdf

The OIS is the coordinator in Ireland for the EU Safer Internet Programme and channels EU funding to four partner organisations:

- Professional Development Service for Teachers (PDST) Technology in Education – part of the Department of Education and Skills – website www.webwise.ie
- Irish Society for the Prevention of Cruelty to Children Childline service
- National Parents Council (Primary)
- hotline.ie run by the Internet Service Providers Association of Ireland.

The OIS produces awareness-raising materials in soft and hard copy which are made available free of charge to the public. The materials include a series of booklets as well as other materials related to the annual Safer Internet Day which is held in early February each year. In addition the OIS has a dedicated website at www.internetsafety.ie. The website contains the awareness-raising materials as well as further information and links to relevant organisations working for internet safety.

Internet Safety Advisory Committee

The Internet Safety Advisory Committee is made up of representatives from the four partner organisations in the EU Safer Internet Programme as well as representatives from industry and the police force, academics and experts in the area of internet safety. The Committee advises the OIS on internet safety issues, particularly as they relate to children.

4.4. Cooperation and coordination at national level

4.4.1. Legal or policy obligations

In Ireland there is no legal obligation on the private sector to report cyber attacks.

Through the Office of Emergency Planning (OEP), the National Cyber Security Centre is the lead government department in responding to these types of issues, and can call on the facilities of the OEP to coordinate response and recovery operations. Attacks of a criminal nature are investigated in conjunction with the Computer Crime Investigation Unit, which has the statutory responsibility, as part of An Garda Síochána, for the investigation of criminal offences.

Cooperation is ongoing in all of the above and is subject to regular review as part of the working groups involving the banking industry and law enforcement[14]. However the Payment Card and Counterfeit Currency Unit of the Garda National Economic Crime Bureau reports that cooperation, while it exists, could improve significantly in terms of reporting mechanisms and information exchange.

The Computer Crime Investigation Unit is part of a number of working groups in which it shares trends, advice and cooperation material with partner agencies within the private sector, including academia, industry and technology corporations. It also exchanges intelligence LEA bulletins with the private sector where appropriate and liaises with appropriate bodies to strengthen data exchange, technical support and investigative techniques.

[14] See the 'Be Aware Beat Fraud: A Guide to Fraud Prevention' document which was a joint release by the Irish Banking Federation, An Garda Síochána, the police service of Northern Ireland and the Irish Payment Service Organisation Limited (Appendix B.4).

The agencies involved include, but are not limited to, the Hi-Tech Crime Forum at the Banking Federation of Ireland, the Irish Telecommunications Security Fraud Forum, University College Dublin and technology companies. The CCIU has begun a process of introductory visits to e-commerce multinationals and ISPs in order to strengthen cooperation and exchange mechanisms.

Where requested as part of a formal order issued pursuant to legislation or by the courts, private sector agencies will cooperate with ongoing investigations in terms of preservation, disclosure or notification of illegal activity over their networks.

4.4.2. Resources allocated to improve cooperation

LEA equipment and resources need to be both updated and increased as methods of offending develop and grow. Training and knowledge also needs to be updated. Staffing levels reflect the resources available and directly affect the capacity of the relevant units to deal with the level of offending and investigations at hand.

The Crime and Security Branch of An Garda Síochána is tasked with improving and implementing cooperation measures with the communications and ISP agencies within the state. In addition, other sections within An Garda Síochána, including the Garda Drugs and Organised Crime Bureau, the Garda National Economic Crime Bureau, the Computer Crime Investigation Unit and the Paedophile Investigation Unit work closely with the private sector and continually seek to improve the cooperation and exchange mechanisms that exist. However, no specific resources are allocated within these units to that role. Existing exchanges take place on the basis of either cooperation or of Memoranda of Understanding between the organisation and An Garda Síochána.

4.5. Conclusions

- Ireland is a common law country. There is no specialised court or specialised prosecution office for the prosecution or adjudication of cybercrime offences.
- An Garda Síochána is the national police service of Ireland, with over 14 000 Gardai and civilian employees serving all sections of the community. It focuses on national security and international security, public safety, detecting and preventing crime, policing roads, community engagement and collaboration, and inter-agency collaboration to solve problems and improve the quality of life for citizens. There are 28 Garda district areas.
- The Garda National Economic Crime Bureau is the main unit and it has responsibility, among other things, for cyber-enabled fraud, payment card offences and computer crime investigations.
- Furthermore, there is a Paedophile Investigation Unit which investigates, gathers intelligence, enforces legislation and coordinates paedophile crime cases.
- The investigation of cybercrime offences is carried out by a specialised police unit within An Garda Síochána (the Computer Crime Investigation Unit). However, other police officers may investigate this type of crime if mandated to do so. The CCIU is providing training and advice on cybercrime and has developed training courses for investigators in association with University College Dublin. The CCIU is also involved in international police cooperation, acting as the 24/7 contact point.
- The team was provided with information about a plan to regionalise the specialised police with jurisdiction for investigating cybercrime (at least six regional teams), and to establish separate units for computer forensics.

- Prosecutors have no investigative functions and no power to direct the Irish police (An Garda Síochána) or other agencies in their investigations. However, the Director of Public Prosecutions may advise investigators in relation to the sufficiency of evidence and the appropriateness of charges or in relation to legal issues arising in the course of investigation.
- The structure of the court system comprises a court of final appeal, the Supreme Court, and courts of first instance, which include a High Court with full jurisdiction in all criminal and civil matters, and courts of limited jurisdiction, the Circuit Court and the District Court. Other courts in operation are the Special Criminal Courts (Special Criminal Court No. 1 and Special Criminal Court No. 2) and the Court of Appeal.
- Cooperation with the private sector is considered to be good. There are regular contacts between law enforcement authorities and the private sector in order to strengthen data exchange, technical support and investigative techniques.
- The Computer Crime Investigation Unit has begun a process of introductory visits to e-commerce multinationals and ISPs with a view to enhancing cooperation and exchange mechanisms. Among the partner agencies are the Banking Federation of Ireland, the Irish telecommunications sector and other technology companies.
- The cooperation of the Irish government and national police with University College Dublin (UCD) and the Irish Banking Federation should be mentioned as best practices of public-private partnerships in the fight against cybercrime.
- Cooperation with providers of information society services (i.e. over-the-top service providers or cloud service providers) appeared to be less well-developed than with providers of electronic communications services (i.e. telecommunications service providers), and significant issues were reported, e.g. with access to electronic evidence, as challenges to cybercrime investigations.

5. LEGAL ASPECTS

5.1. Substantive criminal law pertaining to cybercrime

5.1.1. Council of Europe Convention on Cybercrime

Ireland signed the Cybercrime Convention on 28 February 2002. Draft legislation to enable Ireland to ratify the Convention was well advanced in 2010 but was affected by developments at European level. It was proposed that a Criminal Justice (Cybercrime) Bill would give effect to provisions of the Convention not already provided for in Irish law and also a 2005 EU Framework Decision on attacks against information systems, with a view to having a single, cohesive piece of legislation dealing with cybercrime. However, the European Commission then brought forward a proposal for a Directive on attacks against information systems to replace the 2005 Framework Decision. Work on the Cybercrime Bill was put on hold pending finalisation of the Directive. When Directive 2013/40/EU was formally adopted in August 2013 a review of the Bill was undertaken to ensure compliance with both the Directive and the Convention and to establish if further drafting would be necessary. However, a decision of the European Court of Justice in April 2014 has necessitated a revision of Ireland's data retention legislation which was being relied upon to give effect to the Budapest Convention. This work is currently being undertaken by the Department of Justice and Equality.

In the meantime, given the urgency attached to transposition of the EU Directive on attacks against information systems, which had been overdue since 4 September 2015, the Bill was re-drafted to give effect to the Directive only at this point. The Criminal Justice (Offences Relating to Information Systems) Bill was accordingly published on 19 January 2016. It is hoped to have this legislation enacted in the current parliamentary session.

It is proposed to return to the matter of ratification of the Cybercrime Convention when the question of revised data retention legislation has been settled. The current legislative programme for the Department of Justice and Equality makes provision for the drafting of a Cybercrime Bill to give effect to provisions of the Cybercrime Convention not already provided for in national law in order to enable ratification of the Convention. It should be noted, however, that key provisions of the Convention relating to offences against information systems are already covered in the Criminal Justice (Offences Relating to Information Systems) Bill 2016.

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

The Criminal Justice (Offences Relating to Information Systems) Bill 2016 ('the 2016 Bill') provides for implementation of Directive 2013/40/EU. The published Bill is available at the following link: http://www.oireachtas.ie/documents/bills28/bills/2016/1016/b1016d.pdf

The programme for government includes a plan to implement the provisions of EU Directive 2013/40/EU on attacks against information systems. The Criminal Justice (Offences Relating to Information Systems) Bill 2016 (see Appendix A.3) was introduced in the Oireachtas[15] in January 2016 and is awaiting a hearing by legislators.

[15] Houses of the Oireachtas consist of the Dáil (lower house) and the Seanad (upper house) and make up the sole legislating body in Ireland.

Cybercriminal acts are prohibited by a number of single statutory provisions contained in different parent legislative acts. There is no central Cybercrime Act which covers all types of online offending. A number of issues are only relevant at the time of trial or at the point of sentence following a person's conviction for an offence, including cybercrime. There are no judicial or governmental guidelines which set out exactly what circumstances or rules apply and most are considered on a case-by-case basis by the trial court.

Irish law references different categories of *mens rea* which consider the issue of the perpetrator's understanding of their crime, including cybercrimes. These categories include intent, recklessness, negligence and mistake. Particular criminal law provisions require an intention to commit the offence while others also consider recklessness as a basis for prosecution. Intent is viewed as either **direct**[16], where the accused has a 'fixed purpose' in their actions and outcome, or **oblique**[17], where the consequences are a natural and probable result of their actions. The courts[18] have held that recklessness in criminal responsibility can be either subjective or objective and is subordinate only to the issue of intent. Where an accused takes an unjustified risk of which they were aware, they would be considered reckless in their actions and bear responsibility for the consequences. On the contrary, where the risk, while unjustified, was not one of which the accused was aware this objective risk could be vindicated at trial.

16 *The People (DPP) v Murray* [1977] IR 360.
17 *The People (DPP) v Douglas & Hayes* [1985] ILRM 25 CCA.
18 *The People (DPP) v Murray*, n24 above.

In Ireland judges are independent in the matter of sentencing, as in other matters concerning the exercise of judicial functions, subject only to the Constitution and the law. In regard to sentencing, the approach of the Irish Parliament has generally been to specify in law a maximum penalty for an offence, so that a court, having considered all the circumstances of a case, may impose an appropriate penalty up to that maximum. The court is required to impose a sentence which is proportionate not only to the crime but to the individual offender, in that process identifying where on the sentencing range the particular case should lie and then applying any mitigating factors which may be present. An important safeguard rests in the power of the Director of Public Prosecutions to apply to the Court of Appeal to review a sentence she regards as unduly lenient.

While aggravating or mitigating factors are not generally included in the legislation they can include the following:

- a guilty plea and if the plea was early
- previous convictions
- the person's character, health and mind-set
- the person's age and family circumstances
- remorse
- the impact on the victim
- whether there was violence involved and its level
- the circumstances of the offence.

Statutory Provision has been made so that where a serious offence is committed as part of or in furtherance of a criminal organisation, it shall be treated as an aggravating factor for the purpose of determining sentence.

The issue of multiple crimes or reoffending is generally considered by the trial judge at sentence and can colour the sentence handed down. In many cases the longest sentence is imposed in cases of multiple offences, and the other crimes are taken into consideration.

The primary statutes covering cyber offending, and included in the questionnaire, are as follows:

a. Acts unique to information systems

This section provides information on legislation to combat acts involving information systems, in particular those related to cyber attacks:

- illegal access to an information system
- illegal system interference
- illegal data interference
- illegal interception of computer data
- misuse of devices – production, distribution, procurement for use, import or otherwise making available or possession of computer misuse tools.

Criminal Damage Act 1991 (see Appendix A.4)

This is the central piece of legislation covering attacks on computer networks and ICT infrastructure. The legislation will be updated with the passing of the Criminal Justice (Offences Relating to Information Systems) Bill but is currently the only legislation prohibiting such crimes.

- Section 1 of the Act of 1991 outlines the **definitions** in terms of damage, property and data but does not define cybercrime.

  There is no definition in Irish law for the term cybercrime and no plans to introduce one in pending legislation. The section includes data as property that takes the form of information which can be accessed by means of a computer. The definition states that data can be damaged by adding, altering, corrupting, erasing or moving it to another location on a computer system or storage medium. It also occurs where the person fails to do something which results in damage.

- Section 2 of the Act of 1991 provides for the offence of **damaging property, including data**.

  The offence of damaging property would include the physical damaging of the computer or system. It also includes contributing to any act which results in any of the above and applies to an offence committed against a computer inside or outside the state. An act of damage would be one which includes rendering a system inoperable or unfit for use by any means, whether it is a physical attack on the equipment or an attack on the data or software it contains. However it is suggested that the current law does not prohibit a distributed denial of service (DDoS) attack as in such cases the computer is often still functioning even though it is no longer accessible.

Section 2 provides that the offence of damaging property occurs where there is an intent to damage or where the person is reckless as to the potential for damage. The definition of recklessness adopted in this section is one of subjective recklessness as mentioned above.

The penalties for committing an offence of damage to a computer, a computer system or data are:

a. on summary conviction (lower courts), a fine not exceeding a specified maximum or imprisonment not exceeding 12 months, or both;
b. on conviction on indictment (higher court), a fine not exceeding a specified maximum or imprisonment for life (if by arson) or a term not exceeding 10 years (if by other means), or both.

There is no provision for a minimum sentence.

- Section 3 of the Act provides for an **attempt to commit damage** to property, including data, and carries a penalty:
  a. on summary conviction, of a fine not exceeding a specified maximum or imprisonment for a term not exceeding 12 months, or both;
  b. on conviction on indictment, of a fine not exceeding a specified maximum or imprisonment for a term not exceeding 10 years, or both.

- Section 4 of the Act refers to the **possession of implements** with the intention of using them to commit an offence of criminal damage to property, including data. While the section does not specifically reference software tools or programs, it could be inferred to include them. As such the section could be used to prosecute an offence of the production, distribution or possession of hacking tools or viruses. The offence carries the same penalty as an offence under section 3 above.

