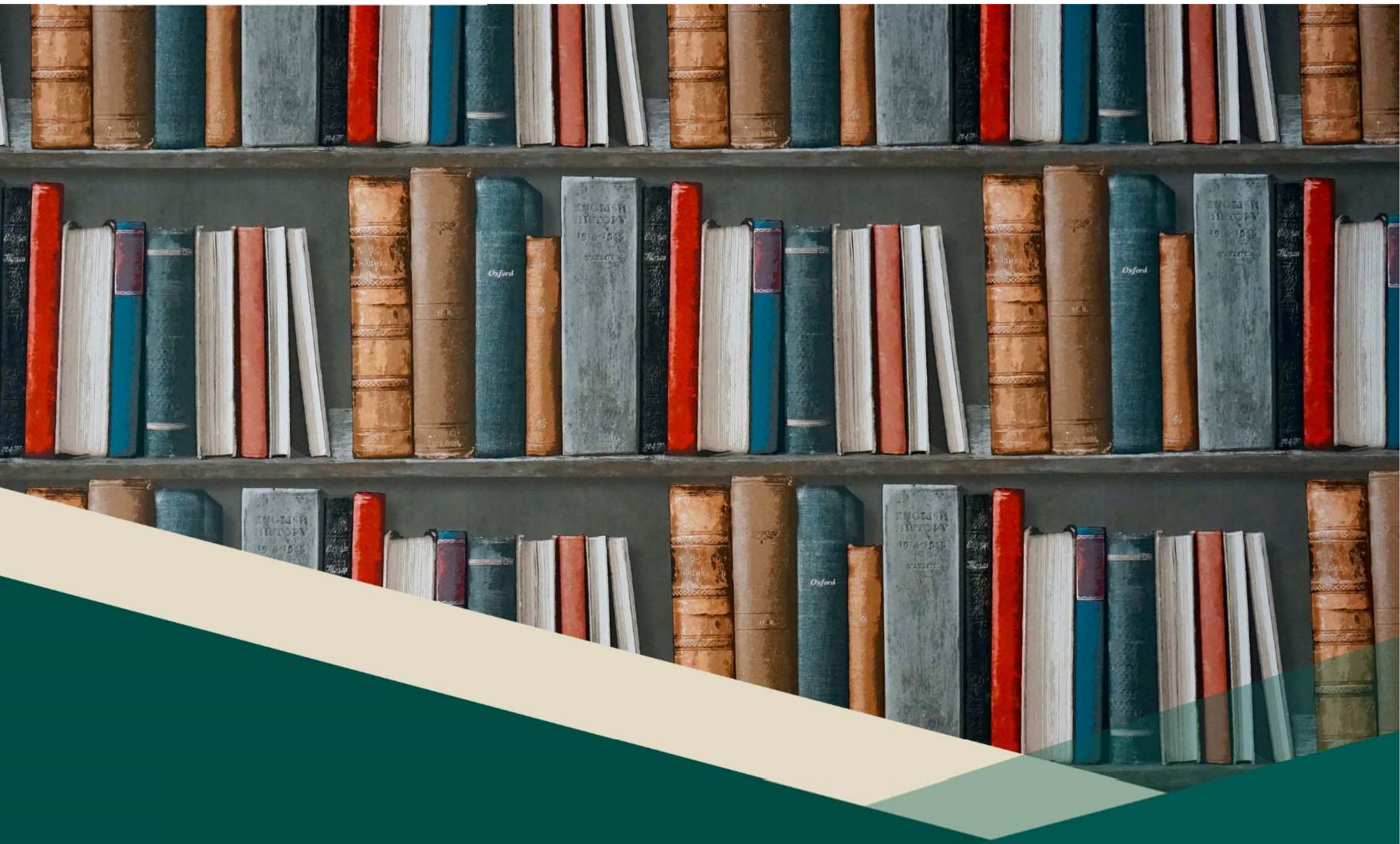
An Roinn Dlí agus Cirt
agus Comhionannais
Department of Justice
and Equality

Research and Data Analysis Unit



Cybercrime: Current Threats and Responses

A review of the research literature

Co-Authors Sheelagh Brady & Caitríona Heinl,

SAR Consultancy & EXEDEC

October 2020

An Roinn Dlí agus Cirt
agus Comhionannais
Department of Justice
and Equality

Foreword

According to the Irish Central Statistics Office (CSO), as of 2018, 89 per cent of households have Internet access at home, an increase of 17 per cent since 2010 (Central Statistics Office, 2018). On an individual level, 82 per cent of individuals used the Internet in the three months prior to their interview (Central Statistics Office, 2018). These statistics are important in the Irish context as they provide insight into the numbers of people with access to the Internet within the Irish population. In the context of this research these figures also provide an indication of the threat posed by cybercrime as it is reasonable to assume that as the number of internet users increases so too does the level of crime in the online world. The threat posed by cybercrime is something policy makers are continuously striving to adapt to and overcome and the Department of Justice and Equality is no different in this regard. This has also been a growth area over the last six months as enterprising criminals have exploited fertile new ground online during the Covid-19 pandemic.

A commitment to developing a strong evidence base for the policy and other work of the Department was the objective of our 2018-2020 Data and Research Strategy and also formed a core part of the Department's radical structural transformation in 2019.

As we continue to establish new ways of working, we will seek to continuously improve our capability in the development of evidence based work. As part of this process, we have already shared three other pieces of research over the last year. The first report focused on the important area of victims' interactions with the criminal justice system. The second report focused on the area of confidence in the criminal justice system. Our most recent publication was an evidence review of recidivism and policy responses carried out by Professor Ian O'Donnell of Institute of Criminology and Criminal Justice School of Law, University College Dublin. This new publication on cybercrime by co-authors Sheelagh Brady and Caitríona Heinl provides a worthy addition to that growing body of research as we seek to better understand and respond to emerging issues in the Department's remit.

Many of the traditional forms of crime which the Department has always played a role in combatting have now moved, at least partly, online. The Department is continually trying to develop policies and deploy effective criminal justice responses to such crimes. With regard to specific cybercrime offences, much of the focus to date has been on cyber-enabled crimes such as combatting online child sexual abuse and exploitation and economic crime. We have also concentrated our efforts on meeting international standards in this sphere and are working towards ratification of the Council of Europe’s Convention on Cybercrime (the Budapest Convention). The publication of this report will assist in developing further policy responses, particularly in relation to newer forms of cyber dependent crimes. We also work with colleagues in many other government departments and state agencies in the areas of cybercrime and cyber security. With regard to heightening awareness and prevention of cybercrime, the National Cyber Security Centre and the Garda National Cybercrime Bureau are running a campaign as part of European Cyber Security month to alert the public to the risks of cybercrime and ensure that people can better protect themselves online. This campaign is one of the key objectives of the National Cyber Security Strategy published at the end of 2019.

I very much welcome this research which will provide policy makers within this Department and further afield with food for thought concerning the current and emerging threats as well as useful models of best practice for combatting cybercrime. I want to thank and commend the co-authors for their work in researching this complex and ever evolving phenomenon.

Oonagh McPhillips

Secretary General, Dept. of Justice and Equality

Contents

Executive Summary

This piece of research examines the existing research literature on cybercrime including current and emerging threats, the Irish anti-cybercrime landscape and models of best practice for combatting cybercrime in order to inform both policy and practice across the criminal justice system in Ireland – in other words, it is not a policy report with concrete policy recommendations. It first explores the lack of consensus surrounding the term 'cybercrime' which is largely used to encompass a range of criminal activities that use information and communication technologies (ICTs). Differing definitions are often used, depending on the purpose to which they are applied, be that research, legislative, or policy making. Section Two of the report examines the ever-evolving threat landscape that requires a constant revision of responses at national and international level. This is especially the case where opportunities for cybercrime are growing because of an increasing attack surface brought about by the growth of ICTs, new technologies and more Internet users per capita. This is particularly important for Ireland given that it may not only suffer the direct consequences of cybercrime, but because of its status as a location of choice for many global technology companies and other multinationals. This means that the country must have top-tier advanced cyber readiness capabilities and avoid the indirect consequences of cybercrime such as loss of confidence from outside investors. Yet, the report finds that it is difficult to measure both the direct and indirect consequences of cybercrime. And while cybercrime-related activities occur daily, they are often not reported to An Garda Síochána. Such under-reporting, which is discussed in more detail within the report, will likely limit the ability to create effective policy solutions.

The most significant cybercrime trends and threats currently include: (1) Ransomware; (2) Other malware threats; (3) Data breaches and network attacks; (4) Spearphishing (targeting specific individuals for the purposes of distributing malware or extracting sensitive information); and (5) Attacks against critical infrastructure. These types of trends present new challenges both at home and abroad such as impacting targets indiscriminately, exacerbating already low levels of reporting to the authorities, and legislative challenges, thus calling for new policy solutions that are referenced in more detail in the report. Other trends that should ideally continue to be considered by law enforcement and policy-makers involved in the fight against cybercrime include the growing connections between cybercrime and malevolent state activity; IoT/future cities and smart meters; cloud security; emerging technologies; third party vendor risks and supply chain attacks; wide public and commercial

availability of tools and techniques as well as “Darknet” concerns; poor security cultures; the terrorist-cybercrime nexus, and pervasive anonymisation tools.

The third section of the report identifies key legislation including an assessment on its effectiveness. The key piece of Irish legislation is the Criminal Justice (Offences relating to Information Systems) Act of 2017 which amends previous Acts and gives effect to EU Directive 2013/40/EU on attacks against information systems. However, the codification of cybercrime still remains scattered across many Acts. Additionally, the transposition into Irish law of regulatory instruments like the EU NIS Directive and GDPR means that Irish individuals and entities will now be accountable for not meeting compliance obligations. This means that preventative measures are now more likely to be introduced by organisations, thus driving better resilience in the wake of cybercrime - even though it may be too soon to gauge their effectiveness on crime prevention.

Many countries, including Ireland, use a combination of traditional legislation (or at least not specifically developed to target cyber activities) and specific legislation for cyber-related activities. Irish policy-makers could ideally begin to address gaps that arise in relation to new cybercrimes where non-specific legislation is sometimes limited. Nonetheless, the report finds that while effective legislation is desirable, it is not always feasible to have legislation in place to meet the rapid pace of technological change. This means other methods (such as technology neutral provisions *et al*) could be considered to complement the more lengthy legislative process. Notably, there is limited research on the effectiveness of existing legal instruments, but analyses in the area of crime prevention more generally is better researched. Aspects of these learnings on traditional crime prevention and criminology could be transferable to the area of cybercrime.

The report highlights the implications of the lack of resourcing for An Garda Síochána in relation to cybercrime investigations and prosecutions, and the final report section finds that there is a lack of systematic reviews of best practices, both from an academic and operational perspective - even though there is a growing array of research which may result in improved mechanisms to measure success in the near future. This section identifies perceived good practices in academic writings and through interviews with key stakeholders, which align closely for the most part. It is found that the local and contextual conditions in place should be assessed before importing a model into a new area, as these are likely to have a significant impact on any new model. Moreover, any new policy practice should include mechanisms for evaluating success or lack thereof. However, this requires reliable and consistent statistics which seem to be lacking.

The report observes that any course of action should take a methodological approach to defining a roadmap for activities. Activities of this nature could include a whole of government approach, and also incorporate non-governmental stakeholders given the inherent complexities associated with cybercrimes. The report further notes from the literature that there is space for Ireland to enhance its existing, highly prized, partnerships in this area. Improvements could place Ireland in a good position to develop a systematic means of establishing best practice, and build on the rich eco-systems of universities, tech companies, law enforcement and other relevant stakeholders. To further enhance such partnerships, more formal mechanisms of collaboration could be considered.

Lastly, in terms of awareness raising, the research shows that a shift from general campaigns is needed towards more precise efforts to bring about better cybersecurity and resilience in the wake of cybercrime, mindful also of the need to reduce the risk of creating a culture of fear or a culture where victims are blamed.

List of Abbreviations

AI	Artificial Intelligence
BPFI	Banking and Payments Federation Ireland
C&AG	Comptroller and Auditor General
CCPCJ	Commission on Crime Prevention and Criminal Justice
CEPOL	European Union Agency for Law Enforcement Training
CETs	Council of Europe Convention on Cybercrime
CI	Critical Infrastructure
CIT	Cork Institute of Technology
CJS	Criminal Justice System
COE	Council of Europe
CSIRTs	Computer Security Incident Response Team
CSO	Central Statistics Office
DDoS	Distributed Denial of Service
DoS	Denial of Service
DRD	Data Retention Directive
DSP	Digital Service Providers
EC3	European Cybercrime Centre
ENISA	European Union Agency for Cybersecurity
EU	European Union
FBI	Federal Bureau of Investigation
FDI	Foreign Direct Investment
GDPR	General Data Protection Regulation
GNCCB	Garda National Cyber Crime Bureau
ICT	Information and Communications Technology
IDA	Ireland's inward investment promotion agency
IoT	Internet of Things
IP	Internet Protocol
IS	Islamic State

ISAC	Information Sharing and Analysis Centre
ISP	Internet Service Provider
IT	Information Technology
ITU	International Telecommunications Union
J-CAT	Joint Cybercrime Action Taskforce
JHA	Justice and Home Affairs
LEAs	Law Enforcement Authorities
LED	Law Enforcement Directive
NCA	National Crime Agency
NCSC	National Cyber Security Centre
NIS	Network and Information Systems
OES	Operators of Essential Services
OSINT	Open Source Intelligence
PLA	People's Liberation Army (China)
R&D	Research & Development
RATs	Remote Access Trojans
SCVO	Scottish Council for Voluntary Organisations
UCD	University College Dublin
UK	United Kingdom
UNGGE	United Nations Group of Governmental Experts
UNODC	United Nations Office of Drugs and Crime

Section 1: Introduction

According to the Irish Central Statistics Office (CSO), as of 2018, 89 per cent of households have Internet access at home, an increase of 17 per cent since 2010 (Central Statistics Office, 2018). This is in line with the EU average where in 2018, 89 per cent of the EU-28 Member State households had Internet access (Eurostat, 2019). According to the EU Digital Economy and Society Index (DESI) (2020), Finland, Sweden, the Netherlands and Denmark have the most active Internet users, followed by the UK, Malta, Estonia, and Ireland. Ireland, along with Spain, recorded the largest improvement with respect to activity levels since the last EU DESI index report.

In Ireland in 2018, 82 per cent of individuals used the Internet in the three months prior to their interview (Central Statistics Office, 2018). The EU DESI index (2020) noted that Ireland recorded an eight per cent increase in percentage points in relation to regular Internet users since the last review of 2019. As probably expected, the percentage of individuals between the age of 16 and 44 years, who had recently used the Internet (within the previous three months) was twice the corresponding figure for persons aged 60 to 74 years - these equated to 97 per cent and 48 per cent respectively (Central Statistics Office, 2018). This is also reflected in the EU DESI index (2020), which reports that the most active Internet users are young individuals. Mobile phones or smartphones appeared to be the most common methods of accessing the Internet, with 86 per cent of individuals reporting such use in 2018 (Central Statistics Office, 2018). Conversely, of those who had used the Internet in the last three months, only 24 per cent reported doing so using a desktop computer.

These statistics are important in the Irish context as they provide insight into the numbers of people with access to the Internet within the Irish population. They are also important in the global context given that it is forecasted that the global number of Internet users will rise to 6 billion by 2022 and 7.6 billion by 2030 (Statistica, 2018), illustrating the wider online community that is now more easily accessible to the Irish population. Given the focus of this research report on cybercrime, these figures are also important in the context of crime, more specifically cybercrime, especially as noted by Conway and Brady (2018) if Braithwaite's assertion to crime in the offline world holds true for cyberspace. Braithwaite asserted that as the population increases so too does the crime rate (per capita). Therefore, if one were to apply this theory to online activity, one would expect to see that as the number of Internet users increases, so too does the level of crime in the online world. Kennedy (2018) in an article for Silicon Republic noted this increase, reporting that cybercrime in Ireland is double global figures and quoting Chief Superintendent Pat Lordon from An Garda Síochána who stated “economic crime, fuelled by cybercrime, is becoming more prevalent and more costly for Irish businesses” (Kennedy, 2018, 1). A more nuanced discussion about these cybercrime figures in the Irish landscape is found within Section Two below.

Interestingly, a UK National Crime Agency (NCA) report, “The Cyber Threat to UK Business 2016/2017”, identifies a change in the nature of cybercrime. The NCA reported then that “cybercrime is becoming more aggressive and confrontational” (National Crime Agency Website, 2017). They further note that these trends were evident across various forms of cybercrime, such as high-tech crimes, data breaches and sexual extortion. Furthermore, the European Union Agency for Network and Information Security (ENISA), in its Threat Landscape Report 2017 noted that the “complexity of attacks and sophistication of malicious actions in cyberspace continue to increase” (ENISA, 2018).

This piece of research, which is funded by the Department of Justice and Equality, is therefore timely given that cybercrime is a fast growing area of crime, and because we are becoming increasingly reliant on technology in our day-to-day lives both at home and in the work place which can raise the potential for exposure to cybercrimes. There are lots of traditional crimes which fall under the remit of the Department that can now be committed via the Internet or information and communications technologies (ICTs), many of which can have serious consequences. Nonetheless, the main focus of this report is on cyber-dependent crime. As laid out in Section Two of the report, there is now what some describe as a “tectonic shift” in the cybercrime threat landscape where law enforcement and policy-makers’ understanding of modern cybercrime must likely now include expanded attack surfaces that provide more opportunities for criminals where there are growing numbers of interconnected devices and the Internet of Things (IoT). While the discussion surrounding Internet access through desktop computers and smartphones has been significant to date, the fight against modern cybercrime is facing into a period of expanded attack surfaces and disruptive technologies not witnessed before.

In line with Department of Justice and Equality requirements, this literature review examines cyber-dependent crime, the existing research literature on cybercrime including current and emerging threats, the Irish anti-cybercrime landscape and models of best practice for combatting cybercrime in order to inform both policy and practice across the criminal justice system in Ireland. The report acknowledges that cybercrime issues can be multi-faceted and as a result often span several government departments, competencies and portfolios. This review primarily examines the subject matter from the perspective of the Department of Justice and Equality. This means that some cyber threats (such as those associated with state security) have not been examined – although the report references instances where there is a nexus between state and criminal activity. Moreover, this report mainly focuses on cybercrimes with less focus on cybersecurity and cyber resilience measures.

To achieve these goals, the study answers the following questions:

- What are the current and emerging threats posed by cybercrime to Ireland and other developed countries?
- What relevant legislation is in place to combat cybercrime and how effective has this been?
- What are the models of best practice for responding to the threat of cybercrime nationally and internationally?
- What learning can be provided to inform future policy and legislative developments for combatting cybercrime?

Methodology

A review of the literature on cybercrime was conducted for the purpose of this project. A systematic approach was used to assess the quality and relevance of the literature found. See a summary of this review in Appendix A. The use of secondary sources has both advantages and disadvantages. For one, published studies are often subjected to 'publication bias', meaning significant and positive results are often more likely to be published (Dempster, 2003). Furthermore, given the topic under review, many good practices are never systematically reviewed, and therefore are not often included in academic portals. As discussed in a later section of this report, other drawbacks of over-reliance upon academic sources for discussions on contemporary cyber threats is often timeliness and relevance. By the time academic material will complete the publication cycle, key trends may have changed significantly given the rapidly changing nature of the cyber threat landscape and critical emerging technologies. Nonetheless, material from academia may provide analytical rigour and historical depth, thus grounding insights in a contextual framework. Therefore, to mitigate these issues, a broad range of secondary sources are included in this review. These include the use of a range of governmental open source material from law enforcement, intelligence and policy communities as well as non-governmental sources such as reputable global cybersecurity vendors, consultancy companies, and academia or research institutes. Therefore, only documents available within the public domain were used. It is acknowledged that these documents have their own limitations. For one, the degree of confidence in the findings can be difficult to assess.

Nonetheless, the inclusion of this broad range of documents is believed to mitigate many, although not all, of the limitations of each of these sources.

To further enhance robustness, ten interviews were conducted with a range of experts in the field of cybercrime from across academia, the private sector, as well as national and European law enforcement agencies. A purposive sampling method was used. Interviewees were selected primarily based on their expertise and experience in the area. One key area of expertise omitted from the sample relates to legal expertise. Efforts were made to engage experts for interview and review of Section Three of the report, but they were unsuccessful. Some legal experts were happy to speak about more traditional cyber-enabled crimes, but felt less competent in relation to those cybercrimes that would not come about if it were not for the use of ICTs (in other words, cyber-dependent crimes), which is an interesting finding in and of itself.

Literature search strategy

A systematic search strategy was used to identify research on cybercrime threats, the relevant legislation in this area and its effectiveness, and the models of best practice for responding to the threat of cybercrime nationally and internationally. A number of well-known databases were initially searched, such as Web of Knowledge, Scopus, ProQuest, Oxford Journals Online, Cambridge University Press Online Journals, Sage Journals Online, JSTOR Arts and Sciences, and Taylor & Francis Journals. These databases were chosen because they are interdisciplinary in nature, and include a broad range of peer-reviewed journal articles, reports and academic texts. Initially, the search strategy was designed to be as inclusive as possible, in an attempt to maximise the number of relevant articles. A number of practical issues were found in the searches. For example, in terms of academic articles on cybercrime legislation in Ireland the majority of articles pre-date the introduction of the Criminal Justice (Offences relating to Information Systems) Act 2017, which was enacted in Ireland to formalise arrangements in law and to comply with EU requirements on capabilities, cooperation and reporting. The Act amended the existing laws used to address cybercrime, such as the Criminal Damage Act 1991, the Bail Act 1997 and the Criminal Justice Act 2011, and also gave effect to certain provisions of the EU Directive 2013/40/EU on attacks against information systems. This means that many of the arguments presented in these sources are outdated.

Secondly, as Shah, Jones and Choudrie (2019) note, while research offers recommendations and some best practice for frameworks to combat cybercrime, cybercrime literature of this nature is still young. As a result, systematic reviews are limited. They also found that “there is limited literature available in terms of theories of cybercrime management” (p.1125). The academic literature that does exist in relation to cybercrime largely relates to internal fraud in the banking and other public and private sectors (Shah, Jones and Choudrie, 2019). As a result, and as mentioned above, a range of additional sources is used to mitigate such limitations. These include a range of governmental open source material from law enforcement, intelligence and policy communities as well as non-governmental sources such as reputable global cybersecurity vendors and consultancy companies. The potentially partisan nature of these publications is noted later in this report, and a critical view was maintained by the authors in reviewing these documents.

Inclusion and exclusion criteria

Extensive efforts were made to review all available information. However, given the extent of this area of study, coupled with the terms of reference (TOR), inclusion or exclusion criteria were established to ensure a more targeted approach. Such criteria was largely based on ‘relevance’ to the topic area. Material was also selected that focused on cybercrimes pertaining to the Department of Justice and Equality, rather than, for example, security and defence. To be included, articles, reports, and all documentary sources must have a focus on cybercrime, and more specially, cyber-dependent crimes. Definitions relating to the understanding of cyber-enabled and cyber-dependent crimes are discussed below. Relevance was determined against the guiding questions provided in the tender document and measured under a three-tiered classification process of high, medium and low. Given that this report examines three key areas, documents are assessed against one of these areas. For example, if a document is highly relevant to threats, but has low relevance to either or both of the other two areas, it is still said to be of high relevance. To guide the reader, the relevance of documents is broken down across the key areas of threat landscape, legislation and best practices. Documents that were not deemed to be relevant to any of the three areas were excluded. A large number of articles and reports were excluded for this reason. For example, studies relating specifically to cyber-enabled crime and articles pre-dating the Criminal Justice (Offences relating to Information Systems) Act 2017 are excluded. That said, articles relating to legislation that was not amended by this 2017 legislation are included. Document sources must have been published in 1990 or later, except for legislation if still applicable.[1] This timeframe also represents a period in which the changing nature of the threat landscape has occurred, for example, the introduction of broadband, 24/7 connectivity and more recently, the increase in Internet-enabled devices and IoT. Furthermore, all documents must have been published in English. Studies that do not meet these criteria are excluded.

Analytic strategy

Each publication is entered into a table dedicated to each section of the report. The headings used include: (i) author; (ii) year of publication; (iii) name of publication; (iv) type of study; (v) evaluation type and strength; (vi) relevance to one of the three project sections; and (vii) additional information. This process helped in assessing the relevance to the topic. The key topics under review and the guiding questions provided in the tender document were used to identify initial themes. However, as articles and reports were further analysed, other themes or contrasting themes emerged. These are documented and discussed within the document. Both authors had regular discussions about emerging findings, trends and themes. This was important in ensuring the relevant links between the three sections are identified and discussed.

Quality assessment

Two approaches to quality assessment were undertaken. The first related to the work of each of the authors. Each author independently reviewed the others work and feedback was given. Once a final draft was completed, the draft was reviewed by Dr. Shane Horgan of Edinburgh Napier University. Dr. Horgan provided feedback and comments on areas that required additional work. These recommendations were taken on board and addressed in the final version of the report. Appendix A includes a data coding process matrix outlining the quality of the publications reviewed.

Overview of the Report

The report is structured as follows:

[1] The research for this report was conducted in 2019, for the most part, and therefore annual reports or statistics used largely relate to 2018, as these were the most recently available annual reports at that time.

Section 1.1 considers foundational questions related to the definitions of cybercrime.

Section 2 examines research on the current and emerging threats posed by cybercrime to Ireland and other developed countries. It begins by framing the discussion surrounding current and emerging cybercrime threats. It then examines the broad trends behind the pervasiveness of cybercrime, before presenting the current and emerging threats in European, other developed countries and Ireland. It ends by examining the factors with an impact on the evolving cybercrime threat landscape.