- Section 5 of the Act prohibits the offence of **unauthorised access** to a computer system and is extraterritorial in nature as it applies to access to a system inside or outside the state. An attempt to access without authority is also an offence as the section states that it does not matter if data was actually accessed. A difficulty arises with this offence as it is classified as a minor offence. As such it must be prosecuted within a particular time frame, which is often exceeded by the time needed to obtain evidential data from the sources, including those outside the state. The applicable penalty on conviction in the lower courts is a fine not exceeding a specified maximum or imprisonment for a term not exceeding six months, or both.

The Criminal Justice (Offences Relating to Information Systems) Bill 2016 covers the following:

- illegal access to an information system – covered in section 2 of the Bill, which makes it an offence
- illegal system interference – covered in section 3 of the Bill
- illegal data interference – covered in section 4 of the Bill
- illegal interception of computer data – covered in section 5 of the Bill
- misuse of devices (for the purpose of commission of the above offences) – covered in section 6 of the Bill.

'Information system' and 'data' are defined in section 1 of the Bill as follows:

'information system' means —

(a) a device or group of interconnected or related devices, one or more than one of which performs automatic processing of data pursuant to a programme, and

(b) data stored, processed, retrieved or transmitted by such a device or group of devices for the purposes of the operation, use, protection or maintenance of the device or group of devices, as the case may be.

'data' means any representation of facts, information or concepts in a form capable of being processed in an information system, and includes a programme capable of causing an information system to perform a function.

These definitions are essentially the same as those contained in Article 2 of the EU Directive 2013/40/EU.

With regard to intent, all of the offences created under sections 2 to 6 of the 2016 Bill include the notion of intent.

Section 8 of the 2016 Bill provides that fraudulent use of the personal data of another person will be treated as an aggravating factor when the court is determining a sentence for illegal interference with an information system or computer data (offences under sections 3 or 4 of the Bill).

The 2016 Bill does not refer to mitigating factors. However, the activities to which sections 2 to 6 of the Bill relate must be carried out deliberately and 'without lawful authority' to be considered offences. This means that those legitimately entitled to carry out certain activities, such as maintaining, testing or protecting an information system, are not behaving illegally.

Multiple crimes can be sentenced separately, including through the use of consecutive sentencing, or treated as an aggravating factor for the purpose of sentencing. Recidivism is treated as an aggravating factor for the purpose of sentencing. These are standard principles in Irish criminal law.

Penalties for offences under sections 2 to 6 of the 2016 Bill are set out in section 8 of the Bill. These range from a fine of up to EUR 5 000 and/or a term of imprisonment of up to 12 months on summary conviction, to a fine and/or a term of imprisonment of up to 10 years on conviction on indictment, depending on the seriousness of the offence. Section 8 also provides that a person who commits an offence under the search warrant provisions in section 7 will be liable, on summary conviction, to a fine of up to EUR 5 000 or a term of imprisonment of up to 12 months.

The elements of incitement, aiding and abetting and attempt are covered separately in Irish criminal law. Section 7 of the Criminal Law Act 1997 provides that: 'Any person who aids, abets, counsels or procures the commission of an indictable offence shall be liable to be indicted, tried and punished as a principal offender.'

The offences covered in sections 2 to 6 of the 2016 Bill are all indictable offences and are therefore subject to this general provision.

b. Content-related acts

This section provides information relating to legislation to combat content-related acts, in particular those relating to child sexual abuse online and child pornography:

- computer-related production, distribution or possession of child pornography
- computer-related solicitation or 'grooming' of children.

There are a number of offences contained in the Child Trafficking and Pornography Act 1998[19] which would cover the computer-related acts listed above. These are:

Section 3 – child trafficking and taking, etc., a child for sexual exploitation

Section 4 – allowing a child to be used for child pornography

Section 5 – producing, distributing, etc., child pornography

Section 6 – possession of child pornography.

Section 3: Child trafficking and taking, etc., a child for sexual exploitation

(1) A person who trafficks a child for the purposes of the sexual exploitation of the child shall be guilty of an offence and shall be liable upon conviction on indictment—

(a) to imprisonment for life or a lesser term, and

(b) at the discretion of the court, to a fine.

(2) A person who—

(a) sexually exploits a child, or

(b) takes, detains, or restricts the personal liberty of, a child for the purpose of his or her sexual exploitation,

shall be guilty of an offence and shall be liable upon conviction on indictment—

(i) to imprisonment for life or a lesser term, and

(ii) at the discretion of the court, to a fine.

[19] http://www.irishstatutebook.ie/eli/1998/act/22/enacted/en/html

Section 4: Allowing a child to be used for child pornography

(1) Without prejudice to section 3, any person who, having the custody, charge or care of a child, allows the child to be used for the production of child pornography shall be guilty of an offence and shall be liable on conviction on indictment to a fine not exceeding €31 743.45 or to imprisonment for a term not exceeding 14 years or both.

(2) For the purposes of this section—

(a) any person who is the parent or guardian of a child or who is liable to maintain a child shall be presumed to have the custody of the child and, as between parents, one parent shall not be deemed to have ceased to have the custody of the child by reason only that he or she has deserted, or does not reside with, the other parent and child,

(b) any person to whose charge a child is committed by any person who has the custody of the child shall be presumed to have charge of the child, and

(c) any person exercising authority over or having actual control of a child shall be presumed to have care of the child.

Section 249 of the Children Act 2001 also includes the offence of causing or encouraging a sexual offence against a child.

Section 5: Producing, distributing, etc., child pornography

(1) Subject to sections 6(2) and 6(3), any person who—

(a) knowingly produces, distributes, prints or publishes any child pornography,

(b) knowingly imports, exports, sells or shows any child pornography,

(c) knowingly publishes or distributes any advertisement likely to be understood as conveying that the advertiser or any other person produces, distributes, prints, publishes, imports, exports, sells or shows any child pornography,

(d) encourages or knowingly causes or facilitates any activity mentioned in paragraph (a), (b) or (c), or

(e) knowingly possesses any child pornography for the purpose of distributing, publishing, exporting, selling or showing it,

shall be guilty of an offence and shall be liable—

(i) on summary conviction to a fine not exceeding €2 500 or to imprisonment for a term not exceeding 12 months or both, or

(ii) on conviction on indictment to a fine or to imprisonment for a term not exceeding 14 years or both.

(2) In this section 'distributes', in relation to child pornography, includes parting with possession of it to, or exposing or offering it for acquisition by, another person, and the reference to 'distributing' in that context shall be construed accordingly.

Section 6: Possession of child pornography

(1) Without prejudice to section 5(1)(e) and subject to subsections (2) and (3), any person who knowingly possesses any child pornography shall be guilty of an offence and shall be liable—

(a) on summary conviction to a fine not exceeding €2 500 or to imprisonment for a term not exceeding 12 months or both, or

(b) on conviction on indictment to a fine not exceeding €6 348.69 or to imprisonment for a term not exceeding 5 years or both.

(2) Section 5(1) and subsection (1) shall not apply to a person who possesses child pornography—

(a) in the exercise of functions under the Censorship of Films Acts, 1923 to 1992, the Censorship of Publications Acts, 1929 to 1967, or the Video Recordings Acts, 1989 and 1992, or

(b) for the purpose of the prevention, investigation or prosecution of offences under this Act.

(3) Without prejudice to subsection (2), it shall be a defence in a prosecution for an offence under section 5(1) or subsection (1) for the accused to prove that he or she possessed the child pornography concerned for the purposes of bona fide research.

Definitions

Section 2 of the Act provides the interpretation for these offences, including a definition of child pornography. The text of section 2 is as follows:

Interpretation

2. – (1) In this Act, except where the context otherwise requires –

'audio representation' includes –

(a) any such representation by means of tape, computer disk or other thing from which such a representation can be produced, and

(b) any tape, computer disk or other thing on which any such representation is recorded;

'child' means a person under the age of 17 years;

'child pornography' means –

(a) any visual representation –

(i) that shows or, in the case of a document, relates to a person who is or is depicted as being a child and who is engaged in or is depicted as being engaged in explicit sexual activity,

(ii) that shows or, in the case of a document, relates to a person who is or is depicted as being a child and who is or is depicted as witnessing any such activity by any person or persons, or

(iii) whose dominant characteristic is the depiction, for a sexual purpose, of the genital or anal region of a child,

(b) any audio representation of a person who is or is represented as being a child and who is engaged in or is represented as being engaged in explicit sexual activity,

(c) any visual or audio representation that advocates, encourages or counsels any sexual activity with children which is an offence under any enactment, or

(d) any visual representation or description of, or information relating to, a child that indicates or implies that the child is available to be used for the purpose of sexual exploitation within the meaning of section 3,

irrespective of how or through what medium the representation, description or information has been produced, transmitted or conveyed and, without prejudice to the generality of the foregoing, includes any representation, description or information produced by or from computer-graphics or by any other electronic or mechanical means but does not include –

(I) any book or periodical publication which has been examined by the Censorship of Publications Board and in respect of which a prohibition order under the Censorship of Publications Acts, 1929 to 1967, is not for the time being in force,

(II) any film in respect of which a general certificate or a limited certificate under the Censorship of Films Act, 1923 to 1992, is in force, or

(III) any video work in respect of which a supply certificate under the Video Recordings Acts, 1989 and 1992, is in force;

'document' includes –

(a) any book, periodical or pamphlet, and

(b) where appropriate, any tape, computer disk or other thing on which data capable of conversion into any such document is stored;

'photographic representation' includes the negative as well as the positive version;

'visual representation' includes –

(a) any photographic, film or video representation, any accompanying sound or any document,

(b) any copy of any such representation or document, and

(c) any tape, computer disk or other thing on which the visual representation and any accompanying sound are recorded.

(2) The reference in paragraph (a) of the definition of child pornography to a person shall be construed as including a reference to a figure resembling a person that has been generated or modified by computer-graphics or otherwise, and in such a case the fact, if it is a fact, that some of the principal characteristics shown are those of an adult shall be disregarded if the predominant impression conveyed is that the figure shown is a child.

(3) In any proceedings for an offence under section 3, 4, 5 or 6 a person shall be deemed, unless the contrary is proved, to be or have been a child, or to be or have been depicted or represented as a child, at any time if the person appears to the court to be or have been a child, or to be or have been so depicted or represented, at that time.

(4) For the purposes of this Act, except where the context otherwise requires –

(a) a reference to a section is to a section of this Act,

(b) a reference to a subsection or paragraph is to the subsection or paragraph of the provision in which the reference occurs,

(c) a reference to any enactment shall be construed as a reference to that enactment as amended, adapted or extended, whether before or after the passing of this Act, by or under any subsequent enactment.

Sexual exploitation

An offence under section 3 of the Act of 1998 (child trafficking and taking, etc., a child for sexual exploitation) contains, in subsection (5), the following definitions particular to this section:

(5) In this section—

'child' means a person under the age of 18 years;

'sexual exploitation' means, in relation to a child—

(a) inviting, inducing or coercing the child to engage in prostitution or the production of child pornography,

(b) the prostitution of the child or the use of the child for the production of child pornography,

(c) the commission of an offence specified in the Schedule to the Sex Offenders Act 2001 against the child; causing another person to commit such an offence against the child; or inviting, inducing or coercing the child to commit such an offence against another person,

(d) inviting, inducing or coercing the child to engage or participate in any sexual, indecent or obscene act, or

(e) inviting, inducing or coercing the child to observe any sexual, indecent or obscene act, for the purpose of corrupting or depraving the child,

and 'sexually exploits' shall be construed accordingly;

'trafficks' means, in relation to a child—

(a) procures, recruits, transports or harbours the child, or—

(i) transfers the child to,

(ii) places the child in the custody, care or charge, or under the control, of, or

(iii) otherwise delivers the child to,

another person,

(b) causes the child to enter or leave the State or to travel within the State,

(c) takes custody of the child or takes the child—

(i) into one's care or charge, or

(ii) under one's control,

or

(d) provides the child with accommodation or employment.

Intent/recklessness

All of the relevant offences in the Act of 1998 require 'intent' on the part of the offender.

Aggravating/mitigating factors

Section 3A of the Act of 1998 provides that certain offences under section 3, when committed by a public official in the performance of his or her duties, will be treated as an aggravating factor for the purposes of sentencing. A 'public official' means an officer or employee of a public body.

In addition, it is an element of sentencing principles that any aggravating factor may be taken into account by a judge in determining sentence for an offence, subject to the proscribed maximum sentence available.

Minimum and maximum penalties

There are no minimum penalties for the relevant offences. Maximum penalties are up to life in prison.

Multiple crimes/recidivism

Multiple crimes can be sentenced separately, including through the use of consecutive sentences, or treated as an aggravating factor for the purposes of sentencing. Recidivism is treated as an aggravating factor for the purposes of sentencing.

Incitement, aiding and abetting and attempt

Section 3(3) of the Child Trafficking and Pornography Act 1998 makes it an offence to cause another person to commit an offence under section 3.

Section 3(4) of the Child Trafficking and Pornography Act 1998 makes it an offence to attempt to commit an offence under section 3.

Section 7 of the Criminal Law Act 1997[20] provides that:

'(1) Any person who aids, abets, counsels or procures the commission of an indictable offence shall be liable to be indicted, tried and punished as a principal offender.'

All of the relevant offences under the 1998 Act are indictable offences and are therefore subject to the provision in section 7 above.

In addition, inciting, conspiring and attempting to commit an offence are all offences in common law.

[20] http://www.irishstatutebook.ie/eli/1997/act/14/enacted/en/html

Criminal Law (Sexual Offences) Act 1993[21]

The offence of **soliciting a child** for the purposes of sexual exploitation or for the commission of a sexual offence is prohibited by section 6 of the Criminal Law (Sexual Offences) Act 1993. The offences are those of:

- sexual intercourse
- sexual assault
- buggery.

The section creates a separate offence to the actual offence of engaging in a sexual offence with a child as defined by section 2 or 3 of the Criminal Law (Sexual Offences) Act 2006 and any penalty imposed under the Act of 1993 can be in addition to a penalty imposed for the separate offence of committing a sexual offence with a minor under the Act of 2006.

An offence under section 6 carries a penalty on:

(a) summary conviction of a fine not exceeding a specified maximum or imprisonment for a term not exceeding 12 months, or both;

(b) conviction on indictment to a fine not exceeding a specified maximum or imprisonment for a term not exceeding five years, or both.

[21] As amended by Section 2 of the Criminal Law (Sexual Offences) (Amendment) Act 2007.

c. Acts where computer/IT systems were involved as a tool or target

The following acts are within the group of criminal acts relating to fraud:

- computer-related fraud or forgery
- computer-related identity offences
- sending or controlling the sending of spam.

The Criminal Justice (Theft and Fraud Offences) Act 2001 contains some relevant provisions in this regard.

With the exception of section 9, the offences under the 2001 Act listed below are general, i.e. not specific to computer crime; however, they do not exclude cases where computers are used to commit the offence. They can therefore, depending on the circumstances involved, be relevant to computer-related fraud or forgery or computer-related identity offences.

Section 4 (Theft) provides for the offence of theft if the person dishonestly appropriates property without the consent of its owner and with the intention of depriving the owner of it. A person is liable on conviction on indictment to a fine or imprisonment for a term not exceeding 10 years or both.

Section 6 (Making gain or causing loss by deception) provides that a person who dishonestly, with the intention of making a gain for himself or herself or another, or of causing loss to another, by any deception induces another to do or refrain from doing an act is guilty of an offence. A person is liable on conviction on indictment to a fine or imprisonment for a term not exceeding five years or both.

Section 7 (Obtaining services by deception) provides that a person who dishonestly, with the intention of making a gain for himself or herself or another, or of causing loss to another, by any deception obtains services from another is guilty of an offence. A person is liable on conviction on indictment to a fine or imprisonment for a term not exceeding five years or both.

Section 9 (Unlawful use of computer) provides that a person who dishonestly, whether within or outside the state, operates or causes to be operated a computer within the state with the intention of making a gain for himself or herself or another, or of causing loss to another, is guilty of an offence. A person is liable on conviction on indictment to a fine or imprisonment for a term not exceeding 10 years or both.

Section 25 (Forgery) provides that a person is guilty of forgery is he or she makes a false instrument with the intention that it will be used to induce another person to accept it as genuine and, by reason of so accepting it, to do some act, or to make some omission, to the prejudice of that person or any other person. A person is liable on conviction on indictment to a fine or imprisonment for a term not exceeding 10 years or both. There are also offences of 'Using false instrument' (section 26), 'Copying false instrument (section 27), 'Using copy of false instrument (section 28), and 'Custody or control of certain false instruments, etc.' (section 29).

Copyright and Related Rights Act 2000

The Copyright and Related Rights Act 2000 provides for the protection of copyright and intellectual property rights which are vested in the creators of literary, artistic, dramatic or creative works and would include computer programs to which an author has asserted a right.

- Section 140(1)(b) makes it an offence, inter alia, to sell, rent or lend or offer for same, a copy of a work which is or which the person believes or has reason to believe is an **infringement of copyright**.[22] Therefore the fraudulent offering for sale of duplicate computer programs, games or movie files online on internet trading sites such Donedeal, Ebay® or Amazon® is prohibited and subject to prosecution under the Act. Similar offences occur where a person offers for sale any article which enables copyright infringement by allowing the products to be duplicated[23] or by assisting in defeating inbuilt protection devices which are now built into the programming of many movie and music discs.[24] However it is not an infringement of copyright where the copying or duplication is for personal use[25].

  It is also an offence where an individual, such as an employee, copies an original database from a network which the Act specifies is an original collection of independent works, data or other materials arranged in a methodical way and accessible in any way, and uses that original database without the consent of the copyright owner.

  An offence under the above section carries a penalty on:

  a. summary conviction of a fine not exceeding a specified maximum in respect of each breach or imprisonment for a term not exceeding 12 months, or both;
  b. conviction on indictment to a fine not exceeding a specified maximum or imprisonment for a term not exceeding five years, or both.

22 Cf. *House of Spring Gardens v Point Blank* [1984] IR 611.
23 Section 140(3)(b) Copyright Related Rights Act 2000.
24 Ibid, Section 140(4)(a) (ii) and (b).
25 Ibid, section 81(1) and section 82.

Data Protection Acts 1998-2003 (spam - unsolicited mail) section 2 and **Statutory Instrument 336/2011**

The proliferation of spam communications over public networks is a persistent issue which is addressed in statutory provisions. In addition citizens have the right to opt out of receiving marketing material from online services and where that right is not respected, the person is entitled to make a complaint to the relevant ombudsman, the Communications Regulator or the Data Protection Commissioner. The primary legislative provisions are as follows:

- Section 2 of the 1998 Act provides that it is illegal for a company or organisation to ignore a written request from a person to be excluded from receiving **spam email** or direct marketing material. However, while the section does not include a penalty for a breach of the provision, the complainant is entitled to lodge a complaint with the Data Protection Commissioner, who may impose a fine on the organisation concerned. In addition an offence under the Act is liable on criminal conviction to a penalty on:
  (a) summary conviction of a fine not exceeding a specified maximum; or
  (b) conviction on indictment to a fine not exceeding a specified maximum.

- In addition Statutory Instrument 336 of 2011[26] prohibits, in section 13, the sending of unsolicited electronic mail or SMS messages to a natural person without their consent unless the recipient's email address reasonably appears to be one set up to receive such email communications for an official or commercial purpose. Where a person breaches the provisions of section 13 they will be liable:
  (a) on summary conviction to a fine up to a specified maximum; or
  (b) on conviction on indictment to a fine not exceeding EUR 50 000.

[26] The Statutory Instrument, which is secondary legislation, gives effect to the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 and European Council Directive 2006/24/EC as amended.

- Section 9 of the Child Trafficking and Pornography Act 1998 provides that where an offence of production, possession, importation or distribution of child pornography is committed with the consent, connivance or neglect of an office of a body corporate, that person and the body corporate will be liable to prosecution and may be found guilty as if they had committed the primary criminal offence. Accordingly the penalty imposed would be that which is imposed on the primary offender, as above.

- The Criminal Justice (Theft and Fraud Offences) Act 2001 provides, in section 58, for corporate liability where the offence is committed by the body corporate (or unincorporated) or committed with the connivance or consent of the legal person or arises from the neglect of an officer of the company. In such cases both the individual and the body corporate are guilty of the offence and liable on conviction to the same penalty that applies for the primary offence itself.

- Section 12 of the Copyright and Related Rights Act 2000 provides that where an offence under the Act, including the offence of breach of copyright as it relates to computer systems and programs, etc., is committed by a body corporate or with its consent, connivance or approval or through neglect on the part of an office of the company, that person and the body corporate are liable to prosecution for the offence and subject to the same penalty.
  Section 128 of the Act of 2000 provides for the award of damages by the court in any action for an infringement of copyright. Those damages can be both punitive and exemplary.

- Section 29 of the Data Protection Act 1988/2003 provides that where an offence of breach of privacy or unauthorised disclosure of a person's personal data is committed by a body corporate or with the body corporate's consent or connivance, or through neglect on the part of an officer of the company, the body corporate and that officer are liable to prosecution and on conviction will incur the same penalty.

  Section 31(4) of the Act provides for the imposition of a fine for an offence under the Act where the conviction takes place on indictment.

- Similarly, Statutory Instrument 336/2011 provides that where the offence of breach of a privacy request from a person in the issue of direct marketing or spam mail is committed by a body corporate, it is liable on conviction on indictment to a fine not exceeding EUR 250 000.

- There is no provision in the Criminal Damage Act 1991 for a legal person to be found liable for the offence of damage or unauthorised access to a computer system, or for offences committed by a person with the company's consent, connivance or neglect.

None of the above precludes a civil action being taken against a body corporate for breaches of civil or criminal law by the legal person itself or by its officers or agents. The imposition of a penalty in such cases would be a matter for the court to decide.

- The Criminal Justice (Offences Relating to Information Systems) Bill 2016 also provides for liability for offences under the Bill by bodies corporate. Section 9 provides as follows:

  '9. Where an offence under this Act is committed by a body corporate and is proved to have been so committed with the consent or connivance of any person, being a director, manager, secretary or other officer of the body corporate, or a person who was purporting to act in any such capacity, that person shall, as well as the body corporate, be guilty of an offence and shall be liable to be proceeded against and punished as if he or she were guilty of the first-mentioned offence.'

  Bodies corporate are therefore covered by offences under sections 2 to 6 of the 2016 Bill and liable to the associated penalties set out in section 8.

Current legislation does not provide for the scaling of a cyber attack. The severity of the attack would be an issue to be considered at trial and may influence the trial judge in terms of the penalty imposed on conviction. However, the legislation is silent on such matters save for determining, in most cases, the maximum penalty allowed.

Similarly, the Criminal Justice (Offences Relating to Information Systems) Bill 2016 does not provide specific criteria relating to the scale of the cyber attack. The courts would have regard to the severity and seriousness of the offence in determining the level of the sentence to be imposed within the range of penalties provided in section 8 of the Bill.

Cases considered minor in nature are tried at a lower court on a summary basis, i.e. before a judge of the District Court. Convictions in these circumstances would result in the applicable potential penalty which is lower than that imposed on conviction at a higher court, i.e. on indictment before a judge and jury. The prosecution of such minor cases is conducted by the investigating police officer (garda) or a court presenter who is a member of An Garda Síochána appointed to carry out that role. Where the case is complex a representative of the state prosecution service (Office of the Director of Public Prosecutions) can be requested to present on behalf of the police.

The legislation cited contains the main provisions for offences relating to cybercrime. However, other statutory provisions exist which cover cybercrime, such as:

Type of offending	**Applicable legislation**
Cyberbullying or online harassment	Section 10 Non-Fatal Offences Against the Person Act 1997
Sending offensive material online (SMS/MMS)	Section 13 Post Office (Amendment) Act 1951
Incitement to hatred	Section 2 Prohibition on Incitement to Hatred Act 1989
Advertising prostitution (online)	Section 23 Criminal Justice (Public Order) Act 1994
Assisting or encouraging a suicide	Section 2 Criminal Law (Suicide) Act 1993
Organised crime/online terrorism	Section 72 Criminal Justice Act 2006 (participating in or contributing to organised crime groups)

As outlined above, the Criminal Justice (Offences Relating to Information Systems) Bill 2016 is awaiting its first hearing by the Houses of the Oireachtas and it is anticipated that it will be part of the new administration's programme for government. The sections in this Bill will replace some existing legislative provisions in the Criminal Damage Act 1991 on attacks against computer networks and are designed to give effect to Directive 2013/40/EU.

The Criminal Law (Sexual Offences) Bill 2015 is awaiting further hearing and will, when passed, introduce provisions contained in the Criminal Law (Child Grooming) Bill 2014, along with updating the legislation addressing offences against children and child pornography.

There are no other plans to introduce further amending or codifying legislation in the area of cybercrime.

The current legislative programme for the Department of Justice and Equality makes provision for the drafting of a Cybercrime Bill to give effect to provisions of the Cybercrime Convention not already provided for in national law in order to enable ratification of the Convention. While some preparatory work has already been carried out, further examination of the provisions of the Convention will be required to determine what elements are already covered in Irish legislation and what further legal provisions will be required to facilitate implementation of the Convention. This will involve consultation with and between relevant divisions in the department, possibly other departments, and the Office of the Attorney General.

Finalising this analytical work, drafting the legislation and subsequently enacting it will depend on certain factors: effective coordination between the relevant areas of the department, the availability of dedicated resources within the department and the Office of the Attorney General, and overall governmental and departmental legislative priorities.

In the absence of a cybercrime-specific act, or substantive statutes to address online crime, legislative provisions enacted to tackle real-world crimes are being interpreted to prosecute online crime.

Directive 2013/40/EU has not yet been transposed. However, the Criminal Justice (Offences Relating to Information Systems) Bill 2016 provides for its transposition. Section 10 of the Bill provides that legal jurisdiction extends to the commission of an offence in relation to an information system outside Ireland if the person is an Irish citizen, is ordinarily resident in Ireland or is a body corporate or company under Irish law and the act is an offence under the law of the place where the act was committed. A person is deemed to be ordinarily resident in Ireland if his or her principal residence was located there for the period of 12 months immediately preceding the alleged commission of the offence concerned.

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

Ireland has fully transposed Directive 2011/93/EU and has not experienced any notable difficulties in implementation. Ireland has robust laws in relation to the 20 criminal offences identified in Directive 2011/93/EU. The primary legislation was enacted in 1998 with the introduction of the Child Trafficking and Pornography Act, which identified offenses in relation to the possession, distribution and production of child-abuse material. The legislation defined the scope of and offences arising from the sexual exploitation of children and was further strengthened by the introduction of the Criminal Law (Human Trafficking) Act 2008 and the Criminal Justice (Withholding of Information on Offences against Children and Vulnerable Persons) Act 2012. Further legislation was introduced in the Criminal Law (Sexual Offences) (Amendment) Act 2007, which provided for the offence of child exploitation, and there is currently a proposal before the Oireachtas to introduce the Criminal Law (Sexual Offences) Bill 2015, which is expected to be passed in the coming months. The Bill contains provisions prohibiting the sexual exploitation of children and amends the existing laws on child pornography, including updated definitions and introducing new prohibitions on sexual offences.

C/ Online Card fraud

The Payment Card and Counterfeit Currency Unit of the Garda National Economic Crime Bureau receives regular reports of online credit card fraud. In addition, members of the public and other victims report such offences to their local Garda stations, where they are investigated by individual members. However the Payment Card and Counterfeit Currency Unit of the Garda National Economic Crime Bureau reports that cooperation, while it exists, could improve significantly in terms of reporting mechanisms and information exchange.

Cooperation is ongoing on all of the above and is subject to regular review as part of the working groups involving the banking industry and law enforcement[27]. However, the Payment Card and Counterfeit Currency Unit of the Garda National Economic Crime Bureau reports that cooperation, while it exists, could be improved significantly in terms of reporting mechanisms, security, information exchange, prevention and disclosures.

[27] See the 'Be Aware Beat Fraud: A Guide to Fraud Prevention' document, which was a joint release by the Irish Banking Federation, An Garda Síochána, the Police Service of Northern Ireland and the Irish Payment Service Organisation Limited. (Appendix B.4)

5.2. Procedural issues

5.2.1. Investigative Techniques

- search and seizure of information system/computer data

Damage offences and unauthorised access

Section 13 of the Criminal Damage Act 1991 provides for the issue of a warrant to search and seize anything which a member of An Garda Síochána believes to have been used or be intended for use in the commission of an offence under the Act. In addition, the section provides that a member may operate or cause to be operated any computer system and extract any data found therein.

General power to search and seize under warrant

A search warrant issued under national legislation will in general permit the seizure of anything found at a premises which a member of An Garda Síochána believes may or does contain evidence of an alleged offence. Once seized, the member may submit an application to the Computer Crime Investigation Unit (CCIU) seeking an analysis of the system and the extraction of any relevant evidential data for use in the investigation and, ultimately, at trial.

Powers of search and seizure are contained in section 7 (Search Warrant) of the Criminal Justice (Offences Relating to Information Systems) Bill 2016. Those powers can be exercised in relation to the investigation of offences relating to information systems prescribed in the Bill and include searching for, accessing and seizing a computer. The definition of 'computer' includes a personal organiser and any other electronic means of information storage and retrieval.