Section 3 outlines the relevant legislation that is in place to combat cybercrime. It considers Irish legislation, as well as applicable international and EU instruments. This section then provides an assessment of the effectiveness of legislation in combatting cybercrime in terms of prevention, prosecutions, convictions or other measures.

Section 4 outlines models of best practice for responding to the threat of cybercrime nationally and internationally.

The report concludes with an overview in Section 5 of the most salient findings and key learnings to inform future policy and legislative developments for combatting cybercrime.

1.1 Definitions of cybercrime

This section briefly considers definitional matters relating to the precise definition - or lack thereof - of ‘cybercrime’. This is not an exhaustive discussion. It is an indicative piece that illustrates the lack of agreed definitions, but does not go so far as to suggest or analyse a proposed definition since this is beyond the scope of the literature review. However, this section acts to frame the definitional approach used in relation to this piece of research.

There is no universally agreed definition of the term ‘cybercrime’ nor is there consensus as to what cybercrime actually is (Wall, 2004). It is often a term used to encompass a range of criminal activities that use information and communication technologies (ICTs). Other interchangeable terms are also often used, such as ‘virtual crime’, ‘net-crime’, ‘hi-tech crime’ or ‘computer crime’ (Wall, 2004). The lack of clarity can be confusing and disconcerting and has led to a tendency, amongst some, to label any offence that involves a computer or part thereof as a cybercrime (Wall, 2004). To overcome this, Wall (2004) purports that one should consider how the use of ICT transforms a crime, rather than the act itself. To do this, he suggests the use of an elimination test, in which one thinks about what would happen if the use of ICT were removed from the offence. From this approach, he notes that three different types of opportunity emerge. The first are “behaviours often called cybercrimes that are ‘traditional’ crimes in which a computer has been used” (Wall, 2004: 20, exemplified by the use of ICT in the commission of a crime such as fraud). The second are “hybrid cybercrimes – traditional crimes for which network technology has created entirely new global opportunities” (20), exemplified through global frauds. The third are “true cybercrimes which are solely the product of opportunities created by the Internet and which can only be perpetrated within cyberspace” (20), exemplified through spam, phishing and other forms of social engineering. Similarly, Grabosky (2004) also breaks cybercrime into three forms. These three forms are: (1) conventional crimes committed with computers, such as digital child pornography, piracy, or intellectual property theft, and forgery; (2) attacks on computer networks; and (3) conventional criminal cases such as drug trafficking, in which evidence exists in digital form (Grabosky, 2004).

Although slightly different, these categorisations are important not only in the context of providing clarity about the role of ICT in criminality, but also in relation to response, and especially in the context of legislative applicability. The first of Wall’s two categories stem from traditional crimes, which he suggests are likely to be the subject of existing laws. Any legal problems enforcing such laws when applied to crimes that involve the use of ICT tend to relate more to legal procedures rather than substantive law, he argues. However, he (Wall, 2005a) notes that it is the third category - those crimes that are solely the product of ICT - where problems can exist in regard to responding or managing them. It is this perspective that will be explored further in this research.

Others prefer two categories. Gordon & Ford (2006) argue cybercrime can be distinguished by how a computer or ICT is used in the commission of the offence. For example, category one includes crimes that involve computers or ICT as the primary factor, such as malware, in contrast to category two, which involves humans as the primary factor, such as online grooming. This distinction is somewhat similar to that made in the United Kingdom’s National Cyber Security Strategy (2016-2021) where the term is broken down as cyber-enabled crimes and cyber-dependent crimes (Hull, Eze, Speakman, 2018). This distinction is often said to be based on new and old crimes.

Cyber-dependent crimes are viewed in the United Kingdom as new crimes, which could not exist without ICT, often described as ‘true cybercrimes’. In legal parlance, ICT is required to commit the Actus Reus[2] of the crime. While cyber-enabled crime, often said to be traditional crimes, are enhanced or scaled through the use of ICT (Hull, Eze, Speakman, 2018). For example, online fraud where fraud can be conducted without the use of ICT, but its scale and reach can be increased through the use of ICT. Two of the most widely published instances of cyber-enabled crime relate to fraud and theft (McGuire & Dowling, 2013; p 4). In short, cyber-dependent crimes are often viewed as cybercrimes in their purest form, while in contrast, cyber-enabled crimes are often referred to as traditional crimes - those that can still be committed without the use of ICT.

The European Commission relies on three categories to define cybercrime. According to the EU Cyber Security Strategy 2013:

> "Cybercrime commonly refers to a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target. Cybercrime comprises traditional offences (such as fraud, forgery, and identity theft), content-related offences (such as online distribution of child pornography or incitement to racial hatred) and offences unique to computers and information systems (such as attacks against information systems, denial of service and malware)" (p 3).

In operational terms, the European law enforcement agency, Europol, understands cyber-dependent crime in the following way:

> "[A]ny crime that can only be committed using computers, computer networks or other forms of information communication technology (ICT). In essence, without the Internet, criminals could not commit these crimes. It includes such activity as the creation and spread of malware, hacking to steal sensitive personal or industry data and denial of service attacks to cause financial and/or reputational damage" (European Cyber Crime Centre (EC3), 2019, p. 14).

The 2013 EU Directive on attacks against information systems establishes minimum rules on the definition of criminal offences. The objectives of this Directive are to approximate the

[2] The actus reus "consists of some act or some omission forbidden by law. The conduct of the accused must come within the forbidden action. The actus must be directly attributable to the accused and not to another person, unless the accused incited that other person or they shared a common purpose. The actus must be done voluntarily" (Doolan, 2011, 133).

criminal law of the EU Member States in the area of attacks against information systems by establishing minimum rules concerning the definition of criminal offences (2013/40/EU (1)).

Many nations do not adopt a statutory or case law definition of cybercrime, because requirements of the definition change depending on the purpose in which the definition is used, for example, research, legislation, policy making (UNODC, 2013). The limited use of a strict definition in national legislation is an issue discussed in detail in the UNODC report ‘Comprehensive Study on Cybercrime’ 2013. The findings of this study note that nations do not appear to be concerned with having a strict definition. The results of their questionnaire showed that “out of almost 200 items of national legislation cited by countries in response to the Study questionnaire, fewer than five per cent used the word ‘cybercrime’ in the title or scope of legislative provisions. Rather, legislation more commonly referred to ‘computer crimes, electronic communications, information technologies, or ‘high-tech crime.

To illustrate the status quo described by the UNODC (2013) and the ways in which the term differs across jurisdictions, the following matrix is included below. The National Cyber Security Strategies of six nations were examined to compare and contrast different definitions or descriptions of ‘cybercrime’. This is not an exhaustive list, but an illustration of the differing non-legislative definitions or descriptions used across jurisdictions. Of these six strategies, two (one of which is the Irish National Cyber Security Strategy 2019-2024), do not define or describe the term, but do address the issue of cybercrime. Therefore, in respect to Ireland a general definition of cybercrime as described on the Department of Justice and Equality website is used in the table below for the purposes of this report. While, in respect to the Danish definition, this was taken from the Cyber Threat Against Denmark document 2019.

Table 1

Country	**National non-legislative definitions or descriptions of the term ‘cybercrime’**
Australia	‘Cybercrime’ refers to crimes directed at computers, such as illegally modifying electronic data or seeking a ransom to unlock a computer affected by malicious software. It also includes crimes where computers are part of an offence, such as online fraud (Australian Government, 2016, p 15).

Denmark	Cybercrime refers to perpetrators that use cyber attacks to commit financially motivated crimes (Danish Government, 2019, p 6).
Ireland	Cybercrime comprises traditional offences (e.g. fraud, forgery and identity theft); content related offences (e.g. online distribution of child sexual abuse material, hate speech or incitement to commit acts of terrorism); and offences unique to computers and information systems (e.g. attacks against such systems, spread of malware, hacking to steal sensitive, personal or industry data and denial of service attacks to cause financial and/or reputational damage). Electronic devices are also used to sell and transfer all sorts of illicit goods and services, from illicit drugs to online child sexual abuse and exploitation materials to lists of stolen credit card numbers (Department of Justice, Website, 2020)
The Netherlands	The term cybercrime covers a broad range of criminal actions, from classic crime in digital form to new crime. This involves, for instance, hacking computers to transfer money to criminal bank accounts or turning on cameras and microphones undetected to be able to spy on people in their own surroundings (Dutch Government, 2018, p 35).
New Zealand	Crimes that are committed through the use of computer systems, and are directed at computer systems. Examples include producing malicious software, denial of service attacks, and phishing. Cyber-enabled crimes [are] crimes that are assisted, facilitated or escalated in scale by the use of technology. Examples are cyber-enabled fraud and the online distribution of child exploitation material (New Zealand Government, 2019. p 16).
United Kingdom	Cyber-dependent crimes - crimes that can be committed only through the use of Information and Communications Technology (‘ICT’) devices, where the devices are both the tool for committing the crime, and the target of the crime (e.g. developing and propagating malware for financial gain, hacking to steal, damage, distort or destroy data and/or network or activity). Cyber-enabled crimes - traditional crimes which can be increased in scale or reach by the use of computers, computer networks or other

	forms of ICT (such as cyber-enabled fraud and data theft) (United Kingdom's National Cyber Security Strategy, 2016, p 17).

1.2 Classification of cybercrime used for the purpose of this report: 'Cyber-dependent crime'

Given the saturation of Internet-connected technologies in everyday life, much of all crime exists on a technological spectrum. Wall has since abandoned this definitional work, as the distinctions he makes have become increasingly blurred. Furthermore, many offenders may engage in a range of cyber-enabled, cyber-dependent and offline offences for the purpose of achieving their goals. This can complicate definitions and add to the problems of assessing cybercrime levels (discussed later in the report). Furnell (2003) notes that it may be more important to make sense of the actual threat posed, the harm it causes and how to prevent it, than focus on situating cybercrimes into particular categories. He suggests that definitional work is hampered by the rapid speed of threat emergence mentioned above, as well as the broad range of actors.[3]

In any case, for the purpose of this report, the classification of 'cyber-dependent crime' is used, and is one based on typology. More specifically, cyber-dependent crime refers to illicit activities such as, unauthorised access offences; illegal interception of communications, illicit online markets; theft of services; theft of resources; piracy; destruction or damage of data; website defacement; interfering with the lawful use of a computer; the production and/or distribution of malware; denial of service; and terrorism (Yar & Steinmetz, 2019; Grabosky, 2017). This approach also takes into consideration the fast pace at which technologies develop and change, and is cognisant that this list is subject to change and extension.

This approach is based on two key factors, namely:

[3] See Dunn-Cavelty on threat framing and the ways in which this has been mobilised for political gain – and ultimately left cybercrime representing something of an empty vessel meaning both everything and nothing.

I. The Department of Justice and Equality has conducted considerable work in the area of cyber-enabled crime such as content related offences. As a result, it was agreed that this research report would specifically focus on cyber-dependent crimes.

II. The extent of current and future threats facing Ireland is such that dedicated research in relation to cyber-dependent crime is warranted. For example, the background note for the consultation held in preparation for the second Irish cybersecurity strategy specifies "that some of these new vulnerabilities are simply new manifestations of age-old activities, and involve the mere theft of data or money. Others are entirely new, and include the remote destruction of data or critical infrastructure (CI)." (Department of Communications, Climate Action and Environment, 2019, p.5.).

Again, this report is best viewed through a criminal justice focused lens, rather than security or defence, even where overlapping matters may arise. It is beyond the scope of this report to consider these overlaps between agency mandates when dealing with cyber-related matters. While this report is not exhaustive, it aims to provide an overview of the existing research literature on cybercrime including current and emerging threats, the Irish anti-cybercrime landscape and models of best practice for combatting cybercrime, pertaining to the Department of Justice and Equality for the most part, in order to inform both policy and practice across the criminal justice system in Ireland.

Section 2: What are the current and emerging threats posed by cybercrime to Ireland and other developed countries?

2.1 Framing the discussions surrounding current and emerging cybercrime threats

An understanding of the nature and extent of modern cybercrime risks facing Ireland will help to determine suitable responses and measures for their prevention and mitigation. This section therefore provides an overview and analysis of the current and emerging threats posed by cybercrime to Ireland and other developed countries, as set out in the reviewed literature. As the introductory section specifies, cybercrime for the purposes of this report is understood to comprise offences unique to computers and information systems. This could include, for example, attacks against such systems, spread of malware, hacking to steal sensitive, personal or industry data and denial of service attacks to cause financial and/or reputational damage.[4] In other words, this section does not consider current and emerging cybercrime offences that comprise traditional offences such as fraud or content related offences (Department of Justice and Equality, 2019).

This section first highlights a number of contextual questions surrounding modern cybercrime, followed by more detailed analysis on the threat landscape in Europe, developed countries and Ireland. It lastly highlights other considerations that can impact the evolving cybercrime threat landscape in Ireland. Throughout the analysis, further detail is provided on the following factors: (1) The prevalence of cybercrime and issues in assessing the levels of cybercrime; (2) The extent to which threats may vary from country to country and what factors create such variation; (3) Specific threats to which Ireland may be particularly vulnerable, and (4) Analysis of such threats to Ireland which may be of particular concern from a criminal justice perspective.

While this part of the report outlines the dangers associated with contemporary and emerging cybercrime threats, hacking is not a new phenomenon. Nearly twenty years ago, academics were already writing about cybercrime as the “newest security threat in the world today…distinct from any other threat facing the world…” (Speer, 2000; see Taylor, 1999 for a more extended history). Yet, there is a present-day risk that analyses

[4] Note that ‘hacking’ is understood to be criminal activity, rather than ethical hacking or pentesting.

and public reporting continue to perceive cybercrime activities such as malware, hacking and bots as a new problem that are therefore very difficult to combat because of their modern nature (Arthur, 2018, p.3). While the threat landscape does continue to constantly evolve and mature requiring a constant revision of mitigation and responses at national and international level, these types of perceptions can often also lead to a fearful narrative surrounding cyber threats, most obviously evidenced within sensationalist headlines. Hacking is decades old and many recent malevolent cyber incidents that are sometimes perceived or described as novel were either outlined in academic research as much as 20 years before or arise from old flaws and exploits that are still prevalent (Arthur, 2018, p.3). The background note (2019) for the consultation held in preparation for the second Irish cybersecurity strategy partly captures this sentiment, highlighting that

> “[S]ome of these…new and confounding vulnerabilities are simply new manifestations of age old activities, and involve the mere theft of data or money. Others are entirely new, and include the remote destruction of data or critical infrastructure (5)”.

A general pattern of evolution often underpins these cyber-related threats and trends - this “Darwinian evolution” that can be ascribed to the nature of cybercriminals’ and defenders’ activities means that efforts to enhance cybersecurity often results in cybercriminals maturing their tactics, techniques and “business models” (Kaspersky Lab, 2018, p.1). For instance, criminal cyber activities are generally conducted against broad categories of targets such as individuals, small organisations and medium to large corporations, as well as against State assets such as critical infrastructure (CI) or government resources (Hilliard, 2018). As cybercriminals’ techniques and tools become more sophisticated, it seems that they will likely then focus their attention on more lucrative targets such as large organisations (even where the literature would likely need to explore the implications on these expected sophisticated activities against large organisations some of which may have greater incentives and means to protect themselves). Law enforcement describes this three-fold pattern as follows. First, criminals become more sophisticated with particular tools. Second, these tools become more sophisticated and easier to obtain, and third, criminal focus becomes more targeted and shifts towards small businesses and larger targets with higher profits than individuals (EC3, 2018, p.17). Moreover, as law enforcement responses displace cyber-criminal activity, it can sometimes lead to ratcheting up of the operational security of the actors themselves (Decary Hetu et al. 2017). For example, this pattern is presently evident in recent threat assessments surrounding criminals’ use of ransomware, which is described in more detail below. Understanding that this is a traditional pattern of evolution of criminal cyber activity, law enforcement (in Ireland at national level and/or abroad together with other law enforcement authorities) could consider taking additional steps to implement solutions that are thus more proactive and long-sighted.

Even though the ever-increasing complex threat landscape garners much public attention, currently there are two broad concurrent trends towards both simplicity as well as complexity, which thus exacerbate overall complexity within the threat landscape (Kaspersky Lab, 2018*, p.1)*. The first tendency towards simplicity means that criminals may be driven by cost efficiency and thereby employ simpler efforts in development of tools or techniques and attack methods (Kaspersky Lab, 2018, *p.2)*. They may, for instance, tend to use publicly available off-the-shelf malware (possibly tailoring it marginally) or rely on victim's poor security measures (Kaspersky Lab, 2018, *p2)*. In other words, there is often no need to develop new malware where older software is sufficient for criminal purposes. Cybersecurity companies such as Kaspersky Lab (2018, p2) further notes the growing ease of doing business for less skilled cybercriminals where malware is marketed and criminal services sold within the drastically expanding "hackers' bazaar" that very often includes user support.

On the other hand, ICTs as well as other emerging technologies such as AI and machine learning are maturing at great speed. There seems to be consensus across stakeholders that the associated risks are increasing exponentially, so much so that such complexity cannot be fully understood anymore (European Commission, 2017a and Kaspersky Lab, 2019). Similarly, technological progression in tools and techniques employed by cyber attackers continues (Kaspersky Lab, 2018, p2*)*. Global cybersecurity vendors flag increased anonymity as one of the most important developments behind this recent "tectonic shift" in the threat landscape. Such anonymity can be provided through the emergence of legitimate online tools such as Bitcoin and other cryptocurrencies that allow untraceable payments as well as Tor-like networks allowing anonymous online communication and trade of both information and technologies (Kaspersky Lab, 2018, p1-2).

2.1.1 A NEED TO DRAW ON NUMEROUS GOVERNMENTAL AND NON-GOVERNMENTAL RESEARCH SOURCES

Analyses in Ireland of the evolving nature of current and emerging cybercrime threats must be conducted against the backdrop of these types of general patterns. Moreover, unlike other traditional fields of security and crime, concrete analyses on 'cyber' require a consideration of material from a variety of governmental and non-governmental sources. There are lots of different actors and academic disciplines involved in the study of 'cyber', which means that it can sometimes be difficult to draw on a coherent body of knowledge that can inform policy, practice and prevention, thus justifying the need to draw on a wide range of material. This section of the report relies on a range of governmental open source material from law enforcement, intelligence and policy communities as well as non-governmental sources such as reputable global cybersecurity vendors, consultancy companies and academia/research institutes. While such stakeholders may sometimes have different perspectives and interests, the report will outline significant divergences where relevant. Global cybersecurity vendors' findings are often particularly insightful and timely given the industry's global reach and cybersecurity intelligence networks with sight across most regions. This report purposefully draws on material from cybersecurity vendors of different national origins to ensure a fair and broad approach, thereby avoiding over-reliance on U.S. vendors. It is generally understood that several global cybersecurity vendors often have timely sight of threats and trends as well as capabilities that many government authorities will lack. There is an unwritten understanding, however, that some of these corporate reports may mostly highlight those areas where they have services or products to offer in return (BH Consulting, 2015). For example, industry reports on cybersecurity practices in Irish businesses might heavily emphasise the interest of Irish stakeholders in biometric technological solutions for poor cybersecurity practices. Whereas intelligence outfits seriously question our ability to protect such biometric information given the very serious long-term consequences of failing to do so properly (Heinl, 2019). Moreover, government authorities may often have non-technical attribution capabilities and law enforcement or intelligence insights that corporations specialising in technical attribution will naturally lack.

The drawback of over-relying upon academic sources for discussions on contemporary cyber threats is often timeliness and relevance. By the time academic material will complete the publication cycle, key trends may have changed significantly given the rapidly changing nature of the cyber threat landscape and critical emerging technologies. Nonetheless, material from academia may provide analytical rigour and historical depth, thus grounding insights in a contextual framework. Unlike many traditional security and crime fields, law enforcement, intelligence authorities and policy-makers in Ireland will likely also have to collaborate with such non-governmental stakeholders in order to combat modern cybercrime effectively (see also Wall 2007 Policing Cybercrime). That said, there is much literature on the drawback of multi-agency public-private partnerships (Yar and Steinmetz 2019; Levi and Williams 2013).

2.2 Understanding broad trends behind the pervasiveness of cybercrime

The prevalence of cybercrime often correlates with opportunities for these crimes to be conducted that is presented by a changing and increasing attack surface brought about by the growth of ICTs and new technologies. Much of the policy literature notes that increasing individual and national dependence on digital technologies is creating an opportunity for more exposure to nefarious activities (European Commission, 2017a). As far back as 2011, academic studies found that wealthier nations with more Internet users per capita had higher cybercrime activity (Kigerl, 2011). This section notes that it is difficult to ascertain the level of cybercrimes that are indeed committed in Ireland and there is a need for greater transparency as to the level of risk. In Ireland's case, the State now ranks seventh in the 2019 EU Digital Economy and Society Index which means that it is now among the leading ranks of EU Member States in terms of the uptake and use of digital technologies (European Commission, 2019a, p.3). This sophisticated, and growing, technological advancement could then mean that Ireland – like other technologically sophisticated countries- can be an attractive target for crime actors and disproportionately vulnerable to malevolent state and non-state cyber activities where such ranking "reflects an underpinning set of vulnerabilities" (Heinl, 2019 and Department of Communications, Climate Action & Environment, Draft Public Consultation, 2019, p.1). This hypothesis relies on a so-called 'connectivity paradox' which means that '[w]hereas during the Cold War it was assumed that technological supremacy would equate to strength and safety, in the digital era, as the most technologically sophisticated countries become ever more cyber-dependent, technological advancement has had the opposite effect, with those societies becoming disproportionately vulnerable to cyber attack' (Wilton Park, 2018). Ireland, like most EU Member States, has highly developed ICT-dependent infrastructure (Department of Communications, Climate Action & Environment, Draft Public Consultation, 2019, p.9). In other words, these developments are reflective of this "connectivity paradox" whereby the most technologically sophisticated countries become even more cyber dependent and their technological advancement means they are becoming disproportionately vulnerable to cyber attack (Wilton Park, 2018). Notably, however, high levels of vulnerability may not directly translate into high levels of criminal activity. Such levels of vulnerability, which enable opportunities for cybercriminals, are also contributing factors to threat variances between regions and lesser-developed countries vis-à-vis more developed and technologically advanced jurisdictions like Ireland or other EU Member States.

Another factor for developed countries like Ireland to consider is the impact of cybercrime activity in Ireland and other developed countries from those countries that often account for more of the variation in cybercrime activity than others – in other words, this subsequently affects nations with less criminal activity given the ability for these activities to reach beyond national borders (Kigerl, 2011). High levels of unemployment in such countries are one of a number of reasons for such variation (Kigerl, 2011). Furthermore, experts find that different levels of capacity for ICT security among States can increase vulnerability in an interconnected world (UN Group of Governmental Experts, 2015, p.6).

Some states may lack sufficient capacity to protect their ICT networks and a lack of capacity can make the citizens and CI of a State vulnerable or make it an unwitting haven for malicious actors (UN GGE, 2015, p.10). In other words, such havens and other states' lower levels of capacity for ICT security can potentially impinge upon the safety of Ireland's citizens and CI. This means that An Garda Síochána and policy-makers could ideally consider the development of solutions that reach beyond Irish borders to assist in mitigating these problems for collective security. For example, the UN GGE of 2015 endorsed the recommendations of capacity building in the 2010 and 2013 GGE reports whereby the 2010 report recommended that States identify measures to support capacity building in less developed countries (p.10). The 2013 report called on the international community to work together in providing assistance to improve the security of critical ICT infrastructure; develop technical skills and appropriate legislation, strategies and regulatory frameworks to fulfil their responsibilities; and bridge the divide in the security of ICTs and their use (p.10). Goals to pursue sustainable cyber capacity building within Ireland's national cyber security strategy for the period 2019-2024 could hopefully begin to address this problem in part where growing Internet penetration may result in emergence of safe havens that can be exploited by international criminal networks. Cyber capacity building efforts have been established by several countries for many years through bilateral capacity building initiatives as well as regional endeavours facilitated by nation states or international organisations such as INTERPOL and the Global Forum on Cyber Expertise (GFCE) as well as EU capacity building endeavours. In this case, Ireland could develop its own bilateral capacity building initiatives or leverage/complement efforts conducted at regional and international level that align with the State's priorities.

Cybercrime levels are sometimes also described in economic terms. The economic impact of cybercrime in Europe, for example, apparently grew “fivefold” from 2013 to 2017 (European Commission, 2017a). Whereas the overall cost of cybercrime to the Irish economy was estimated to be Euro 630 million in 2014 (Harris and Singla, 2014). However, given that in the majority of cases, it is often difficult to trace cybercriminals and even more difficult to pursue successful prosecutions, there can be challenges with the metrics for how cybercrime levels are assessed (European Commission, Building strong cybersecurity, 2017).[5] This can further include the measurement of both direct and indirect consequences of cybercrime that can be difficult to measure. This is a complex

[5] Crimes have a number of classifications such as ‘recorded crime’, a ‘reported crime’ and a conviction.

challenge and measurements can vary to great degrees. For example, the UK’s Home Office produced a research report on this question after establishing a working group. The report included a summary of why the literature is difficult to reconcile and why cost estimates can vary significantly (Home Office, 2018). In short, if the Government of Ireland would like to ensure that measurements are useful, they would likely need to be carefully devised, revised and employed routinely, while also acknowledging their precarity. Nonetheless, a number of studies have developed methodologies to measure the cost of cybercrime (Anderson et al 2012; Rainer, 2013; Anderson et al 2019).