Fraud/Computer Misuse Search

Section 48 of the Criminal Justice (Theft and Fraud Offences) Act 2001 permits the search of a premises where an offence under that Act is suspected and where such offence carries a minimum sentence of five years' imprisonment. This would include the offences like theft, forgery and using a computer to make a gain or a loss. The warrant permits the search and seizure of anything found on the premises or in the possession of any persons on the premises where the member of An Garda Síochána has reasonable grounds to believe it may contain evidence of the offence. In addition, the warrant specifically permits the officer to seize and, for long as is necessary, retain any computer or other storage medium, and to operate that computer or cause it to be operated, and if necessary require the person having control of or access to it to provide any password or other information required to access the system. Any person who obstructs the lawful search, including by failing to give the password or other access data, commits an offence and is liable to both arrest and prosecution.

However, prosecution for withholding passwords is generally not done due to the right against self-incrimination. Surveillance warrants can be obtained under the Criminal Justice (Surveillance) Act 2009 to monitor computers that use encryption, and this can overcome difficulties in serious criminal cases where it is known that encryption is being used and passwords will not be handed over.

Drugs Search

The search of computer data or the system on which it is stored is permissible under a warrant issued to an investigating officer subject to a number of statutory provisions. Section 26 of the Criminal Justice (Drug Trafficking) Act 2006 allows for a premises and the persons therein to be searched where there are reasonable grounds to believe that those persons have in their possession a controlled drug or that such a drug is on the premises. The search warrant permits the search and/or seizure of anything found therein; this has been held to include a computer or computer network.

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

At present, only post and telephone communications are subject to interception under the Interception Act 1993. The interception of computer traffic and its collection is severely restricted and permitted only in exceptional circumstances under a warrant issued by the Minister for Justice and Equality.

1. Section 2 of the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993 allows for the issuing of a warrant by the Minister for Justice and Equality which, where the matter is in the interests of the security of the state or a criminal investigation, shall authorise the interception of telecommunications data where it is required for the security of the state or for the investigation of a criminal offence. The warrant shall only be issued if:
   a. the Minister is satisfied that the investigation concerns a serious offence carrying a penalty of imprisonment of five years or more and that it involves a serious risk to a person or property, loss of life or substantial gain for the person involved;
   b. the Minister is satisfied that all other means of obtaining the required information have failed, are likely to fail or prove insufficient;
   c. it is likely that the material gathered would be of evidential value;
   d. in the case of an attempt to commit the offence, the material would assist in preventing, detecting and investigating the offence;
   e. the interception is justified based on the importance of the data it will produce.

The authorisation will cease to have effect if the Commissioner of An Garda Síochána considers it is no longer necessary.

The issuing of such warrants by the Minister is subject to oversight by a judge of the High Court.

Amendments proposed to interception legislation seek to extend current interception powers in relation to telephony to internet communications such as email. Consideration may be given to amending the interception legislation to cover the interception of content data.

- preservation of computer data

The general power to preserve data arises from the warrant authorising its seizure in the first place, as referred to above. In addition, where the data arises from the search of a system or device which has been seized under warrant or the lawful search of an arrested person, the data may be preserved where there is reason to believe it is evidence of a criminal offence.

Data may be held until the conclusion of a trial. There is no specific reference in legislation to the preservation of data – where it is not personal identification information – after the conclusion of a trial or for intelligence purposes.

The preservation of data by a service provider on behalf of law enforcement is subject to mutual agreement and the eventual submission of a disclosure request by the LEA involved. However, section 3 of the Communications (Retention of Data) Act 2011 requires service providers to retain data for two years in the case of data from fixed and mobile telephony services and for one year in the case of data relating to internet access, email or telephony activity.

Retention of traffic data is covered by section 3 (obligation to retain data) of the Communications (Retention of Data) Act 2011. This provides that a service provider must retain data referred to in Part 1 of Schedule 2 to the Act for two years (this data is essentially fixed network and mobile telephony data to identify the source, destination, date and time, etc., of a telephone communication) and data referred to in Part 2 of Schedule 2 for one year (this data relates to internet access, email and telephony data to identify the source, destination, date and time, etc., of an internet communication). (The 2011 Act is aimed at telecommunications service providers and does not extend to the owners of private computer systems.)

Access to retained traffic data is covered by section 6 (Disclosure request) of the 2011 Act. A disclosure request may only be made in relation to serious offences (arrestable offences and certain specified offences).

Retention of, and access to, content data is not covered by the 2011 Act.

- order for stored traffic/content data

There are a number of provisions in Irish legislation relating to production orders (issued by a court) for evidential material. These include section 52 of the Criminal Justice (Theft and Fraud Offences) Act 2001 (theft and fraud offences), section 63 of the Criminal Justice Act 1994 (drug trafficking, indictable offences and asset confiscation) and section 15 of the Criminal Justice Act 2011 (specified white collar offences).

A more detailed analysis of existing production order provisions should be undertaken to determine whether these are sufficient for computer-related offences or whether new computer-specific provisions are required in relation to production.

A member of An Garda Síochána not below the rank of Chief Superintendent[28] may issue a request to a service provider requiring disclosure of the data above where he/she is satisfied that it is required for:

a. the prevention, detection, investigation or prosecution of a serious offence carrying a penalty of five or more years' imprisonment
b. the safeguarding of state security
c. the saving of a life

[28] The order may also be issued by a colonel of the Defence Forces where required for the security of the state, or by a revenue officer not below the rank of Principal Officer where required for the prevention, detection, investigation or prosecution of a revenue offence.

Section 7 provides that a request issued under section 6 shall be complied with by the service provider. However, the Act does not provide for any penalty where the service provider fails or refuses to comply.

Requests for data held outside the state are subject to mutual assistance requests, which are provided for in the Criminal Justice (Mutual Assistance) Act 2008.

- order for user information

Specific provision for orders for the disclosure of user information is not provided for. However, requests can be made under section 6 of the Communications (Retention of Data) Act 2011. In addition, the Data Protection Act 1988/2003 provides for the issuing of a request under section 8 by a member of An Garda Síochána not below the rank of Chief Superintendent (or a designated colonel of the Defence Forces) where personal data is required in the interests of state security or by any member of An Garda Síochána if the disclosure is

- required for the purpose of preventing, detecting or investigating an offence
- required for the purpose of apprehending or prosecuting an offender
- required in the interests of the state's international relations
- required urgently to prevent injury or damage to health, or serious damage to/loss of property
- required under any enactment or order of the court
- made with the consent of the data subject or his/her representative

An Garda Síochána employs acceptable best practice in terms of the investigation of cybercrime and its forensic examiners undergo regular training in techniques. Its members also undergo specialist training in interviewing skills which apply equally to the investigation of cybercrime offences. In addition, the CCIU carries out onsite triage examinations against computer media and online profiles in search and interview situations where an immediate extraction of evidential data or material is required.

The CCIU has recently established an incident room and appointed a Senior Investigating Officer to investigate serious cybercrime matters; this, in turn, has helped build the experience and capability of the CCIU in these matters.

5.2.2. Forensics and Encryption

The unit does not perform remote forensic examinations. However, in the case of social media or email accounts, the unit will examine their contents with the consent of their owners or where an order of the court is granted to do so. A full record of the interaction with the accounts would be kept as these would not be classified as a fully forensic examination.

Encryption is increasingly becoming a problem in the investigation of online crime or cybercrime. It is frequently being used by offenders to protect their data and the illegal material in their possession. In addition, the use of end-to-end encryption by an increasing number of service providers makes the interception or interpretation of material difficult.

On a limited number of occasions, content encryption has been successfully bypassed as a result of a brute force or dictionary attack or where the suspect has provided the password or phrase needed to bypass the encryption. In the case of a search under a warrant issued pursuant to the Criminal Justice (Theft and Fraud Offences) Act 2001, the suspect is required to provide decryption codes, but as the penalty for failing to do so is less than the probable penalty for the primary offence of which they are suspected, they often refuse or claim not to remember.

Authorities involved in the encryption of electronic data and the investigation of cybercrime offences cooperate on a regular basis as required. They also liaise on an ongoing basis and as part of mutual working groups and forensic or cyber forums.

The services of EC3, University College Dublin and other centres are used to attempt to break encryption when it is encountered. There is no decryption centre within An Garda Síochána.

There has been limited success in addressing the issue of decryption in all areas including access, content data and end-to-end encryption.

5.2.3. E-evidence

Data

The Criminal Damage Act 1991 defines data as any 'information in a form in which it can be accessed by means of a computer [including] a program'. The Communications (Retention of Data) Act 2011 defines data as traffic data or location data and the related data necessary to identify the subscriber or user. The Criminal Justice (Theft and Fraud Offences) Act 2001 does not contain a definition of data but does define 'information in non-legible form' as information kept (by electronic means or otherwise) on microfilm, magnetic tape or disk, or in any other non-legible form. The Criminal Justice (Offences Relating to Information Systems) Bill 2016 provides for a comprehensive definition of data as any representation of facts, information or concepts in a form capable of being processed in an information system, including a programme capable of causing an information system to perform a function. There is no specific definition in Irish law for the terms content data, traffic data or computer data.

Information System

An information system is defined in the Criminal Justice (Offences Relating to Information Systems) Bill 2016 as:

a. A device or group of interconnected or related devices, of which one performs the processing of data using a programme, and
b. The data that is stored, processed, retrieved or transited by the device or group of devices for whatever purpose

On the Bill's enactment, this will be the only definition of an information system in Irish law. There is no definition of the other terms referred to above. However, what constitutes an order and its format is a matter of normal practice and agreed format within the various agencies involved.

E-evidence consists of, but is not limited to, registry information, internet traffic history, content data, images and other files, and IP addresses. A general warrant can be obtained under section 10 of the Criminal Justice (Miscellaneous Provisions) Act 1997 for obtaining any evidence for any arrestable offence - an offences which is punishable by five or more years' imprisonment. E-evidence derived from business records has to be served in the manner prescribed under section 6 of the Criminal Evidence Act 1992, as amended.

In recent financial trials, An Garda Síochána and the Office of the Director of Corporate Enforcement submitted large amounts of data electronically to the office of the DPP. The prosecution served all documentation for the trial electronically on encrypted hardware, and the evidence was presented electronically to the trial court and jury during the trial.

Where a system or computer is seized or surrendered in a criminal investigation, its data is forensically collected by a qualified forensic examiner under laboratory conditions and using approved forensic software. That data is stored on a secure standalone network within the Computer Crime Investigation Unit, backed up to tape. Where production is required by a prosecutor or at trial, a copy of the data is extracted, a hash value calculated, and the copy is produced along with a statement from the examiner outlining the processes used, the data found and its authenticity.

There are no rules specific to e-evidence. Its admissibility is, as with any piece of evidence, dependent on the rules of evidence and the trial court. Evidence must be obtained on foot of a legal process, lawfully obtained and relevant. This also applies to evidence from outside the state. E-evidence is generally served by certificate pursuant to section 6 of the Criminal Evidence Act 1992, save where there is judicial notice of the reliability of the particular evidence.

5.3. Protection of Human Rights/Fundamental Freedoms

While the 2006 Working Group on Privacy considered that there was a lack of clarity as regards the protection of privacy rights in Ireland, the legal position has evolved considerably since that point.

There has been extensive case law and legislative development in relation to data protection - both at EU and national level. There has also been further development of Irish case law on the Constitutional right to privacy, as well as further development of case law at European and Irish level on the right to privacy under the European Convention on Human Rights.

In addition, the Law Reform Commission issued a detailed Report in late 2016 on harmful online communications and digital safety, which particularly addresses the balancing of the right to privacy and the right to freedom of expression in the internet context (see chapter 1, Guiding Principles) and whose recommendations are currently under examination by the Department of Communications and by this Department.

Freedom of Expression

Article 40.6.1º of the Constitution reads as follows: 'The State guarantees liberty for the exercise of the following rights, subject to public order and morality:

i. The right of the citizens to express freely their convictions and opinions. The education of public opinion being, however, a matter of such grave import to the common good, the State shall endeavour to ensure that organs of public opinion, such as the radio, the press, the cinema, while preserving their rightful liberty to expression, including criticism of Government policy, shall not be used to undermine public order or morality or the authority of the State.'

Privacy

While the Constitution of Ireland does not specifically reference the right to privacy, it has been recognised by the courts[29] as an unenumerated (unwritten) right under Article 40 of the Constitution.

[29] *Norris v Attorney General* [1984] IR36. *Kennedy v Ireland* [1987] IR587. *Cogley & Ors v RTE* [2005] 2 ILRM 529

ECHR

In addition to the above, as a signatory, Ireland is bound by the European Convention on Human Rights, as transposed into Irish law by the European Convention on Human Rights Act 2003, which guarantees under Article 8 that all persons have a right to respect for their private lives, which shall not be interfered with by government or other authority save in accordance with the law and in the interests of public safety or national security, or for the prevention of crime or the protection of health, morals or the rights and freedoms of others.

Similarly, Article 10 of the European Convention on Human Rights asserts that all persons have a right to freedom of expression, including the right to hold opinions without interference from the state, subject to similar restrictions as above for Article 8. The Irish state recognises it obligations to uphold those rights, and An Garda Síochána, in the exercise of its policing duties, strives to protect and respect those individual rights.

Statutory Protections

While there is no specific legislation which directly protects the privacy of a person or their right to freedom of expression, the following statutes do impose protection for personal data as outlined. The provisions of the statutes also allow for the disclosure of personal data or Personal Identification Information to law enforcement authorities where required for the prevention, investigation or prosecution of an offence. As such, a disclosure order would be submitted to online service providers seeking personal data held against online access records or Internet Protocol (IP) addresses.

1. Data Protection Act 1988/2003

Section 2 of the Act places an obligation on a data controller (person having control of personal data) to ensure that personal data is free from unauthorised access, alteration, disclosure or loss.

Section 8 of the same Act provides that members of An Garda Síochána may seek the disclosure of personal data from any source where that data is required for the prevention, detection or investigation of an offence. However, there is no penalty for non-compliance with an order issued under this provision.

2. Communications (Retention of Data) Act 2011

The Act gives effect to Directive 2006/24/EC on the retention of data generated over public communications services and networks.

Section 3 of the Act requires service providers to retain data for two years where the data is gathered as a result of fixed network and mobile telephony service use, and one year in the case of data gathered as a result of internet access, email or internet telephony services.

Section 6 of the same Act provides for the disclosure of personal data by the service provider, on request, to a member of An Garda Síochána not below the rank of Chief Superintendent, where he/she is satisfied that the data is required for the prevention, detection, investigation or prosecution of a serious offence (meaning an offence outlined in the Act or carrying a penalty on conviction of five or more years' imprisonment), for safeguarding state security or for the protection of life. However, the Act does not provide for a penalty where a service provider fails or refuses to comply with an order issued pursuant to section 6.