While cybercrime-related activities occur prolifically on a daily basis, they are often not reported to law enforcement – in the case of Ireland, apparently only five per cent of cybercrimes are reported to An Garda Síochána (Gallagher, 2019). Law enforcement authorities (LEAs) are also challenged when pursuing successful prosecutions for reasons that include: (a) the need for better capacity to identify those responsible for cyber attacks; (b) the difficulty in finding useful information for cybercrime investigations (mostly in the form of digital traces); (c) the speed of malicious cyber activities that overwhelm law enforcement procedures; (d) the need for better forensic capabilities and the difficulties associated with different cross-border forensic procedures; and (e) ineffective cross-border cooperation (European Commission, 2017a). These challenges are described in more detail later in the report. Moreover, Ireland is an outlier in a number of cases within the Eurobarometer cybersecurity survey for metrics on willingness to report to the police. The common response to cybercrime (such as an email or social media account being hacked) for respondents in Ireland would be to contact their Internet service provider as compared to other EU member states’ respondents where the most common response remains going to the police. Victims’ willingness to report can be affected by factors that include: (1) awareness; (2) stigma; (3) seriousness; (4) unawareness of who to report to; (5) uncertainty as to what cybercrime actually means, and at what point minor disorder constitutes a criminal offence. Whereas businesses may also suffer from lack of awareness, but also concerns about reputational damage. Moreover, comparative measurements are hard to make even internationally where there can be definitional inconsistency or ambiguity, or where there are a variety of priorities across police organisations to record, even to the extent that having a system in place to record or label an incident as ‘cyber’-related may not be that common. This means that how we count, or what value we attach to cybercrime (whether money was lost or measure harms beyond financial) means that our estimates are at best very rough. As Wall (2007) points out, this is likely not only as a result of these types of factors, but also a result of the way people understand the police role and threshold of seriousness required to engage with the police. Clough (2012) includes a useful discussion on the challenges of managing and recording the prevalence of cybercrime in general.

EU strategy documents note that the common practice of placing many users (sometimes thousands of users) behind one IP address can make it technically challenging to investigate criminal online behaviour (European Commission, 2017a). In the Irish context, the ability to assess within the public domain the prevalence of cybercrime is difficult because of the lack of public data specific to Ireland. Many independent and non-governmental reports on cybercrime focus on the United States, the EU or the United Kingdom (BH Consulting, 2015). Even though a number of industry reports have been written specifically on the Irish landscape (which are referenced below), this is by no means close to the number of reports covering other countries and jurisdictions. Furthermore, the number of cyber threats averted by security agencies and law enforcement in Ireland may not always be public knowledge given the perceived sensitivity of some of these subjects, in which case there is a risk that the general public does not realise the full extent of the problem (Hilliard, 2018). Moreover, while LEAs across the EU, including An Garda Síochána, submit data on incidents to Europol's EC3 for assessment on the level of cybercrime, a mere five per cent level of reporting to An Garda Síochána in Ireland will likely limit the ability to form a clear picture for law enforcement and policy purposes (as mentioned above, while cybercrime-related activities occur prolifically on a daily basis, they are often not reported to law enforcement – in the case of Ireland, apparently only five per cent of cybercrimes are reported to An Garda Síochána (Gallagher, 2019)). Policy and applied solutions that aim to increase the level of reporting in Ireland are likely needed, in addition to the reporting and compliance requirements stemming from the implementation of new legislation as a result of the EU General Data Protection Regulation and NIS Directive. Moreover, a vast majority of incident reports to the National Cyber Security Centre (NCSC) are not reported to An Garda Síochána.

It is likely that financially motivated cybercriminals may find Ireland is an attractive target given the presence of major global software companies, the top ten global ICT companies, social media companies, numerous supercomputers and a rising number of data centres (Department of Communications, Energy & Natural Resources, 2015-2017 and Cahill, 2018). While multinational corporations or major global companies are often harder targets given their likely high level cybersecurity protections and their vast resources that can be applied to security, they still continue to be lucrative and attractive targets for criminals given the extent of personal information and data that can be accessed and potentially even used for other criminal purposes. The State is also host to a thriving international financial centre. Dublin is apparently now ranked as the third largest tech cluster in Europe, with expectations that the tech sector could grow even more with increasing interest from both international and indigenous firms (Keane, 2018). The State has been cognisant for many years that Ireland thus faces a more complex set of risks than many other countries given the presence of many data centric international companies and the growing numbers of data centres together with the associated risks of potential reputational damage (Department of Communications, Energy & Natural Resources, 2015-2017, p.5). In other words, Ireland may have more to lose than other states facing similar levels of cyber activity, including indirect consequences of cybercrime such as loss of confidence from outside investors and reputation as a weak link in European security. Such a potential loss of confidence could be further exacerbated by negative reporting on the state of cybersecurity in Ireland. Recent media reporting on the Comptroller and Auditor General audit in 2018, which finds that the Irish National Cyber Security Centre (NCSC) “appeared to have no strategic plan, and raised questions over its funding structures”, is one such example (Hilliard, 2018). Notably, the Department of Communications has since rebutted these allegations of deficiencies within press enquiries (Hilliard, 2018). Additional examples of negative perceptions about the state of cybersecurity in Ireland include reporting on a survey conducted ahead of the Dublin Info Sec 2016 cybersecurity conference where it was found that 90 per cent of businesses surveyed thought then that the country is not prepared for a potential attack on the State (O’Donovan, 2016). Prior to the publication of the current national cyber security strategy (2019-2024), commentators have thus noted that this second cyber strategy should reaffirm in late 2019 that Ireland’s status as a location of choice for many global technology companies means that the country must have top-tier advanced cyber readiness capabilities (Day, 2019). These capabilities should be along the lines of comparable advanced economies such as the United Kingdom, other EU Member States and the United States.

Nonetheless, other surveys such as the 2019 survey by a tech consumer website (Comparitech) note that ‘Ireland is in the top 10 in the world when it comes to cybersecurity’ given that Ireland sees ‘just under 4 per cent of mobile phones infected with malware, as well as almost 8 per cent of computers’ (Irish Examiner, https://www.irishexaminer.com/breakingnews/business/irish-cybersecurity-among-the-best-in-the-world-902629.html, February 2019). Other statistics provided in this survey include 0.5 per cent of Irish online users having been the subject of financial malware attacks. That said, representatives of the tech consumer website note that ‘[d]espite some countries having clear strengths and weaknesses, there is definite room for improvement in each and every one….[w]hether they need to strengthen their legislation or users need help putting better protections in place on their computers and mobiles, there’s still a long way to go to make our countries cyber secure’ and there is room for ‘significant improvements’. They note that this is often on account of the constantly changing cybersecurity and cyber scam landscape. Other vendor reports (Specops Software) note that the Netherlands is the most vulnerable European country, holding the highest rate of cybercrime, explained to be on account of the large number of cloud provider incoming attacks (PrivSec Report, https://gdpr.report/news/2020/02/25/privacy-ireland-ranked-least-vulnerable-european-country-to-cybercrime/, February 2020). Whereas 'Ireland ranks as the most cyber secure and least vulnerable European country, having the lowest cybercrime encounter rate in every category expert [typo:except] cloud provider attacks, where it experienced 0.36% incoming attacks' (PrivSec Report, February 2020).

Drawing upon findings within a 2018 PwC report, the Minister for Justice, Charlie Flanagan, is reported to note an increase in cybercrime incidents when explaining that this is a notable threat to Ireland's attractiveness as a business location for investors and a concern for Ireland's digital economy (McLaughlin, 2018). In other words, indirect consequences of cybercrime can easily also manifest in Ireland if left unaddressed. Media articles on the PwC report note that more than 60 per cent of Irish businesses reported cybercrime incidents in a two-year period (McLaughlin, 2018). The survey, which was conducted on "77 organisations from across all key sectors and industries", specifically notes that 49 per cent of Irish companies surveyed experienced economic crime over a two-year period, and of those crimes reported, 61 per cent experienced cybercrime (PwC, 2018). In 2016, 45 per cent of businesses surveyed for the Dublin Info Sec conference confirmed that they had already been victim to cyber incidents (O'Donovan, 2016). A later Microsoft report on large organisations in Ireland finds that 44 per cent of the surveyed public and private sector organisations' employees have had difficulties with phishing, hacking, "cyber fraud" or other cyber attacks, with 31 per cent reporting problems in their personal capacity and 18 per cent in their workplace (Amárach Research, 2019 (commissioned by Microsoft)). Nonetheless, by way of contrast, the UK Cybersecurity Breaches 2019 survey (or similar surveys in other jurisdictions) are reports that can be consulted on comparable breaches experienced by businesses that are published by government departments together with research institutes, rather than relying too heavily on industry reports like those cited above as a source for this information.

Notably, the numbers of those companies experiencing cybercrime has apparently now grown in Ireland - it is now double global levels of 31 per cent despite increased levels of awareness and more resources being allocated to address risks (PwC, 2018). Organisations report average losses fuelled by such cybercrime in Ireland at approximately Euro 810,000 and nearly 70 per cent of those surveyed confirmed that the same amount or more has been spent on the clean-up and subsequent investigations (PwC, 2018). Notably though, the PwC report authors do explain that the vast majority of these businesses perform cyber attack vulnerability risk assessments and operate cybersecurity programs at a higher rate than global companies searching for incidences of cybercrime (PwC, 2018). This means that respondents are investing in methods to enhance their cybersecurity, and higher levels of cybercrime are likely to be detected. This may also partly explain why cybercrime is reported by such surveys as higher in Ireland as compared to global counterparts. That said, such increases in crime are also explained to not only be a reflection of better detection methods, but also because more cybercrime is in fact being conducted (PwC, 2018). Notably, there seems to be variation elsewhere where for example the UK CSEW saw a 13 per cent decrease in computer misuse offences between 2017 and 2018 (although these statistics apparently remain experimental). In 2016, six out of ten businesses in Ireland were expected to be the victim of cybercrime throughout the following year (O'Donovan, 2016). In more recent years, the Irish community still expects cybercrime activity to be the most disruptive economic crime from 2018 to 2020 according to PwC (PwC, 2018).

While such industry reports are insightful, they cannot possibly portray the true prevalence of cybercrime activities. LEAs like Europol publish strategic threat assessments as well as other online literature, but traditionally security agencies are more likely to be averse to publicly portraying their work. Law enforcement reports from An Garda Síochána that must be submitted to European counterparts could shed some further light on the actual prevalence of cybercrime in Ireland from a law enforcement perspective specifically, albeit recognising that under-reporting and obstacles to successful prosecutions may hinder the ability to establish a complete picture of the actual cybercrime landscape in Ireland. The authors of this report further explored whether the Central Statistics Office (CSO) might also have additional statistics on cybercrime levels. However, such statistics do not seem to be currently available given the lack of classification of crimes as 'cybercrimes'. This will be discussed further in Section Three in relation to the effectiveness of legislation in the context of reporting cybercrime.

The traditional secretive dynamic in relation to security agencies could change going forward, however, where the field of cybersecurity has caused intelligence agencies in other jurisdictions, such as the United Kingdom, to ensure that part of their work is public facing, including by publishing timely and informative material for public consumption. In order to better prepare individuals and businesses in the wake of cyber incidents, British experts are now messaging at home and abroad that the "fear and mystique" often associated with cyber threats and the field of security are not useful for sound public policy, thus signalling a shift in how cybercrime is approached in the United Kingdom through a culture of increasing openness (Hilliard, 2018; see also Renaud 2016 and

Bada and Nurse 2019) – “Fear and mystique has been the enemy of sound public policy” (Cieran Martin, NCSC UK).

The Head of the United Kingdom’s National Cyber Security Centre (NCSC UK) now describes this agency as the most transparent public cybersecurity agency in the world through its release of unprecedented levels of information and its ambitions to continue declassifying much information in a well-managed way (Hilliard, 2018). This approach aims to help the general public to be better prepared by increasing their understanding of the real nature and prevalence of cyber threats. Similarly, EC3 at Europol publishes a reasonable amount of literature for public consumption, including public advisories. These are the types of steps that national law enforcement and policy-makers could take in Ireland in order to more effectively combat modern cybercrime. These are practical steps towards better informing the public and providing tools and advisories to increase their cybersecurity, rather than traditional awareness-raising activities (this report will address the advantages and disadvantages of awareness-raising activities in later sections). Nonetheless, metrics would likely be required to prove the effectiveness of such new steps.

2.3 Current and emerging cybercrime threats in Europe, other developed countries and Ireland

This section provides a broad overview of the dynamic nature and likelihood of contemporary cybercrime threats as well as possible impact on individuals, organisations, and governments with particular emphasis on the Irish context and developed EU Member States. Europol’s European Cyber Crime Centre (EC3) publishes an annual strategic report from an EU law enforcement perspective which provides a helpful working framework. Subsequently, the most significant ongoing and emerging cybercrime trends from law enforcement, industry and intelligence community perspectives include the following threats: (1) Ransomware; (2) Other malware threats; (3) Data breaches and network attacks; (4) Spearphishing; and (5) Attacks against critical infrastructure.[6]

[6] This report does not address ‘hacktivism’ activities.

2.3.1 RANSOMWARE

Ransomware continues to be the key malware threat in both law enforcement and industry reporting, even though LEAs consider that it is beginning to slow (EC3, 2018, p.7-9). Cybersecurity vendors describe ransomware as a “cybercriminal business model” and “one of the most truly ‘NextGen’ threats” since technologically it is supported by a range of attacking tools and techniques as well as anonymisation measures such as cryptocurrencies and mesh networks (Tor/I2P) that have “triggered higher uses of ransomware” (Kaspersky Lab, Reality vs Delusion, 2018). Both law enforcement and industry find that ransomware will continue unabated, having become “a staple attack tool” and very quickly accommodating aspects of other successful malware such as affiliate programmes (where ransomware is developed and distributed for a cut of the ransom payment to cybercriminals who then spread the malware as ‘affiliates’) and crime as-a-service business models (when professional criminals develop advanced tools, “kits” and other packaged services which are then offered for sale or rent to other criminals who are usually less experienced) so that it is more available to all levels of cybercriminal (EC3, 2018, p.26). That said, Symantec finds that there was a drop in ransomware activity in 2018, observing that WannaCry, copycat versions and NotPetya are inflating inflection figures so that if these worms are removed from the statistics, there is a higher drop in infection figures by approximately 52 per cent (Symantec Corporation, Internet Security Threat Report, 2019, p.16; See also Fireeye and Crowdstrike). Notably, NotPetya and Wannacry are now attributed to state and state-sponsored actors, rather than criminals – this new trend of criminal state activity is discussed in more detail below. In short, there is some divergence between reports on the actual level of ransomware.

Even though WannaCry and NotPetya are attributed to state-related activity, both WannaCry and NotPetya exemplify the ability of such ransomware attacks to spread globally at great speed where over 150 countries and 300,000 victims were indiscriminately affected (notably, NotPetya is increasingly described as destructive malware by western sources rather than original descriptors that referred to it as ransomware). In other words, even where the Irish state or its citizens may not be a primary target, such malicious activities can spread in an indiscriminate manner at great speed globally, thus likely affecting Irish interests too. Irish law enforcement and policy-makers will therefore likely need to include these types of scenarios within their future strategic thinking whereby Ireland might not be considered an immediate target but the country can be affected indiscriminately. In the case of WannaCry and NotPetya, key CI in the EU such as health services, telecommunications, transport and manufacturing industries were affected. Critically, victims were impacted indiscriminately in which case strategic assessments that are conducted on the likelihood of a developed country like Ireland being directly targeted by criminal (or state actors conducting crime) must now also take into account the potential for victims to be impacted indiscriminately as a consequence of these types of possible ransomware activities in future (Heinl, Peace and Security in Cyberspace, 2019). In terms of non-state related cybercriminal activity, cybercriminals have earned USD 25 million through other ransomware strains, which further shows a high disparity between the amount of losses to victims compared to actual criminal revenue where some estimates suggest a global loss of over USD 5 billion in 2017 (although overall damages from ransomware attacks can apparently be difficult to quantify) (EC3, 2018, p.16).

More recently, differences are reported between EU Member States where ransomware activities in some states continue to be untargeted and indiscriminate against citizens and businesses whereas other Member States report more customised and professional campaigns (EC3, 2018, p.17). This development reflects the traditional trajectory of maturing cybercrime activities as described earlier in this report. Similarly, a Eurobarometer report found that seven per cent of Irish Internet users were victims of ransomware in 2015 and globally consumers were the majority group of ransomware victims until 2017. Since then, however, the majority of infections have begun to occur in businesses instead - accounting for 81 per cent of all ransomware infections according to some industry reports (BH Consulting, 2015 and Symantec Corporation, 2019, p.16). Other vendors describe this as a prominent change in direction such that “Big Game Hunting” is rising so that a combination of targeted techniques, tactics and procedures are being employed together with ransomware across large organisations to reap larger financial rewards (Crowdstrike, 2019, p.7). This change has apparently also come about on account of a decline in exploit kit activity as a channel for ransomware delivery where the primary distribution method in 2018 was email campaigns since enterprises are apparently more affected by email-based attacks given that email is the main communication tool (Symantec Corporation, 2019, p.16). In addition, more consumers use mobile devices where essential data is often backed up to the cloud and most significant ransomware families still target Windows based computers which means that the likelihood of consumers’ devices becoming infected is declining (Symantec Corporation, 2019, p.16). Cybersecurity vendors also suggest that another factor is their own enhanced ability to fight ransomware through tools such as email protection, behavioural analysis or machine learning (Symantec Corporation, 2019, p.16 and Kaspersky Lab, 2018).

2.3.2 OTHER MALWARE THREATS

The 2018 PwC survey of Irish businesses found that half the respondents were targeted through malware (including ransomware) at higher rates than those seen globally (36 per cent) (PwC, 2018, p.14). The report further finds that Ireland is being especially targeted by cybercriminals. Significant contemporary malware threats to consider include financial malware, mobile malware, Remote Access Trojans (RATs), and cryptomining malware.

There are a number of factors to consider. First, although the financial sector argues that financial malware continues to be a significant threat, less than one quarter of EU Member States' LEAs reported a significant number of cases and industry reporting seems to be focusing less on financial malware (EC3, 2018, p.18). The financial sector is arguably one of the most advanced sectors in tackling cyber threats, which may partly explain such statistics.

A second growing risk is mobile malware aided by the growing use of mobile phones and tablets, where the global number of smartphones by the end of 2016 was already 2.1 billion (EC3, 2018). While ransomware attacks seem to be less successful when used against mobile phone users, cybersecurity vendors note an important gap given that mobiles are now becoming highly integrated into corporate business processes and data flows but not into corporate cybersecurity infrastructures (Kaspersky Lab, 2018, p.4). Kaspersky Lab reports warn of an imminent "burst of attacks against the mobile" given rising geopolitical tensions, the growing popularity of mobile banking and high volumes of sensitive data present on these devices (Kaspersky Lab, 2018, p.4). European LEAs also flag mobile banking as a potential driver for further growth and development of such mobile malware (EC3, 2018, p.26). Notably, it does not seem to be uncommon for some mobile devices to arrive with malware pre-installed at some point in the supply chain beneath the user-controllable operating system layer (Kaspersky Lab, 2018, p.4).

Industry reporting seems to mainly flag Africa, Asia and the United States for much of this mobile malware activity (EC3, 2018, p.18). Regions such as Africa and Asia are commonly known for very high, and growing, use of mobiles/smartphones where many citizens may often prefer such devices or they may be less costly than computers which is an especially pertinent factor in less economically or digitally developed countries (CSO figures provided in the introductory sections of this report point to higher usage of mobile Internet access in Ireland too). Whereas EU LEAs report a different trend in Europe whereby mobile malware has not so far been extensively reported in Europe (EC3, 2018, p.18). An additional explanation for such variance between regions and industry reporting on the prevalence of mobile malware is law enforcements' observation about an ongoing lack of awareness in the general population about how to deal with mobile phone cyber incidents (EC3, 2018, p.18). From a criminal justice perspective, it seems that victims of mobile malware in Europe are more inclined to approach their provider rather than make police reports, and few will report to the police at all (EC3, 2018, p.18). Questions to then consider include how such information is recorded by these companies, and what is in fact done once such a report is made. Nonetheless, EC3 reports still expect mobile malware to be a future threat for individuals and organisations in Europe (EC3, 2018, p.7). This future threat may become even more significant in the Irish context where Irish banks are now directing their customers towards mobile banking and mobile banking authentication methods. Moreover, already low levels of reporting of cybercrime in Ireland are likely to be exacerbated by under-reporting in relation to mobile malware incidents.

The third set of risks to consider include RATs, although this threat seems to be in continuing decline. EU Member States that do report such cases note, however, their use against networks and companies rather than individuals for data theft, extortion, malware dropping, or unauthorised financial transactions (EC3, 2018, p.18). Europol's annual threat assessment finds that while banking Trojans will still be a priority for the financial sector, sophisticated cybercriminals are directing their focus towards business process compromise, targeting payment systems such as the SWIFT network from within a bank's internal networks (EC3, 2018, p.26).

Cryptomining malware is regularly cited as an emerging, and soon to be pervasive, threat by both industry and European law enforcement. Its use is expected to increase and it will likely become a "regular, low risk revenue stream" for cybercriminals – often attractive for reasons such as anonymity and low barriers to entry (Crowdstrike, 2019, p.60; EC3, 2018, p.9; Symantec Corporation, 2019, p.15). This is otherwise known as cryptojacking where cyber criminals run coinminers on victims' devices and use their central processing unit power and Internet/device bandwidth to mine cryptocurrencies without their permission, often through legitimate websites. By the end of 2017, 0.22% of the top 100,000 websites had cryptomining scripts, and industry reports highlighted large cryptomining botnets as well as cryptomining malware on SCADA systems (EC3, 2018, p.19). While activity is observed to decline when cryptocurrency values drop significantly, Symantec reports that significant levels of criminal activity sometimes still continue, including with a shift towards targeting businesses (Symantec Corporation, 2019, p.15). The value of Monero dropped by approximately 90 per cent whereas cryptojacking only dropped by nearly 52 per cent in 2018 for example, suggesting that some criminals still find their activity profitable or they are waiting until cryptocurrency values rise again (Symantec Corporation, 2019, p.15).

From a criminal justice perspective, law enforcement notes that while it is not illegal in some cases, cryptomining is still creating additional revenue and thus motivation for criminals to attack legitimate websites to exploit visitors' systems, possibly even breaking a victim's system as a result (EC3, 2018, p.19). Europol reports note that there is also "true cryptomining malware" delivered by a malicious payload like other malware which also uses the infected machines processing power to mine cryptocurrencies such as

Bitcoin (which needs higher processing power) (EC3, 2018, p.19). Notably, law enforcement apparently finds this activity easier to detect, but there were no formal law enforcement reports of any cases in 2018 most likely because of its nature as an emerging threat and questionable legality (EC3, 2018, p.19). While a noteworthy incident did occur in Finland where healthcare systems were severely disrupted, it also seems that damages to victims are broadly speaking difficult to quantify and investigate (EC3, 2018, p.19 - Note that cryptocurrency depositories and any entity with significant amounts of cryptocurrencies is a likely target for cybercriminals). Again, a gap that could be explored is where cryptomining may not be always be illegal but it is used by criminals to create additional revenue and where Europol's EC3 raises concerns about questionable legality and difficulties in investigation which may also be an issue for law enforcement in Ireland.

2.3.3 DATA BREACHES AND NETWORK ATTACKS

The nature and purpose of data breaches and network attacks such as illegal acquisition, destruction or denial of access for financial gain are constantly growing in both scale and significance. Prominent cases in recent years include the British Airways and Marriott breaches, the breach of 87 million Facebook users' records, and the Equifax breach where the sensitive information of over 100 million individuals was stolen. Although the breach of Bulgaria's National Revenue Agency only included four million records (a relatively smaller number given recent cases), personal information of nearly 70 per cent of the country's citizens was exfiltrated (BH Consulting, 2019). In the case of Ireland, many services provided by the State rely to some extent on ICT systems such as a wide range of databases with personal data of millions of citizens and business data of companies operating in the State (Department of Communications, Energy & Natural Resources, 2015-2017, p.6). Europol reports note the risk of illegal acquisition of data following such data breaches, where criminals often use this data to facilitate other criminal activity, while industry cites personal, payment and medical data as the most commonly compromised (EC3, 2018, p.7). Of those incidents reported to European law enforcement, it seems that the most common motive is illegal acquisition of data with a view to using it for several reasons that are dependent on the nature of the data (EC3, 2018, p.22). Criminals may use such data to extort victims to prevent data disclosure (including intellectual property), or the data may be used for other fraudulent activity such as phishing (EC3, 2018, p.22). That said, law enforcement reports concede that the ultimate destination of this data is often not known (EC3, 2018, p.22).

United States' intelligence community assessments indicate that non-state actors like transnational criminals and terrorist groups will attempt to access classified information to support their objectives, and they will use cyber means to perform their illicit activities

(Director of National Intelligence, 2019; see also Grabosky (2017)). A recent related threat includes a criminal's goals to gain access (and/or control) to internal systems and processes to conduct other criminal activity (EC3, 2018, p.22). For example, access to internal email systems to conduct Business Email Compromise (also known as CEO fraud) or control systems to access payment platforms like SWIFT (EC3, 2018, p.22). Notably, motives may range from causing malicious damage (including to critical data) to gaining access to infrastructure in order to sell servers on criminal markets (EC3, 2018, p.22). Nearly a third of such breaches involve internal actors, organised criminal gangs carry out approximately 50 per cent of such activities and 12 per cent is conducted by state sponsored actors (EC3, 2018, p.22).

To date, the financial sector has been perceived as the most targeted sector whereas now it is healthcare organisations. Fifty eight per cent of victims are small businesses (EC3, 2018, p.22). The financial sector is arguably now one of the most advanced sectors at combatting malevolent cyber-related activity. Financially motivated cybercriminals are thus likely to focus their efforts on less cyber secure sectors. This currently includes the healthcare sector, which is an attractive target for cybercrime for two main reasons: it is a rich source of valuable data and its defences are weak given the poor security of healthcare data and devices as well as historically poor cybersecurity practices (Coventry and Branley, 2018). Other vulnerable industries that are becoming more attractive to criminals are smart/IoT initiatives such as future smart buildings/smart cities.