The use of disclosure orders is subject to judicial oversight, which is designed to ensure that they are not being abused and that requests are necessary and made in accordance with the law and due process.

The Constitution of Ireland sets out the protections which apply to a citizen's fundamental rights. Some of those rights are directly enumerated, such as privacy, while others are unenumerated, such as the right to freedom of expression. However, the courts have consistently held that such unenumerated rights, including those set out in the European Convention on Human Rights, are inherent in Article 40 of the Constitution.

The investigation of cybercrime offences is carried out by law enforcement, and both common law and criminal legislation provide for situations in which personal rights and freedoms can be set aside. Those include situations where a person, place or thing is:

a. subject to search under warrant issued by a court or other authority
b. subject to search on arrest
c. required to account for their actions
d. subject to interception of data under warrant or ministerial order
e. required to disclose personal identification information in accordance with the law
f. ordered to refrain from disclosing persons, addresses or details by a court in order to protect the privacy or rights of an accused or victim

5.4. Jurisdiction

5.4.1. Principles applied to the investigation of cybercrime

The general principle is that jurisdiction in criminal matters is territorial. This means that jurisdiction is limited to offences committed within the territory of the state. However, there are exceptions to this principle where national laws make specific provision for jurisdiction matters.

Information is set out below with regard to jurisdiction provisions relating to cybercrime offences.

Criminal Damage Act 1991

While the Act is silent as regards jurisdiction in matters of damage per section 2 to property, including data, the courts have held that jurisdiction is decided by either the location of the offender or the targeted system at the time of the offence. Where the offender is located within the state, the jurisdiction of the courts to prosecute is established.

The Act establishes jurisdiction in offences involving unauthorised access to computer systems, as prohibited by section 5, where it states:

'A person who without lawful excuse operates a computer—

(a) within the State with intent to access any data kept either within or outside the State, or

(b) outside the State with intent to access any data kept within the State,

shall, whether or not he accesses any data, be guilty of an offence'.

Criminal Justice (Theft and Fraud Offences) Act 2001

The Act does not canvass the issue of jurisdiction in its initial interpretative provisions. However, it does consider the issue of jurisdiction at section 9, which prohibits the unlawful use of a computer for gain or loss. The section provides that:

(1) A person who dishonestly, whether within or outside the State, operates or causes to be operated a computer within the State with the intention of making a gain for himself or herself or another, or of causing loss to another, is guilty of an offence.'

The location of the perpetrator[30] is of no consequence to a prosecution. However, the computer being used to commit the offence must be based in Ireland for an offence to arise. This does not mean that the computer being directly used to cause the loss or gain must be located there. It is possible to use one computer to manipulate another, located in the jurisdiction of Ireland, to commit the offence. The section provides that to merely cause a computer in the state to be operated, no matter how trivially, would constitute an offence.

Where a theft is committed online by a resident or citizen of the state, the courts will assert jurisdiction to try the offender for the crime when the victim loses control of the funds within the state.

The Sexual Offences (Jurisdiction) Act 1996[31]

Section 2 of the Act provides for jurisdiction with regard to sexual offences committed outside the state by citizens of the state or persons ordinarily resident in the state, provided that the offence constitutes an offence in the place in which it takes place and, if done in Ireland, would constitute an offence there.

The 1996 Act also provides for jurisdiction in circumstances where a citizen or person ordinarily resident in the state attempts (subsection 2), aids, abets, counsels or procures (subsections 3 and 4), conspires with or incites another person (subsections 5 and 6) to commit an offence.

Offences under sections 3 and 4 of the Child Trafficking and Pornography Act 1998 are offences for the purposes of section 2 of the Sexual Offences (Jurisdiction) Act 1996.

30 Section 18(c) of the Interpretation Act 2005 applies in that where the term 'person' is not specifically defined by the Theft Act, it can refer to a body corporate, a group of persons or an individual.

31 http://www.irishstatutebook.ie/eli/1996/act/38/enacted/en/html

Criminal Justice (Offences relating to Information Systems) Bill 2016

Section 10 of the Bill provides that legal jurisdiction extends to the commission of an offence in relation to an information system outside the state if the person is an Irish citizen, is ordinarily resident in the state or is a body corporate or company under the law of the state and the act is an offence under the law of the place where the act was committed. A person is deemed to be ordinarily resident in the state if he or she has had his or her principal residence there for the period of 12 months immediately preceding the alleged commission of the offence concerned.

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

Jurisdiction is decided between the prosecutorial services of both states. There is no statutory provision concerning such cases. The maxim applied in some cases is the likelihood of a successful prosecution and the preclusion against a dual prosecution for the same offence[32]. In addition, it may be possible to use the desk of Eurojust to resolve these cases.

Ireland has not used provisions related to Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings in relation to cybercrime cases[33].

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

Disclosures from online profiles and cloud storage facilities are obtained by way of mutual assistance requests submitted to the state in which the data is held. Direct access to the content of such profiles and storage facilities is obtained by way of the consent of the user/owner of the profile or account.

32 Ne bis in idem.

33 OJ L 328, 15.12.2009, p. 42.

5.4.4. Perception of Ireland with regard to legal framework to combat cybercrime

Cybercrime presents a growing and significant threat to both the security of the state and the personal and property rights of individuals and corporations within the state. The Convention on Cybercrime requires participating states to ensure that they have in place robust legislation which can be used to both prevent and prosecute online crime in all its guises. As a signatory to the Convention there is an obligation on Ireland to ensure that its laws are sufficient to address existing cybercrime offences and provide for new trends in this unique area of offending. While it could be said that the existing legislation provides for a significant number of the offences outlined in the Convention, it is arguable that the law is fragmented and antiquated with many provisions added on to unrelated parent legislation, such as the abovementioned Criminal Damage Act 1991. In addition, some statutes do not adequately provide for the nature of the offences and their transnational character, such as unauthorised access or Distributed Denial of Service attacks. The legislation does not define a computer or other core elements of cybercrime, and some definitions are confusing or outdated. While it is acknowledged that some of these issues will be addressed with the introduction of the Criminal Justice (Offences Relating to Information Systems) Bill 2016, the introduction of a dedicated Cybercrime Bill which codifies all existing provisions under one Act and provides for developments and new trends in online crime would be welcomed.

The legal framework in terms of the disclosure of subscriber details does not contain coercive powers for a service provider who fails to provide the requested information.

The area of mutual assistance requests and the significant delays in obtaining disclosure data from outside the jurisdiction require attention.

Cybercrime is a transnational offending type and as such should be addressed in a united and similar fashion by cooperating states if investigations and prosecutions are to succeed. As such, An Garda Síochána would support any approach to streamlining legislative provisions on a European basis in terms of cybercrimes and online offending types.

The international nature of cybercrime enables offenders to commit online crimes and move on within moments. However, investigators are required to process evidence and information over mechanisms and routes that can lead to delays and result in data being lost with the passage of time or cases becoming statute barred. In addition, differing legislation across jurisdictions can result in confusion as one jurisdiction may not classify the offence as such or rules of engagement may provide for different obligations in terms of what can and cannot be done. Simplification of data-exchange mechanisms needs to be examined.

5.5. Conclusions

- Ireland has had in place what might be considered 'computer crime' offence provisions since the 1990s. The relevant legislation in this regard is the Criminal Damage Act 1991, which provides for the offence of unlawful accessing of data. Over the years, some other specific provisions dealing with computer-related crimes in the area of fraud have been added.
- Ireland has no special provisions on cybercrime offences as described in the Budapest Convention and Directive 2013/40/EU. The provisions of the Criminal Damage Act 1991 or the Criminal Justice (Theft and Fraud Offences) Act 2001 are the main instruments covering cybercrime offences, computer data being included in the notion of property. However, the bill covering cybercrime offences, which, it was said, would bring Ireland's legislation into line with the abovementioned Directive and Budapest Convention, is pending parliamentary procedures.

- Ireland signed the Cybercrime Convention on 28 February 2002 but has yet to ratify it. The other relevant EU Directives in the field have also yet to be transposed into Irish legislation. At the time of the evaluation visit, the Criminal Justice (Offences relating to Information Systems) Bill 2016, which transposes Directive 2013/40/EU on attacks against information systems, was at the first stage of reading in the parliament.
- The Criminal Law (Sexual Offences) Bill 2015 was awaiting further hearing and, once passed, will introduce the provision contained in the Criminal Law (Child Grooming) Bill 2014, along with updating the legislation addressing offences against children and child pornography in order to ensure compliance with Directive 2011/93/EU.
- All matters related to electronic evidence are dealt by way of general rules on admissibility. During the evaluation visit, it was mentioned that Ireland's rules on the admissibility of evidence are rather strict, which often creates obstacles for electronic evidence, notably when obtained from another country, e.g. through MLA requests. Issues were also reported in the context of obtaining electronic evidence: whereas cooperation with providers of electronic communications services appears to be functioning rather well, issues were reported in relation to cooperation with information society service providers (i.e. Over-The-Top service providers/cloud service providers).
- The invalidation of the Data Retention Directive by the ECJ in April 2014 has triggered a revision of Ireland's Data Retention Regime legislation, which was being relied upon to give effect to the Budapest Convention. On data retention, there is still a pending case before the national court (DRI case), and the legislation is still in place but for the moment it relies on data preservation provisions. The national authorities are reviewing data retention legislation in light of recent ECJ rulings.
- The national authorities highlighted the need to replace the Data Retention Directive. They consider that the solution should be found at European level.
- There are no penalties set out in national law for non-cooperation with a disclosure request from LEA.

6. OPERATIONAL ASPECTS

6.1. Cyber attacks

6.1.1. Nature of cyber attacks

In relation to the nature and number of recent cyber attacks, accurate information is only available in respect of government systems and cases where entities have reported issues of their own volition. On that basis, in recent months Ireland has seen the same increase in ransomware attacks as the rest of the EU. There was also a sustained DDOS attack across a range of sectors in January which, while substantial, had little effect on services due to attenuation measures in place.

In addition, a number of corporations have been the subject of CEO (Chief Executive Officer) fraud attempts, where fraudulent financial correspondence is sent to the accounts department of the company requesting the payment of a significant sum to a new bank account for an existing customer or supplier. Some attempts have been successful. However, in cooperation with the Banking Federation and the individual financial institutions, the funds have been stopped or recovered in most cases. The Computer Crime Investigation Unit and the Garda Press Office have publicised the existence of such fraud in the media and on existing law enforcement forums.

6.1.2. Mechanism to respond to cyber attacks

Through the Office of Emergency Planning (OEP), the National Cyber Security Centre is the lead government department in responding to these types of issues, and can call on the facilities of the OEP to coordinate response and recovery operations. Attacks of a criminal nature are investigated in conjunction with the Computer Crime Investigation Unit, which has statutory responsibility, as part of An Garda Síochána, for the investigation of criminal offences.

An Garda Síochána and the Computer Crime Investigation Unit regularly submit mutual assistance requests to multiple jurisdictions in cooperation with the office of the Director of Public Prosecutions. If satisfied with the evidence, legality and proportionality of the request, the Director will issue the mutual legal assistance request.

6.2. Actions against child pornography and sexual abuse online

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

The Garda National Protective Services Bureau has access to and regularly updates the International Child Sexual Exploitation (ICSE) image database. Designated members of the Computer Crime Investigation Unit are due to undergo training in the use of the database and to obtain access to it on completing the training.

Where images or videos are identified, they are taken offline with the assistance of the hotline.ie service and the Internet Watch Foundation (IWF).

6.2.2. Measures to address sexual exploitation/abuse online, sexting, cyberbullying

Regarding the measures in place to address sexual exploitation or sexual abuse online, there are some legislative measures, such as Section 3(2A) of the Child Trafficking and Pornography Act 1998, which provides that:

'(2A) Any person who within the State—

(a) intentionally meets, or travels with the intention of meeting, a child, having met or communicated with that child on 2 or more previous occasions, and

(b) does so for the purpose of doing anything that would constitute sexual exploitation of the child,

shall be guilty of an offence and shall be liable on conviction on indictment to imprisonment for a term not exceeding 14 years.'

Section 3(2B) provides for a similar offence outside the state when done by a citizen of the state or a person ordinarily resident in the state.

Proposed legislative amendments

The Criminal Law (Sexual Offences) Bill 2015[34] was published in September 2015. Amongst other measures, the Bill will strengthen provisions relating to online grooming of children and child pornography.

The Garda National Protective Services Bureau works closely with social media companies based in Ireland, and in particular with the National Centre for Missing and Exploited Children (NCMEC), to detect possible online sexual exploitation/cyberbullying as early as possible and get to child victims in a speedy manner. In addition, members of the Computer Crime Investigation Unit regularly deliver seminars and presentations to corporate and public groups on the misuse of the internet and online abuse or exploitation methods.

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

Section 3 of the Sexual Offences (Jurisdiction) Act 1996 provides that a person who, in the state, makes an arrangement to transport a person to a place within or outside the state or who authorises the making of such an arrangement for or on behalf of another person, knowingly for the purpose of enabling that person or any other person to commit a sexual offence, is guilty of an offence.

34 http://www.oireachtas.ie/viewdoc.asp?DocID=29630&&CatID=59&StartDate=01%20January%202015&OrderAscending=0

Section 4 of the Sexual Offences (Jurisdiction) Act 1996 makes it an offence to publish information likely to promote, advocate or incite the commission of an offence under section 2(1) of the Act.

Offences under sections 3 and 4 of the Child Trafficking and Pornography Act 1998 are offences for the purposes of section 2 of the Sexual Offences (Jurisdiction) Act 1996.

Section 23 of the Criminal Justice (Public Order) Act 1994[35] prohibits the advertisement of prostitution.

The Garda National Protective Service Bureau undertakes intelligence-led operations on convicted sex offenders and potential travelling offenders. Where identified, robust investigations are conducted with the assistance of the Computer Crime Investigation Unit, the Garda National Immigration Bureau and other sections within An Garda Síochána.

The hotline.ie service is actively used in Ireland and proactively addresses the issue of child exploitation over the internet.

The Office for Internet Safety based at the Department of Justice and Equality has the lead on child internet safety. Likewise, the Schools Programme at the Garda Community Relations Bureau addresses internet safety in its programmes delivered to schools, teaching representatives and interested parties.

The Garda National Protective Services Bureau (GNPSB) works closely with academics at University College Dublin, University College Cork and the Royal College of Surgeons in the development of tools that will assist in the detection and prevention of harmful behaviour online. In addition, members of the GNPSB and the Computer Crime Investigation Unit have undertaken courses on tools developed by the FBI to examine illegal P2P activity.

[35] http://www.irishstatutebook.ie/eli/1994/act/2/enacted/en/html

6.2.4. Actors and measures countering websites containing or disseminating child pornography

Hotline.ie service

A hotline service was established in Ireland in 1999. Any suspected illegal content online (including the availability of drugs/legal highs) may be reported by members of the public to the hotline service at www.hotline.ie.

The hotline is operated by the Internet Service Providers Association of Ireland (ISPAI) and it is overseen by the Office for Internet Safety. The hotline provides a central point of contact for members of the public who become aware of child pornography or any other illegal content on the internet in Ireland. The hotline accepts reports, which may be made anonymously, about such material and attempts to identify the source. If the material is hosted in Ireland, it will request that the relevant internet service provider remove it, in accordance with the ISPAI Code of Practice and Ethics. The hotline liaises with An Garda Síochána as appropriate.

To provide a fast response to illegal material hosted outside the Irish jurisdiction, the hotline is a member of INHOPE, the international organisation of internet hotlines. Not all countries have an internet hotline service, and in cases where potentially illegal material is identified by the hotline as being located in such countries, it will forward the report to a specific contact point in An Garda Síochána for transmission and action through international law enforcement channels.

Hotline.ie has a close and ongoing working relationship with An Garda Síochána in relation to illegal content on the internet in Ireland. Specially trained analysts are permitted to view suspected illegal content and, if it is deemed probably illegal, they refer it on to An Garda Síochána and to their own member companies for take-down. Protocols are also in place for the notification and removal of illegal content where it does not originate in Ireland.

In November 2014, An Garda Síochána launched an initiative on the blocking of child abuse material on the internet in Ireland. Under the terms of a Memorandum of Understanding, the company UPC (now Virgin Media) has agreed to block access to child abuse material on its network in Ireland in accordance with a list provided by An Garda Síochána.

The Garda initiative and the work of hotline.ie together are deemed to fulfil Ireland's obligations under Article 25 of EU Directive 2011/93 on combating the sexual abuse and sexual exploitation of children and child pornography. The rest of the Directive is either already covered in Irish legislation or is due to be transposed into Irish legislation by way of the Criminal Law (Sexual Offences) Bill 2015, which is currently on the government's legislative programme.

Internet service providers use whatever systems are best suited, with DNS Poisoning being the most prevalent for filter websites for child pornographic materials.

An Garda Síochána provides ISPs with the Interpol 'Worst of' List to enable them to block sites. However, the actual blocking is a matter for the ISP. The courts are empowered to order an ISP operating in the state to block content over their network. While this has occurred in relation to the distribution or streaming of music content[36], it has not yet occurred in relation to access to child exploitative or abuse material online.

Where a site offering abusive material is identified by An Garda Síochána, a notification is issued to the internet service provider together with a request to disable access. Where the site is identified by hotline.ie or the IWF, a similar process takes place. The take-down is in agreement with the service provider.

[36] *European Union (Copyright and Related Right) Regulations 2012 and EMI Records (Ireland) Ltd & Ors v UPC Communications Ireland Ltd & Ors* [2013] IEHC 204.

Where the server is located in Ireland and is suspected to contain child pornography or abusive material, a search is conducted under the Child Trafficking and Pornography Act 1998 and the server is removed and examined in order to identify the persons involved. Where the server is located outside Ireland, An Garda Síochána works in cooperation with Europol, the hotline service, the IWF or the law enforcement authorities within the relevant Member State in which the server is found. Where the material is identified on a network which has a representation in this jurisdiction, contact can be made with the LE section within that company or network.

An Garda Síochána actively targets the production and distribution of child pornographic material over the internet and regularly investigates allegations of possession of such illegal material. Two units are tasked with the investigation of cases involving child pornography. The Computer Crime Investigation Unit is the primary unit tasked with the investigation of online crime, and it supports investigations in conjunction with the Paedophile Investigation Unit (PIU) of the GNPSB and local policing units. It carries out the forensic examination of computer media in such cases and gives expert testimony at court in trials. The unit is part of the Garda National Economic Crime Bureau and consists of a detective inspector, five detective sergeants and 18 detective gardaí who are all forensically trained in the examination of computers and related media. The unit is due to expand shortly as part of an ongoing restructuring and relocation plan. In addition, the Paedophile Investigation Unit of the GNPSB deals exclusively with online child exploitation. It currently has one detective sergeant and five detective gardaí, with plans to expand that number. The GNPSB also contains the Sexual Crimes Management Unit and other sections involved in the investigation of sexual offences and management of sexual offenders. Both the CCIU and PIU utilise the powers conferred under existing legislation, and in particular the Child Trafficking and Pornography Act and the Criminal (Human Trafficking) Act 2008.

6.3. Online card fraud

6.3.1. Online reporting

The Payment Card and Counterfeit Currency Unit of the Garda National Economic Crime Bureau receives regular reports of online credit card fraud. In addition, members of the public and other victims report such offences to their local Garda stations, where they are investigated by individual members. However, there are no statistics available on the prevalence of such offences, and it is likely that much of this type of crime goes unreported.

6.3.2. Role of the private sector

Cooperation is ongoing on all of the above and is subject to regular review as part of the working groups involving the banking industry and law enforcement[37]. However, the Payment Card and Counterfeit Currency Unit of the Garda National Economic Crime Bureau reports that cooperation, while it exists, could be improved significantly in terms of reporting mechanisms and information exchange.

6.4. Other cybercrime phenomena

While An Garda Síochána and the respective units addressing online card fraud issue regular crime prevention notices and advice to the public and industry, the introduction of measures are a matter for the financial organisations controlling the data and production of the equipment or cards involved.

[37] See the 'Be Aware Beat Fraud: A Guide to Fraud Prevention' document, which was a joint release by the Irish Banking Federation, An Garda Síochána, the Police Service of Northern Ireland and the Irish Payment Service Organisation Limited. (Appendix B.4)

6.5. Conclusions

- The Banking and Payment Federation Ireland is composed of the institutions offering internet banking services out of Ireland, An Garda Síochána, UCD, the Centre for Cyber Security and Cybercrime Investigation, the Police Service of Northern Ireland, the ISPAI and other government departments.
- The keys to fighting high-tech crime are: trusted relationship, information sharing, feedback, two-way communication between stakeholders, consequently being able to do some trend analyses on these bases.
- The most frequent attacks from an industry perspective are DDOS, email hacking (spoofing CEO, CFO mails), phishing, vishing, invoice redirection, money mules, and malware.
- The Irish Telecommunications Security and Fraud Forum, composed by all telecoms sitting together, analyses emerging trends and threats, considering that cybercrime is under-reported and may finance, among other things, terrorist activities.
- The providers cooperate very well with LEA. During investigations, they work together with LEA to see how they can access the information. Therefore both LEA and the telecoms community sat single point of contact (SPOC). The emphasis is on serious offences, for example in life-threatening cases there is a 24/7 system in operation. In the next 12 months, they intend to put in place a real-time response system.
- There is no obligation for the private sector to report cyber incidents. The only concrete information that could be provided was on the basis of the experience of the governmental CERT. However, no statistics were provided to the evaluation team.
- An Garda Síochána can not always give feedback to CERT, even though CERT regularly sends information to An Garda Síochána. A Memorandum of Understanding is currently being put in place between An Garda Síochána and CERT.

- Cooperation between An Garda Síochána and the Irish Banking Federation was mentioned in relation to good practice.
- The office of the Director of Public Prosecutions provided useful information on cases and also judgements on crypto-currency seizure (bitcoin is considered an asset and therefore comes under seizure procedures).
- Participation in two of the EMPACT sub-priorities (cyber attacks and CSE) and national priorities are in line with the policy cycle.
- The identification of victims through ICSE and the work done to train others to use that resource is also a good practice.

7. INTERNATIONAL COOPERATION

7.1. Cooperation with EU agencies

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

Irish authorities underlined that cooperation with EU Agencies is a priority. Europol/EC3, Eurojust and ENISA play a vital role in the identification of cybercrime trends, investigation coordination, mutual exchange of information and intelligence and data analysis on a Europe-wide basis. Their expertise and facilities enable mutual cooperation between Member States and their respective LEA and prosecutorial services. In addition, they provide a streamlined method of determining best practice or procedure in ongoing cooperative measures and data exchange.

Ireland is participating in in two of the EMPACT sub-priorities (cyber attacks and CSE).

Ireland is also a participating Member State in the Eurojust project to set up and maintain a prosecutors' cybercrime network which will facilitate the exchange of cyber-related information, advice, experts' forums and contacts for EU-based cyber prosecutors.

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

Ireland participated in a recent investigation into the activities of the DD4BC cyber exploitation group with EC3, Europol and other Member States. Cooperation in this regard involved participation in joint working groups, active involvement in investigative processes, and submission and collation of evidential data from Irish injured parties to EC3.

In addition, Ireland is a participating Member State in the Eurojust project to set up and maintain a prosecutors' cybercrime network which will facilitate the exchange of cyber-related information, advice, experts' forums and contacts for EU-based cyber prosecutors. A member of the Computer Crime Investigation Unit and a representative from the office of the Director of Public Prosecutions are delegates to the group.

Similarly, CCIU receives notifications from the seconded LEA liaison members who provide intelligence and investigative updates on cybercrime offending and trends, including those occurring in Ireland.

The primary issue for Ireland is the prosecutor-led JIT system which is at variance with the Irish system of law enforcement-led investigations.

Consideration is currently being given to the placement of an Irish police officer with the J-CAT at EC3. This should improve Ireland's capacity and capability in the fight against cybercrime.

Representatives from both the GNPSB and the CCIU participate regularly in the Strategy Group and are members of a number of EMPACT groups, including that on online sexual exploitation. In addition, a member of An Garda Síochána is seconded to EC3 and its child exploitation section.

7.1.3. Operational performance of JITs and cyber patrols

The CCIU has not participated in a JIT to date. However, it has participated in a number of joint operations involving Europol and EC3, and with other Member States where there was a mutual interest identified. The CCIU and An Garda Síochána maintain regular contact with the Irish desk at Eurojust and actively participate in forums and discussion groups of which Eurojust is a member. There is no EU funding allocated to facilitate cooperation.

Ireland has no direct experience of participation in cyber patrols. However, the unit receives notifications from partner agencies arising from cyber patrols and OSINT notifications, and assists the Paedophile Investigation Unit in such programmes.

7.2. Cooperation between the Irish authorities and Interpol

An Garda Síochána actively targets the production and distribution of child pornographic material over the internet and regularly investigates allegations of possession of such illegal material. Two units are tasked with the investigation of cases involving child pornography. The Computer Crime Investigation Unit is the primary unit tasked with the investigation of online crime, and it supports investigations in conjunction with the Paedophile Investigation Unit (PIU) at the GNPSB and local policing units. It carries out the forensic examination of computer media in such cases and gives expert testimony at court in trials. The unit is part of the Garda National Economic Crime Bureau and consists of a detective inspector, five detective sergeants and 18 detective gardaí who are all forensically trained in the examination of computers and related media. The unit is due to expand shortly as part of an ongoing restructuring and relocation plan. In addition, the Paedophile Investigation Unit at the GNPSB deals exclusively with online child exploitation. It currently has one detective sergeant and five detective gardaí, with plans to expand that number. The GNPSB also contains the Sexual Crimes Management Unit and other sections involved in the investigation of sexual offences and management of sexual offenders. Both the CCIU and PIU utilise the powers conferred under existing legislation and in particular the Child Trafficking and Pornography Act and the Criminal (Human Trafficking) Act 2008.

An Garda Síochána participates on an ongoing basis with Interpol in terms of ICSE, intelligence sharing and training measures in all areas, including cybercrime. It submits requests and information to Interpol on an ongoing basis and has a member seconded to Interpol as the Assistant Director for Human Trafficking and Child Exploitation. Regular requests for assistance are submitted to the CCIU via Interpol. These requests are responded to immediately and actioned where possible.

7.3. Cooperation with third states

An Garda Síochána (AGS) is not a party to any policy which applies in such circumstances. However, where necessary, AGS and the Computer Crime Investigation Unit will liaise with the respective cyber units within those countries by using contacts built up by members of the unit when attending training courses or seminars in its own and other jurisdictions.

In the investigation into the DD4BC group, a number of third countries were involved as observers or with other outside status. The coordination provided by Europol ensured that all participants contributed fully to the group and that the maximum investigative benefit was obtained.

7.4. Cooperation with the private sector

Private companies having a branch office in Ireland are subject to Irish legislation in terms of data disclosure and retention. They are subject to the provisions of the Communications (Retention of Data) Act 2011 where the data concerned is held within the state. However, where data is held outside the State private companies may require the MLA process to be followed. In cases of investigations or coercive measures, private companies are subject to search, seizure or investigation in the same way as any other company or entity within the state.

An Garda Síochána and the Police Service of Northern Ireland participate in an annual Cross-Border Crime Forum at which crime trends, including cybercrime and online fraud (including measures to prevent, detect and exchange information), are discussed. In addition, fraud and cybercrime units actively participate in Europol and Eurojust-led initiatives in the investigations of such crimes and all online offending. Discussions and cooperative initiatives are ongoing with LEAs in Europe, the United States and elsewhere.

7.5. Tools of international cooperation

7.5.1. Mutual Legal Assistance

Mutual assistance is covered by the Criminal Justice (Mutual Assistance) Act 2008 which provides for the enactment of international agreements between Ireland and other countries on mutual assistance in criminal matters including the issue of cybercrime.

The Minister for Justice is the central authority for mutual legal assistance and, in this regard, she is responsible for receiving and ensuring the execution of incoming requests. In practice, the Minister's functions are carried out by civil servants in the Department's Criminal Mutual Assistance and Extradition Division. Division personnel (who are not prosecutors, lawyers or police) determine if a request is lawfully made, assess the relevance of evidence sought, establish whether there is dual criminality, pursue enquiries with the service provider, direct police to obtain a production order/search warrant etc. and generally deal with the requesting authorities. The division's personnel are not involved in the investigation and prosecution of domestic offences. The division has a legal adviser seconded from the office of the Attorney General. The legal basis for providing assistance is the Criminal Justice (Mutual Assistance) Act 2008 which gives effect to various international instruments, e.g. the EU Mutual Assistance Convention, the Irish/US Mutual Assistance Treaty etc.