Distributed Denial of Service (DDoS) attacks are not always financially motivated, yet the financial sector and LEAs report DDoS as one of the top threats that is growing in scale given that it is becoming more accessible, low cost and low risk (EC3, 2018, p.7). From a criminal justice perspective, some argue that the increasing availability of services and key capabilities online is contributing to this trend, including access for unskilled individuals, allowing them to bring about "crippling" attacks (EC3, 2018, p.24). Similarly, although website defacement is low impact it is still flagged as a continuing problem, often aided by publicly available tools and there is a risk that such attacks may be a stepping stone towards becoming involved in other serious cybercrime (EC3, 2018, p.25).

There are worries about a future DDoS "Internet breaking" attack at the same scale or higher as the Mirai botnet which was effectively DDoS attacks caused by botnets of compromised Internet of Things (IoT) devices (EC3, 2018, p.24). Given the very high levels of attention on these Mirai attacks, it is likely that financially motivated criminals will not want to risk similar law enforcement and intelligence attention (EC3, 2018, p.24). A key lesson from the Mirai case is highlighted by how the potential for such an attack to occur was already known. On many occasions, the possibility of such cyber risks are already foreseen and written about by academia, the intelligence community, LEAs or the private sector, but little is done to prevent their occurrence in the meantime – 2016 ‘finally saw the emergence of a threat which had been predicted’ since 2014 whereby DDoS attacks originate from botnets of compromised Internet of Things (IoT) devices (EC3, 2018, p.24).[7]

2.3.4 PREFERENCES FOR SPEARPHISHING

Although spearphishing is not a new tool, law enforcement and industry both note the risk of criminals’ current preference for consistently successful methods of infection, including email based spam, phishing and targeted spearphishing, as compared to a decline in the use of exploit kits (Symantec Corporation, 2019, p.17; EC3, 2018, p.20). The 2018 survey of Irish businesses also finds that phishing was the most prominent technique for targeted cyber attacks, followed by malware, and notably more Irish businesses are being targeted through phishing than global numbers – two thirds of Irish respondents were targeted compared to 33 per cent globally (PwC, 2018). Again, the current unreliable nature of measuring cybercrime more generally suggests that caution should be exercised in taking these numbers to mean that Ireland is under greater threat, particularly as the evidence is sometimes derived from actors who may have their own interests.

While phishing is occurring on a very large scale, both law enforcement and industry find that few attempts are in fact successful (EC3, 2018, p.55). Industry flags an expected increase in spearphishing occurring via social media, particularly because of the recent leaks of data from social media platforms like Facebook, Instagram, LinkedIn and Twitter where such data is now available on the market (Kaspersky Lab, Security Bulletin, 2019, p.9; EC3, 2018, p.8). This is an example of an area where concrete awareness raising efforts and tools for the public to pre-empt the potential fallout from such spearphishing via social media could help to reduce future cybercrime using these channels, noting the

[7] Note small scale DDoS for hire services called booting which are predominantly used by young gamers, but whose traffic can have significant disruptive effects on a more localised scale. These services are simple to use and operate via subscription models. The National Crime Agency in the UK has trialled the use of targeted advertising to deter young people getting involved, which Cambridge has produced some evidence about. This threat while on a lesser scale is worth noting based on its potential to disrupt the condensed yet vibrant tech-ecosystem Ireland possesses. See: https://www.repository.cam.ac.uk/handle/1810/297004

limitations associated with awareness-raising endeavours that are discussed later in this report.

2.3.5 ATTACKS AGAINST CRITICAL INFRASTRUCTURE

The former Irish national cybersecurity strategy for the period 2015-2017 recognises the growing awareness of risks posed to CI by cyber operations (Department of Communications, Energy & Natural Resources, 2015-2017, p.7). More recently, the draft consultation document for the second cyber strategy specifies that the increasing centrality of network connected devices to the operations of business and CI means the consequences of cyber-enabled attacks are far more serious than in the past (Department of Communications, Climate Action & Environment, Draft Public Consultation, 2019, p.1). While destructive attacks on CI are generally related to state or politically motivated activities, there are two developments related to CI that have a connection with cybercrime. First, given that there are often high concerns about maintaining CI availability, their systems might not be updated/patched and they are then vulnerable to malware or ransomware, which is a cause for concern where ransomware strains can impact targets indiscriminately. There has, for example, been proof of concept work on ransomware for water filtration plants (Arthur, 2018, p.216).

Second, the United States' intelligence community expects that cybercriminals' actions could increasingly disrupt U.S. CI in the healthcare, financial, government and emergency services sectors as well as threatening its allies' CI (Director of National Intelligence, 2019, p.6 & 18). While not an official military ally of the United States, Ireland works closely with its like-minded American counterparts on numerous security and crime-related matters, and hosts numerous American corporations in the State. Moreover, the United States is a similarly developed and digitally advanced country. Therefore, such threat predictions in relation to expected cybercriminal activity on CI should ideally be taken into account in Irish strategic threat assessments by law enforcement and decision-makers on expected cybercrime activity in the future.

2.4 Other factors with an impact on the evolving cybercrime threat landscape

This section highlights other developments that can have significant impact on the current and expected cybercrime threat landscape, which should ideally be considered by law enforcement and policy-makers involved in the fight against cybercrime. These developments include the following non-exhaustive list:

1. The growing connections between cybercrime and malevolent state activity;
2. IoT/future cities and smart meters;
3. Cloud security;

4. Emerging technologies;
5. Third party vendor risks and supply chain attacks;
6. Wide public and commercial availability of tools and techniques as well as “Darknet” concerns;
7. Poor security cultures;
8. Terrorist-cybercrime nexus; and
9. Pervasive anonymisation tools.

2.4.1 THE GROWING CONNECTIONS BETWEEN CYBERCRIME AND MALEVOLENT STATE ACTIVITY

LEAs are becoming increasingly concerned about the rising volume of public reporting that now attributes global cyber attacks to nation states (EC3, 2018, p.7). From a criminal justice perspective, this means it is becoming more difficult for law enforcement to be clear at the outset of investigations whether they pertain to criminal/non-state or state-sponsored/state activity. Where state actors are involved, it is likely that subsequent investigations will fall outside the remit of law enforcement, and instead fall under national security authorities’ responsibility (EC3, 2018, p.21).

Criminals and state actors are increasingly using similar cyber tools and techniques (EC3, 2018, p.28). In recent times, states are becoming more inclined to resort to malevolent peacetime activities, including the perpetration of cybercrimes, by using cyber tools and techniques to pursue their political and security ambitions. This means that not only are some states using similar tools as criminals in order to avoid detection and obfuscate their activities, but it also means that state capabilities and techniques can potentially be re-used by criminals when they are released into the wild (or leaked/stolen). This is an area where many states, and by extension the Irish State, should work to create mechanisms that address the risks associated with security agency collection of zero-day exploits where it is hoped to reduce cybercrime. For example, WannaCry and NotPetya exemplified the dangers of leaked or stolen tools from U.S. security agencies that reduced collective cybersecurity (see also: Schneier 2017 on the risks of prioritisation of individual nation-state surveillance and other offensive capabilities over collective security which poses a serious threat to everyone). There is thus a question whether regulation or programmes such as vulnerability disclosure programmes are required to address these challenges.

Furthermore, the Irish Department of Communications’ consultation document for the second cyber strategy notes that traditional simplistic typologies of groups of actors such as individuals, criminals and state actors may no longer be as relevant given that some criminal gangs are operating under contract to certain states or lone actors are being organised to act collectively by governments (Department of Communications, Climate Action & Environment, Draft Public Consultation, 2019).

It is not expected that cybercriminals will conduct future attacks of a similar scale to WannaCry or NotPetya (both of which have since been attributed to state actors) because such crime groups generally prefer to avoid high levels of law enforcement and intelligence service attention. Instead, a connection with nation states is expected if such future attacks are to occur (EC3, 2018, p.28). This situation is, however, becoming even more complex where states are increasingly engaging with criminal actors to support their own end goals. There are rising cases of states engaging in cybercrime activities for reasons such as raising financial resources to fund other state activities. Recent examples of this phenomenon include the Lazarus group’s cybercrime activities that are associated with North Korea. The group leveraged U.S. National Security Agency exploits that were leaked by the allegedly Russian Shadow Brokers group (EC3, 2018, p.16). These activities include the Sony Pictures hack, the attack on the international SWIFT banking system targeting the Bangladesh central bank and the Wannacry ransomware that indiscriminately targeted millions of systems globally (Director of National Intelligence, 2019, p.6; Arthur, 2018, p.32).

Cyber-enabled state sponsored theft of intellectual property (IP) is another potential threat for countries like Ireland to consider, especially where there are relatively high levels of R&D and innovation within the State and the country has a reputation as an innovative technology hub. Ireland has especially high levels of foreign direct investment (FDI), which comprises many major American corporations. In particular, the State is host to a significant number of U.S. technology sector corporations. Moreover, Ireland is respected globally for entrepreneurship and a strong culture of innovation. This could mean there is an additional risk that other parts of the economy, including small to medium enterprises and universities, become attractive and vulnerable targets for cyber-enabled IP theft conducted by nefarious state and non-state actors for criminal and other purposes. The security and development of resilience in these sectors and organisations is essential to the security of the State and its economy. The threat posed has prompted Scottish authorities to develop a resilience strategy for each sector to create more solutions tailored to the individual needs of each (Scottish Government. *Cyber Resilience*. Website).

From a criminal justice perspective, countries like the United States have begun to increasingly use criminal indictments for these types of cases that involve state actors or state proxies (including for espionage and election interference). This highlights the increasing move towards criminal justice solutions as a deterrent for the perpetration of cybercrimes by state actors. The United States has partly dealt with states’ cyber-enabled IP theft as a criminal justice matter, notably issuing indictments for five Chinese PLA officers in a landmark case. From a criminal justice perspective, however, there is some disagreement as to whether the current legal framework in the United States does in fact have a deterrent effect on such sovereign states engaged in such state-sponsored cybercrime activity, especially where it does not currently apply extraterritorially (Blinderman and Din, 2017). On the one hand, it is unlikely that such officers would be prosecuted, while on the other hand these proceedings can make life difficult for officers and their families. Nonetheless, other jurisdictions like Ireland should now likely also consider the applicability and effectiveness of their own domestic legal framework for state-sponsored cybercrime in order to examine how such actors could be held accountable, and whether this is an avenue they wish to take.

Lastly, there are growing tendencies of organised crime groups to employ techniques that are traditionally only associated with states such as the use of APTs. There are as a result some definitional debates arising in relation to APTs.

2.4.2 IOT/FUTURE CITIES AND SMART METERS

Security analysts have worried for many years – and continue to worry - that the ever-increasing introduction of the Internet of Things (IoT) is heightening vulnerability to attack. There is a majority view that vendors are connecting devices cheaply without high levels of baked-in security and security-by-design considerations (Arthur, 2018, p.215; European Commission, 2017a; IDC and TXT, 2014). In fact, some analyses find that security levels have worsened since 2003 in some devices such as wifi routers (BH Consulting, 2019). BH Consulting (2019) cites the findings of '"The Cyber Independent Testing Lab" which examined binary hardening features in IoT firmware. It analysed 1,294 products (4,956 versions and 3,333,411 binaries) from 22 vendors between 2003 and 2019. The five-person team concluded security hygiene often worsened over time and found that there were "no positive trends"….this means the average home Wi-Fi router's security has deteriorated since 2003.' Others find that security cameras are the most likely IoT devices to be targeted. With the growing attention on developing so-called smart cities, this risk is expected to worsen with industry warning that IoT botnets should not be underestimated as they keep growing stronger (Symantec Corporation, 2018; Kaspersky Lab, 2019). Smart meters are also considered to be a significant new cyber vulnerability whereby modern economies will likely collapse without electricity, or they may be exploited to exert more powerful DDoS attacks and theft of information.

2.4.3 CLOUD SECURITY

Cloud security presents several security challenges such as misconfiguration issues, vulnerabilities in hardware chips and poorly secured cloud databases. Symantec finds one key lesson drawn from recent incidents is the level of poor configuration enabling these incidents (Symantec Corporation, Internet Security Threat Report, 2019, p.19).

Additional work has been developed by Wall and others interrogating the ways in which these technologies transform or enhance threats.

2.4.4 RISING VULNERABILITY AND CRIMINAL MISUSE OF EMERGING OR DISRUPTIVE TECHNOLOGIES

Emerging technologies such as blockchain, AI/machine learning, quantum and 5G networks will not only continue to increase the potential attack surface for cybercriminals, but they will also present another opportunity for criminals to leverage these technologies for their own malevolent purposes. There are already examples of criminal use of machine learning to improve the effectiveness of phishing (Kaspersky Lab, 2019). Notably, quantum computing advances may mean sensitive information encrypted with today's algorithms will be at "greatly increased risk of decryption", thus challenging current methods of protecting data and transactions (Director of National Intelligence, 2019, p.16). LEA reports often note that crime groups are constantly evolving their modus operandi and often creatively adopt key technologies at better speed than law enforcement and cumbersome government agencies which must often out of necessity operate in a more bureaucratic manner. Note, however, that academics view this thinking as still an abstract concept.