In relation to outgoing requests, the Director of Public Prosecutions is the judicial authority for the purposes of Article 24 of the European Convention on Mutual Assistance in Criminal Matters. An Garda Síochána will submit requests for mutual legal assistance to the Director of Public Prosecutions who will examine the supporting evidence, the legality and the proportionality of the request. The DPP, if satisfied, will issue the request and send it to An Garda Síochána for onward transmission to the central authority. The Minister's function is essentially to transmit the request on behalf of the prosecution service and the police.

Requests are transmitted and received by post. The attached document 'Mutual Legal Assistance in Criminal Matters' (Appendix B.5) from the Department of Justice and Equality outlines the procedure.

Regarding statistics, it is not possible to provide comprehensive statistics in relation to cybercrime specifically. The Criminal Mutual Assistance and Extradition Division does not capture information in such a manner as to allow such statistics to be furnished.

In 2015, the central authority received 915 MLA requests (incoming and outgoing). The vast majority of incoming requests are received from Member States of the EU. However, a significant number of outgoing requests are transmitted to the United States, primarily for evidential material stored by internet service providers (in 2015, 31 % of Irish requests were sent to the US, i.e. 77 of 250 requests). A relatively large number of requests are received for evidential material stored by internet service providers in Ireland – it is estimated that 160 such requests were received in 2015.
There are no specific procedures to be fulfilled as regards MLA requests related to cybercrime. However, there are dual criminality provisions in place generally for requests involving search warrants/production orders. If a request is urgent, an effort will be made to expedite execution of the request if possible.

Insofar as the Garda authorities are concerned, mutual assistance requests are completed and submitted in the same way regardless of the offending type involved. However, the technical nature of cybercrime investigations necessitates that the language used in the request be both specific and understandable. Where a cyber request is received by the Garda authorities, it is generally submitted to a cyber aware unit for their attention and completion of the requested actions.

Assistance is provided in accordance with the Council of Europe and EU mutual assistance conventions as transposed into Irish law. The most common form of assistance sought generally is in obtaining specified evidential material held by service providers (ISPs, telecoms, banks). The position in relation to Mutual Assistance where the interception of telecommunications is concerned is that pending the enactment of the necessary legislation, Ireland is currently only able to give effect to requests for assistance where the interception request relates to telephone based content and communications.

Cybercrime MLA requests seek disclosure of subscriber details, IP records, personal data, financial data, content data and any other data held which may be of evidential value in an ongoing cybercriminal investigation.

With regard to incoming requests, foreign authorities do not generally engage or consult with the central authority prior to sending requests. However, US and UK authorities will make contact from time to time before sending a request. Equally, very often there is police-to-police or prosecutor-to-prosecutor contact prior to the sending of a mutual legal assistance request.

In the case of outgoing requests, the central authority does not generally engage in such consultation.

Apart from issues arising from the volume of requests, the manner in which data is stored poses significant challenges for law enforcement where there is a need to obtain such material speedily in criminal investigations. The legislative framework (globally) is not equipped to deal with how data is stored and accessed. Profound issues arise in relation to obtaining such data:

- there can be difficulty in determining where the data is located – arguably it can be located in several locations
- data may be accessible in a jurisdiction but it may be located (e.g. stored on a server) outside that jurisdiction
- some ISPs may adopt an ultra-legalistic approach and be slow to cooperate in the absence of a warrant
- data may be supplied as intelligence from a jurisdiction but not obtainable from that same jurisdiction as evidence because it is not located there
- data may be 'broken up' and held in several jurisdictions
- data may move from jurisdiction to jurisdiction (and be out of the jurisdiction before a court order can be obtained)
- law enforcement may be entirely dependent on the cooperation of ISPs in tracing the data

One view is that countries should move towards 'constructive possession' and compel ISPs to hand over data which is possibly under their control even if stored in another state. This is contrary to how Irish law generally operates (evidence must be situated in the jurisdiction if a warrant is to be obtained).

An increasing number of requests are received for data stored in Ireland by ISPs. Given the ongoing expansion of the ISP sector there (Facebook, Google and Apple have all announced plans to build data centres), there is a need to plan for a very significant increase.

The Irish/US Treaty is regularly used to obtain specified evidential material held by ISPs.

The Director of Public Prosecutions is the judicial authority for Ireland. An Garda Síochána and the Computer Crime Investigation Unit regularly submit mutual assistance requests to multiple jurisdictions in cooperation with the office of the Director of Public Prosecutions. If satisfied with the evidence, legality and proportionality of the request, the Director will issue the mutual legal assistance request.

7.5.2. Mutual recognition instruments

Generally speaking, this particular form of mutual assistance has not been a feature of the response to cybercrime related activity.

7.5.3. Surrender/Extradition

In relation to outgoing EAWs, it is a matter for the Director of Public Prosecutions to form a view as to whether the offence in question for which a person is sought falls within the scope of the EAW list. It is then a matter for the executing judicial authority to consider the application for the EAW. The Minister has no function in forming a legal view. Similarly, in relation to the making of an extradition request, it is a matter for the Director of Public Prosecutions to form a view as to whether the offence in question for which a person is sought meets the relevant dual-criminality requirement.

The Office of the Director of Public Prosecutions is responsible for issuing all 'outgoing' European arrest warrants and extradition requests, i.e. where the Irish authorities are seeking the arrest and surrender of a requested person who is present in another state whether one of the 28 Member States (EAW) or another state outside of Europe, e.g. the United States of America.

In Ireland, there is no statutory guidance (to date) in relation to which offences fall within the 32 list offences (avoiding the dual-criminality requirement). Ireland is in the process of addressing this matter. However, the Director of Public Prosecutions drafts European arrest warrants and then seeks the issuing judge's endorsement of warrants. The offence(s) contained in an outgoing European arrest warrant are included as 'list offences' in circumstances where the offence(s) listed '*encompasses and reflects the conduct referred to*' (per the decision of the High Court in the case of DPP v Gerrard O'Neil, judgement delivered on 2 February 2016) in the facts contained in the European arrest warrant. A cybercrime offence could therefore fall within the list category of, for example, sexual exploitation of children and child pornography.

All offences in Ireland which could be defined under the heading 'cybercrime' carry a sentence of at least (a minimum of) twelve months' imprisonment and therefore are extraditable under the European Arrest Warrant System.

The Minister for Justice is the central authority for the EAW and extradition and, in this regard, she is responsible for receiving and ensuring the execution of incoming requests. In practice, the Minister's functions are carried out by civil servants in the Department's Criminal Mutual Assistance and Extradition Division. The Minister's primary function relates to incoming requests. In relation to outgoing requests, the Minister's functions are essentially to transmit the requests on behalf of the prosecution service and police. Requests are transmitted and received by post.

As set out above, the office of the Director of Public Prosecutions is responsible for the issue of all 'outgoing' European arrest warrants and extradition requests. Once issued, EAWs and/or extradition requests are then transmitted to the central authority in Ireland, namely the Department of Justice and Equality, which in turn transmits the documents on to the receiving state for execution. In the case of extradition requests, the documents are transmitted by the Department of Justice to the Department of Foreign Affairs for onward diplomatic channel transmission.

It is not possible to provide statistics on the number of requests sent or received in relation to cybercrime specifically.

There are dual criminality provisions in place generally for extradition requests. The average response time for execution of an EAW is six to nine months from the date of arrest. Extradition requests can take three to four years (from the date of arrest). Provisional arrest can be used in relation to extradition.

In relation to 'outgoing' European arrest warrant and extradition requests relating to offences that would fall within the term 'cybercrime', there is significant variance in the length of time it takes to complete them, which may range from one week to years depending on the individual case. Provisional arrests are possible and have been utilised to expedite response times both for European arrest warrants and extradition requests.

Although Iceland and the Kingdom of Norway are both nominated as Member States within domestic legislation (European Arrest Warrant (Application to Third Countries)(Amendment) Act 2012), further domestic legislation needs to be enacted, namely a statutory instrument. Until enacted, no EAW can be issued to either country.

7.6. Conclusions

- Under Irish law, the Minister of Justice is designated as the central authority for mutual legal assistance, European arrest warrant and extradition matters. There is a cybercrime working group within the office of the DPP composed of a cybercrime specialist and two other prosecutors with responsibilities for mutual legal assistance and extradition/EAW.
- The key partners in judicial cooperation are An Garda Síochána, the office of the Director of Public Prosecutions, the office of the Attorney General, the courts, the Irish National Member at Eurojust, and the Revenue Commissioners.
- Judicial international cooperation is carried out through a specialised unit within the Department of Justice. That unit is entitled to receive and to examine the requests and also to assure the execution of the requests through police units. With respect to outgoing requests, the unit is only responsible for transmitting them; the office of the Director of Public Prosecutions has the responsibility of drafting the requests.
- During the onsite visit, it was stressed that the most difficult endeavour is the work with service providers who have to produce the evidence sought. According to the national provisions, service providers can only be obliged to produce evidence located in Ireland.
- The Eurojust member is often used for speeding up the process of mutual legal assistance.

- During the evaluation visit, the participants stressed the fact that the MLA process is time-consuming and the procedures can be cumbersome. According to the competent authorities, 95% of incoming requests are related to ISPs also established in Ireland. The request comes in for examination to the Ministry of Justice, then it is allocated to a case officer (not a lawyer), who makes contact with the ISP/information society service providers, trying to establish where the evidence is located. With telecoms and financial institutions, this is straightforward, but the same level of cooperation is not received from ISP/information society service providers. During the evaluation visit, it was stressed that the majority of incoming requests relate to electronic fraud-related crimes. It was also stressed that for outgoing requests, in urgent cases, the Eurojust channel, police-to-police or bilateral relations (especially with the UK and USA) are used.
- It is anticipated that by 2020, many major ISPs may have data centres located in Ireland. Ireland is supportive of the EU institutions in terms of finding ways to streamline requests for data held by ISPs.
- Eurojust and the Irish National Member are known by the relevant Irish authorities and they are in the process of exploring the best ways to engage and interact with Eurojust.
- No Joint Investigation Team agreement has yet been signed by Ireland, but there is commitment to better assess the matter of setting up a JIT in the future.
- The Irish authorities are very much aware of and support the expert process started at EU level following the 9 June 2016 Council Conclusions on improving criminal justice in cyberspace.
- National police highlighted several times that there is good cooperation with Europol and that they have participated in a few joint actions; Europol has been involved in concrete cases and information exchange via the corresponding channel (SIENA).

- An international and also national problem is the location of e-evidence. A production order for e-evidence can be enforced by the police. The ISPs are not obstructive but in practice difficulties have been encountered in establishing where the evidence is located.
- A working group (Department of Justice, DPP, An Garda Síochána) was established to analyse further work needed to better align with EU instruments and improve international cooperation, mainly because a significant increase in requests received is expected due to the ISPs located there.

8. TRAINING, AWARENESS-RAISING AND PREVENTION

8.1. Specific training

Training is provided to targeted groups within An Garda Síochána and to other groups with a vested interest in the investigation and prosecution of cybercrime offences. The Paedophile Investigation Unit provides training in the area of online child exploitation to personnel within An Garda Síochána. The Computer Crime Investigation Unit provides ongoing training to a broad number of groups, including:

- Gardaí in training at the Garda Síochána College
- Qualified gardaí as part of ongoing in-service training
- Investigators as part of the Senior Investigating Officer and Detective training courses
- Prosecutors in the office of the Director of Public Prosecutions
- Barristers as part of a cybersecurity training programme with the Bar Council of Ireland
- Solicitors and legal practitioners as part of a cybercrime training programme delivered to the Law Society of Ireland
- Ongoing in-house and external training programmes in cybercrime investigations and computer forensics delivered to specialist personnel within An Garda Síochána
- Post Graduate certificate in fraud and e-crime investigation in University College Dublin

- Training programmes delivered to forensic examiners in partnership with:
  - University College Dublin (MSc in Forensic Computing and Cybercrime Investigations)
  - Trinity College Dublin (MLitt in Cybercrime Legislation and Online Investigations)
  - International Association of Computer Investigative Specialists
  - OLAF – European Anti-Fraud Office training programme
  - CEPOL – European Police College
  - ECTEG – European Cybercrime Training and Education Group
  - Software specific training delivered by vendor specialists
  - Other law enforcement agencies as part of mutual training programmes e.g. PSNI, FBI

Forensic examiners and investigators in the Computer Crime Investigation Unit are encouraged to undertake specialist training on an annual basis through training programmes delivered by ECTEG and OLAF. In addition, all examiners are required to undertake the MSc in Forensic Computing and Cybercrime Investigations as part of their training programme. This specialist training is delivered by University College Dublin's Centre for Cybercrime Investigation and consists of optional module learning and examinations in:

- Computer/network/mobile device forensics
- Live Data Forensics
- Malware investigations
- Linux and operating systems technology
- Programming
- OSINT
- Money laundering
- A case study and a research project

As specialists in a changing environment, they are cognisant of the need to update their skills on a constant and evolving basis. They are given the opportunity to self-train, participate in online training programmes and identify specialist courses which would provide them with new or updated training in areas of need. In-house and formal external training programmes are coordinated by a training manager within the Computer Crime Investigation Unit who is tasked with monitoring the training needs of members of the unit and identifying suitable training courses as they become available. In addition, where members of the unit attend external courses, they are required to deliver in-house familiarisation seminars to the remaining members of the unit on their return. External courses are primarily provided by ECTEG, OLAF and Europol/EC3. A training matrix has been developed and is used to identify the training requirements of members attached to the Computer Crime Investigation Unit. Nevertheless forensics and cybercrime training is the responsibility of each individual member at the Computer Crime Investigation Unit.

The annual budget for cybercrime training is in the region of EUR 40 000.

LEA officers attached to the Mutual Assistance section of An Garda Síochána receive training in their area of expertise.

A number of other academic institutes provide or validate cybercrime training as part of their curriculum (Dublin City University) or in tandem with Garda training courses (Garda Training College) and for specialist training courses and modules such as the Garda Fraud Course cybercrime module (University College Dublin). Many third-level institutions in Ireland now provide computer forensics and cybersecurity-related courses, e.g. Institute of Technology Blanchardstown, Dublin City University and Waterford IT.

8.2. Awareness-raising

Awareness training in the area of cybercrime is provided to external bodies such as:

- Association of Compliance Officers of Ireland
- Chartered Accountants Association
- Financial Services Sector
- Small and Medium Enterprises Association
- Irish League of Credit Unions
- The Institute of Education
- Retailers Excellence Ireland
- Irish Telecommunications Sector Fraud Forum

The CCIU has over the past 18 months engaged in a cybercrime/security campaign utilising various media outlets including radio, TV and print media. Presentations have been delivered in conjunction with Information Security Ireland, Data Protection Officers and the Irish Reporting and Information Security Service (private CSIRT).

Input from OIS

- The Office for Internet Safety (OIS), an executive office of the Department of Justice and Equality, makes internet safety awareness-raising materials available in hard copy and on its website www.internetsafety.ie
- The OIS coordinates the EU Safer Internet Programme in Ireland to provide safer internet awareness-raising, helplines and a hotline. This is part-funded by the EU's Connecting Europe Facility (CEF), the budget envelope that deals with transport, energy and communications.

- The OIS produces materials for the annual international Safer Internet Day in February each year. The materials are available in hard copy and on the OIS website www.internetsafety.ie.

  Garda Primary Schools Programme

  The OIS provides An Garda Síochána with copies of its awareness-raising materials for use in their Garda Schools Programme.

  The Garda Primary Schools Programme was first introduced in 1991 and teaches children sensible and responsible patterns of behaviour. The programme consists of a series of presentations and discussions given to school children by local community gardaí who are specially trained. To deliver the programme, gardaí visit primary schools throughout the country to educate children about their responsibilities around their own behaviour when using the internet or mobile phones.

An Garda Síochána provides cybercrime training and awareness programmes and courses in schools, aimed at providing students and young people with the skills needed to safely study and browse online. The Schools Programme targets students in primary and secondary schools in the area of crime awareness and personal security. When requested to do so, the Computer Crime Investigation Unit and other units will deliver presentations on cybercrime and personal cybersecurity at third-level institutions.

8.3. Prevention

8.3.1. National legislation/policy and other measures

While prevention is not provided for in national legislation, it is an issue that An Garda Síochána is actively involved in promoting. The Computer Crime Investigation Unit regularly publicises crime prevention notices on official websites, through the Garda Press Office, on online social networking profiles and through intelligence releases to the public and private industry through the national media, the CrimeCall television programme and other platforms.

8.3.2. Public-Private Partnership (PPP)

While there is nothing in law to prevent the use of public-private partnerships in the fight against cybercrime, An Garda Síochána does not currently engage with PPP in that respect. However, the organisation does use the technical services of a number of private companies in the forensic examination of damaged or corrupt media. In addition, a number of private companies, including academia, have provided training to LEA in the area of cybercrime and this has proved both successful and beneficial.

8.4. Conclusions

- Judges and prosecutors attend national and international training events in the area of cybercrime on an ad hoc basis. ERA seminars are very popular with Irish judicial authorities.

- Following an assessment made by the Legal Training Steering Group, DPP decided to invest in the ERA programme and to provide internal training on current issues with a view to running an internal series. The DPP certificate in cybercrime was a five-part/seven-hour lecture series which was supplemented with GPEN webinars. The assessment of this programme will shape future cybercrime training.

- Training is provided to targeted groups within An Garda Síochána and to other groups with a vested interest in the investigation and prosecution of cybercrime cases.

- In-house and formal external training programmes are coordinated by a training manager within the Computer Crime Investigation Unit. External courses are primarily provided by ECTEG, OLAF and Europol/EC3.

- There is a very well established partnership between An Garda Síochána and University College Dublin (UCD) in terms of specialist training courses and modules. DCU has been working with An Garda Síochána since 1998 and collaborates on EU-funded projects in the field, supporting the cybercrime community.

- Regarding prevention, the Office for Internet Safety of the Department of Justice and Equality revealed the existence of a project co-financed by the EU regarding the establishment of the Safer Internet Centre. Several sub-projects have been run under it, such as webwise.ie, watchyourspace.ie, saferinternetday.ie, and also a few hotlines for parents and children: npc.ie, childline.ie and one regarding suspect online content, hotline.ie.

9. FINAL REMARKS AND RECOMMENDATIONS

9.1. Suggestions from Ireland

Ireland has identified a number of issues which affect the successful investigation and prosecution of offences,

The Irish authorities are of the view that it is well recognised, both nationally and at international level, that we face many challenges in the investigation of cybercrime and cyber enabled crime – these challenges primarily relate to the increased mobility of data, the multi-jurisdictional nature of cybercrime, and the multiplicity of actors that can be involved.

There are also complex issues that arise with regard to jurisdiction in cyberspace which are currently the subject of much debate within the international bodies. Similarly, access to encrypted data for the purposes of criminal investigations is a further complex issue given the competing rights to privacy and freedom of expression that inevitably arise.

Many of these issues will require a possible international solution as they are issues that no one state can effectively address in isolation.

There is also the well recognised need for capacity building amongst law enforcement agencies. In this regard, the demand for both forensic computing and cybercrime investigation services continue to increase and work on capacity building, both nationally and internationally, will remain a priority for some time.

At national level Ireland is continuing to develop its legislative frameworks so as to ensure it keeps abreast of international standards and developments in relation to cyber related phenomena. In December 2016, the Government approved the drafting of legislation which would provide for new and amended criminal offences to tackle online abuse like revenge porn and cyberbullying along the lines set out in the Law Reform Commission Report on Harmful Communications and Digital Safety.

Legislation is currently before the Irish Parliament which bring Ireland's legislation into line with the EU Directive on attacks against information systems and give effect to many of the key provisions of the Budapest Convention. Other legislation, recently enacted by the Parliament provides for the further protection of children against online sexual exploitation and abuse. In addition, legislation relating to Data Retention and Interception is being prepared which will provide for a small number of additional legislative provisions which are required to allow for ratification of the Budapest Convention.

Ireland is committed to ensuring the necessary resources are made available to build law enforcement capacity. On foot of a review of the Computer Crime Investigation Unit (CCIU) under the Garda Síochána's Modernisation and Renewal Programme 2016-2021, a dedicated Garda Cyber Crime Bureau has recently been established to ensure that An Garda Síochána (Ireland's police force) has the capacity and capabilities to deal with cyber crime and cyber security threats. The allocation of the allocation of additional and support staff for the Bureau is ongoing.

The Bureau will continue to strengthen its links with the National Cyber Security Centre; industry partners; national and international stakeholders; and the UCD Centre for Cybersecurity and Cybercrime Investigation in the areas of research, development and training, as well as working closely with law enforcement partners to maintain and develop the capacity of An Garda Síochána to investigate and prevent cyber crime and improve cyber security.

As noted during the evaluation exercise it is intended to establish regional cyber crime units and pilot regional units have already been established in the Southern and South-Eastern Regions.

In addition, the Garda authorities are continually looking to ensure that the latest information, communications and forensic technologies are sourced and deployed to ensure that An Garda Síochána will be properly resourced to meet the evolving needs of a modern effective police force and to take advantage of proven up to date technological developments in crime detection and prevention as they occur. Further, a module on cyber crime investigation has been included in the training programme for all trainee Gardaí, with all other Garda personnel receiving training in cyber crime awareness and cyber crime investigation through the Garda Continuous Professional Development network.

The establishment of the Bureau is also supported by the significant investment of some €330 million in Garda ICT infrastructure, including €205 million under the Government's Capital Plan, between 2016 and 2021.

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 Ireland was able to satisfactorily review the system in Ireland.

Ireland 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 appropriate to make a number of suggestions for the attention of the Irish authorities. Furthermore, based on the various good practices, related recommendations to the EU, its institutions and agencies, and in particular Europol, are also put forward.

The evaluation team also thought it appropriate to highlight a number of good practices that emerged during the evaluation visit.

Good practices

1. Garda partnership with UCD.
2. Garda framework for cooperation with Banking and Payment Federation Ireland.
3. The identification of victims through ICSE and the work done to train others to use that resource.
4. The development of OSINT should be considered a very positive step.
5. Judgements on crypto-currency seizure (bitcoin is considered an asset and therefore comes under seizure procedures).
6. The decentralisation of the Computer Crime Investigation Unit is also a very positive approach that should be continued.
7. The use of Garda seconded experts in other institutions is very useful due to their specific expertise.

9.2.1. Recommendations to Ireland

1. Should finalise the criminal law reform (i.e. have the two bills adopted) and the ratification of the Budapest Convention.
2. Considering the delays reported to the evaluation team, should implement the action plan of their cybersecurity strategy and Garda strategy without further delay.
3. Should consider establishing comprehensive statistics encompassing figures on each stage of criminal proceedings, including numbers of investigations, prosecutions and convictions. Should also consider having statistics on cybersecurity incidents and feedback from gardaí regarding criminal investigations.
4. Should continue the development, in a sustainable way, of the recently set-up National Cyber Security Centre.
5. Should consider creating a national database for CSE materials.
6. Although there is good cooperation between the national authorities and ISPs, Ireland should consider having procedures that could enable authorities to receive answers to their requests in a timely manner, and putting in place a system of penalties for non-compliance/cooperation/failure (administrative or procedural fine).
7. Taking into consideration the specificity of the judiciary system, should assess the training needs of the judiciary and the possibility of providing them with adapted options for specialised cybercrime training.
8. Should take into account the need to more strongly coordinate prevention and awareness-raising activities between the relevant governmental authorities and An Garda Síochána.
9. Should consider participating in or organising JITs as they are a useful tool for obtaining evidence.

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

10. In the discussions with the evaluation team, the national authorities underlined:
    - the need for a harmonised data retention regime at EU level and the need for the EU legislator to find solutions in that respect;
    - the need to identify an international solution for a clear and appropriate framework regulating the relations of the judicial authorities with ISPs across the EU.
11. Consider working at EU level towards a common framework on electronic evidence, and a common approach on crypto-currency.
12. Consider an EU-US arrangement on common procedures with respect to work with ISPs.
13. Consider working on an international scheme to remove the obtention of subscriber information from the MLA process.

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

7th Round of Mutual Evaluations: Practical implementation and operation of European policies on prevention and combating Cybercrime (27 – 30 June 2016)

Monday 27th June

Arrive in Dublin

18:30: Pre evaluation meeting (Evaluators only)

Tuesday 28th June

08:45 – 09:00 Pick-up at Hotel

09:00- 13:00 Department of Justice & Equality – welcome and overview on criminal matters (to include 20min coffee break at 11:00am)

13:00 – 14:00 Lunch

14: - 14:15 Transfer to Department of Communications, Climate Action and Environments

14:15 - 16:30 Department of Communications, Climate Action and Environments

16:30 – 17:00 Transfer to Hotel

18:00 – 20:00 Dinner hosted by the Department

Wednesday 29th June

09:00 -09:15 Pick-up at Hotel for transport to Garda National Economic Crime Bureau, Harcourt Street

09:15 – 12:45 An Garda Síochána – Irish Police Force

12:45-13:45 Lunch

13:45 – 14:00 Transport to Office of Director of Public Prosecutions

14:00 – 16:15 Office of the Director of Public Prosecutions

16:15-16:30 Transfer to Criminal Courts Complex

16:30 – 17:30 Meeting with Judiciary – Criminal Courts Complex

Thursday 30th June

09:00 – 09:15 Pick-up at Hotel – Walk to Department

09:15- 11:15 Department of Justice & Equality on mutual assistance and extradition matters.

11:30 -13:00 Department of Justice & Equality – Wrap up meeting

ANNEX B: PERSONS INTERVIEWED/MET

Meetings on 28 June 2016

Venue: Department of Justice & Equality

Person interviewed/met	**Organisation represented**
Peter Mullan	Department of Justice & Equality
Deirdre Meenan	Department of Justice & Equality
Dermot Woods	Department of Justice & Equality
Ursula Stapleton	Department of Justice & Equality
Yvonne Furey	Department of Justice & Equality
Rachael Woods	Department of Justice & Equality
Una Murphy	Department of Justice & Equality
Barry O'Donnell	Department of Justice & Equality
Geraldine Moore	Department of Justice & Equality

Venue: The Department of Communications, Climate Action and Environment (DCCAE)

Person interviewed/met	**Organisation represented**
Richard Browne	Department of Communications, Climate Action and Environment
Neil Redmond	Department of Communications, Climate Action and Environment

Meetings on 29 June 2016

Venue: An Garda Síochána, Harcourt Square

Person interviewed/met	Organisation represented
Detective Chief Supt Pat Lordan	An Garda Síochána
Detective Inspector Michael Gubbins	An Garda Síochána
Garda Wes Kenny	An Garda Síochána
Sergeant Paul Johnstone	An Garda Síochána
D/Sergeant Mike Smyth	An Garda Síochána
Inspector Eamon O'Loughlin	An Garda Síochána
Sergeant John Cadogan	An Garda Síochána
Detective Inspector Rory Corcoran	An Garda Síochána
Keith Gross	Banking and Payments Federation Ireland
Cheryl Baker,	UCD Centre for Cybersecurity & Cybercrime Investigation
Maureen King,	Irish Telecommunications Fraud Forum

Venue: Office of Director of Public Prosecutions

Person interviewed/met	Organisation represented
Mairead Cotter	Office of the Director of Public Prosecution
Helena Kiely	Office of the Director of Public Prosecution
Liam Sheridan	Office of the Director of Public Prosecution
Jane Farrell	Office of the Director of Public Prosecution
Michael Brady	Office of the Director of Public Prosecution

Venue: Criminal Courts Complex

Person interviewed/met	Organisation represented
The Hon. Mr. Justice John Edwards,	Court of Appeal
The Hon. Mr. Justice Patrick McCarthy,	High Court
The Hon. Mr. Justice Robert Eagar	Circuit Court
Her Honour Judge Melanie Greally	Circuit Court
Judge Michael Walsh	District Court

Meeting on 30 June 2016

Venue: Department of Justice & Equality

Person interviewed/met	Organisation represented
Maura Hynes	Office of Internet Safety
Edward Shortt	Office of Internet Safety
David Fennell	Department of Justice & Equality
Davina Bracken	Department of Justice & Equality
Deirdre Meenan	Department of Justice & Equality
Ursula Stapleton	Department of Justice & Equality

ANNEX C: LIST OF ABBREVIATIONS/GLOSSARY OF TERMS

LIST OF ACRONYMS, ABBREVIATIONS AND TERMS	IRELAND OR ACRONYM IN ORIGINAL LANGUAGE	IRELAND OR ACRONYM IN ORIGINAL LANGUAGE	ENGLISH
CEPOL			European Police College
CERT			Computer Emergency Response Team
ECJ			Court of Justice of the European Union
EC3			European Cybercrime Centre
EMPACT			European Multidisciplinary Platform Against Criminal Threats
ENISA			European Union Agency for Network and Information Security
EUROJUST			European Judicial Cooperation Unit
EUROPOL			European Police Office
GENVAL			Working Party on general Matters, including evaluations
ICSE			Interpol's International Child Sexual Exploitation Database
INTERPOL			International Criminal Police Organization
J-CAT			Joint Cybercrime Action Task Force
JHA			Justice and Home Affairs
LEA			Law enforcement Authorities
MLA			Mutual Legal Assistance