In the case of machine learning/AI systems, current concerns surround their inability to explain decisions that are generated so that outputs cannot be predicted (unlike current systems that are reliant on code and rules). This means that if such systems are deployed in homes, smartphones, and autonomous vehicles, it is not yet clear how susceptible they are to unexpected inputs (such as from cybercriminals) and what outputs that could produce (Arthur, 2018, p.220-221; Symantec Corporation, 2018). Cybercriminals will likely also use such AI/machine learning systems and techniques to support their criminal activities. This could include, for example, using automated systems powered by AI to probe networks and systems searching for undiscovered vulnerabilities to be exploited (Symantec Corporation, 2018). Alternatively, social engineering and phishing could be facilitated through sophisticated video/audio/emails (Symantec Corporation, 2018). These are examples of the types of areas where those officials tasked with combatting cybercrime must equally turn their attention.

2.4.5 THIRD PARTY VENDOR RISKS AND SUPPLY CHAIN ATTACKS ARE EXPECTED TO GROW IN FREQUENCY AND IMPACT

The software supply chain is an increasingly attractive target where attackers implant malware into legitimate software packages during production at the vendor or at a third party supplier (hardware supply chain infections are a future possibility) (Symantec Corporation, 2018). In this case, supply chain attacks exploit third party services and software to compromise a final target and they may take several forms, including hijacking software updates or injecting malicious code into legitimate software (Symantec Corporation, 2019, p.17). This means developers continue to be exploited (Symantec Corporation, Internet Security Threat Report, 2019, p.17).

Supply chain attacks are thus likely to continue, and industry considers third party vendors to be a particularly concerning vector of attack, especially on foot of several well-publicised exploitations such as the British Airways and Marriott breaches. There is already concern that these devices rely on software provided by relatively small numbers of vendors which only adds further risk because an identified vulnerability can be used to rapidly compromise the data or systems of millions of people, globally (Department of Communications, Climate Action & Environment, Draft Public Consultation, 2019). Consequently, organisations are now analysing (or should analyse) the number and security of their third party vendors and suppliers, particularly where this is now perceived to be a good vector for maliciously targeting a whole industry (or even a whole country). It seems that these vectors are less useful for targeted attacks though because the risk of detection is higher (Kaspersky Lab, 2019, p.11).

2.4.6 WIDE PUBLIC AND COMMERCIAL AVAILABILITY OF TOOLS AND TECHNIQUES AS WELL AS "DARKNET" CONCERNS

Industry, law enforcement and intelligence communities emphasise their ongoing concerns about the growing availability and use of publicly and commercially available cyber tools, exacerbated by the leaking and release of states' tools and techniques. This situation is increasing the volume of unattributed cyber activity globally as well as the ability to successfully attribute responsibility to non-state criminals or state actors (Director of National Intelligence, 2019, p.7; Kaspersky Lab, 2019, p.7). According to some firms, the entry barrier for criminals has never been so low, with many effective tools, re-engineered leaked exploits (in other words, exploits that have been leaked or stolen can then be re-engineered by criminals for their own nefarious purposes) and frameworks publicly available for use or customisation (Kaspersky Lab, 2019, p.7).

This situation further underpins the trend described above towards simplification of development and attack methods employed by cybercriminals. This is described by various industry reports as "living off the land" tradecraft whereby criminals are increasingly using legitimate and off-the-shelf tools or techniques – in fact, some groups are only using publicly available tools (Crowdstrike, 2019, p.12; Symantec Corporation, 2019, p.17). Even "script kiddies" can obtain access to more advanced malware and some techniques previously considered the prerogative of targeted attackers are increasingly used for mass infection campaigns (Kaspersky Lab, 2018, p.2).[8] The prevalence of cybercrime is only exacerbated by the release of such malware or tools into the wild since they remain active for other groups' use.

Illicit online criminal markets on the "surface web" and the so-called Darknet/dark web are further facilitating criminals who sell such illicit cybercrime toolkits to engage in criminal activity or to avoid surface net traceability (note that cryptocurrencies also enable such exchanges on the Darknet.) (European Commission, 2017a). Given that criminal activities in cyberspace are increasingly facilitated by these black markets, their existence is harming the information security environment and a better understanding of how these markets operate can help to lay the groundwork for options to minimise their harmful influence (Ablon, Libicki and Golay, 2014). Compromised personal, medical and financial data, which is often key for undertaking cyber-dependent crime, is also available on the Darknet (EC3, 2018, p.49).[9] For example, AlphaBay, which has now been shut down, had listings for malware and computer hacking tools. Although some of the largest such markets were shut down by coordinated international law enforcement efforts in 2017, criminals have since migrated to other markets or platforms like encrypted communication apps (EC3, 2018, p.8 & 46).[10] By way of example, the online service provided through webstresser.org which allowed users to hire others to launch sophisticated DDoS attacks was recently taken down through an international operation led by Dutch police and the United Kingdom's National Crime Agency – the site was apparently responsible for over four million cyber incidents, including many on Irish-based websites and coordinated attacks on Irish government websites in 2016 (Gallagher, 2019). Cyber criminals operating at the "high end of high risk" do not frequently use the dark web, operating instead with established criminal communities outside the Darknet (EC3, 2018, p.48). It is expected that smaller markets which cater to different nationalities and language groups will grow as well as use of encrypted communications apps, thus hindering coordinated international law enforcement detection (EC3, 2018, p.50).

[8] Script kiddies are individuals using existing computer scripts or codes to hack into computers, or may lack the expertise to write their own.

[9] See Hutchings and colleagues for more information on this point and how they are developing methods to study it:
https://www.repository.cam.ac.uk/handle/1810/276060

[10] Note there is additional literature on the effectiveness of such LE take-downs.

Nevertheless, even though law enforcement noted the significant growth in the volume of tools and services related to cyber-dependent crime on Darknet markets in 2017, these recent high profile take downs of major markets means that it may now be more difficult to clarify these numbers and more research is needed (EC3, 2018, p.48).[11]

2.4.7 THE 'HUMAN FACTOR' AND 'SECURITY CULTURE'

A common message found traditionally throughout the literature is that the continuing inertia in relation to security and updates means that most software failures or data breaches are not always inevitable. Variance in cybercrime levels can be a reflection of poorly protected victims and a lack of security culture, especially where criminals specifically target such groups and countries with insufficient cyber resilience. Cybercriminals will use simplistic methods, including targeting victims with poor cybersecurity protections. A 2019 report commissioned by Microsoft on large organisations in Ireland finds that employees are still the weak link in the security system, with poor habits and cyber hygiene that potentially put their organisations at risk (O'Brien, 2019). The report explains that a lack of security training, poor password management, the use of personal devices with work-related data and legacy technology and devices are examples of security risks facing public and private sector organisations, including potential violations of the EU General Data Protection Regulation.[12]

This 2019 report partly shows that little has changed in terms of poor security practices among Irish people since a 2015 Eurobarometer survey then found similarly poor cyber hygiene practices such as poor password management (Amárach Research, Commissioned by Microsoft, 2019). Identified emerging security risks include the increasing tendency for the "boundaries between home and work lives and devices" to blur (Amárach Research, Commissioned by Microsoft, 2019). According to this report, people rather than software or hardware, are the weakest link when combatting cyber-related threats (Amárach Research, Commissioned by Microsoft, 2019, p.13).

[11] Some academics note the benefits to these technologies and that they are not solely connected with criminal activity – they serve important functions in journalism for example. Equally, these systems have had to evolve complex mechanisms for developing trust in suppliers and market places – which have helped improve the quality of products consumers receive. It is these trust mechanisms that might be leveraged and undermined in larger online black data markets to help limit accessibility to these kinds of goods (see https://www.cambridge.org/core/journals/european-journal-of-sociology-archives-europeennes-de-sociologie/article/honour-among-cyberthieves/4B1CBA1B4F8AFC05FC7CD2BD8E44EFE7).

[12] Note the distinction between the organisational contexts where policies can be enforced and or technical controls established.

This is one of the reasons why cybersecurity agencies like the NCSC in the United Kingdom are working to publicly communicate the risks and their likelihood so that there is a better level of security awareness and basic protections on an individual and entity level, thus enabling individuals to be better empowered to act on the information they are given in ways that they could not previously (Hilliard, 2018). Those responsible for the fight against cybercrime in Ireland should ideally begin to consider similar good practices.

2.4.8 TERRORIST-CYBERCRIME NEXUS

It is currently expected that terrorists could obtain and disclose compromising or personally identifiable information through cyber activities and they may use this information to coerce, extort, or to inspire and enable physical attacks. There are also expectations that terrorist groups could cause some lower-end disruptive effects such as website defacement or execute DoS against poorly protected networks (Director of National Intelligence, 2019. P.6). Whereas Europol's threat assessment observes that Islamic State (IS) sympathisers have shown their willingness to buy offensive cyber tools and services from the digital underground, their own internal capability, tools and techniques appear to remain limited (EC3, 2019, p.10). It seems that such groups continue to rent botnets for DDoS attacks rather than develop their own malicious cyber capabilities, even though IS sympathisers apparently stay informed of latest technological developments and the crime-as-a-service business model provides other opportunities (EC3, 2019, p.52). Sympathisers have already carried out a small number of defacements and low level hacks, including of a Swedish radio station (EC3, 2019, p.52). Terror-related groups may also pursue ways to secure support and funding through the use of online networks, enabled through new tools such as cryptocurrency.

2.4.9 PERVASIVE ANONYMISATION TOOLS BECOMING AVAILABLE TO CRIMINALS

Increased anonymity is enabling more cybercriminal activity - triggering, for example, recent waves of ransomware attacks (European Commission, 2017a). Such anonymity is now available for reasons that include the rise of Bitcoin and other cryptocurrencies allowing untraceable payments, as well as Tor-like networks ('Tor' is short for 'The Onion Router' which is an open source privacy network that permits users to browse the web anonymously) and encryption technologies enabling criminals' communication and trade (Kaspersky Lab, 2018, p.1-2).

While these developments are challenging for law enforcement efforts, academic sources argue that there is insufficient evidence to show the true extent of the problem (Walden, 2018). These sources counter-argue the literature that states the use of encryption represents a fundamental and irreversible shift in the balance of power between criminals and law enforcement from what previously prevailed. This is therefore a gap which requires further analysis in the Irish context. This is particularly the case since there is much debate over calls for banning public use of encryption or for back doors to be inserted and the associated implications for privacy, security and resilience.

Section 3: Legislative good practices: What relevant legislation is in place to combat cybercrime and how effective has this been?

3.1 Introduction

Appropriate and up-to-date legislation is required to fully respond to the threats posed by modern cybercrime activity, as identified in the previous section. In the recent past, extensive legislation has been lacking in Ireland, but positive advances have since been achieved. This section identifies the relevant legislation in place to combat cybercrime in Ireland, including a brief assessment on its effectiveness. It initially outlines applicable legislation to cybercrime in the Irish context in a largely descriptive manner, including relevant EU and international instruments. This section then examines how effective such legislation has so far been in combatting cybercrime in terms of prevention, prosecutions, convictions or other measures.

3.2 Irish legislation relevant to cybercrime

Ireland's first National Cyber Security Strategy (2015-2017), which was published in 2015, set out how the Irish government would ensure the security of the country's computer networks and associated infrastructure. It was updated in 2019. Best practices identified in the 2019-2024 strategy will be discussed in more detail in the next section. Key measures related to legislation within that first strategy (2015-2017) included introducing primary legislation to formalise arrangements in law and to comply with EU requirements on capabilities, cooperation and reporting. In this context, the key piece of legislation relevant to cybercrime in Ireland is the Criminal Justice (Offences relating to Information Systems) Act of 2017. This Act amended the Criminal Damage Act 1991, the Bail Act 1997 and the Criminal Justice Act 2011, whilst also giving effect to certain provisions of the EU Directive 2013/40/EU on attacks against information systems. The Criminal Justice (Offences relating to Information Systems) Act 2017 also supplements the offence of "unlawful use of a computer" under the Criminal Justice (Theft and Fraud Offences) Act 2001 - an act not specifically designed to address online crime (Slevin & O'Reilly, 2017). Prior to the enactment of the Criminal Justice (Offences relating to Information Systems) Act 2017, computer crime related offences were handled by the Criminal Damage Act 1991, and Section 9 of the Criminal Justice (Theft and Fraud) Offences Act 2001. McIntyre (2005) highlighted that the Criminal Damage Act 1991 was not initially designed to encompass computer crime, but the inclusion of same was part of a later draft of the Act.

The Criminal Justice (Offences relating to Information Systems) Act 2017 alleviates the ambiguity of previous legislation, whilst also creating new offences for digital acts.

Key provisions of the Criminal Justice (Offences relating to Information Systems) Act 2017 are laid out in detail in Table 2 below.

Table 2

Section 2	A person who, without lawful authority or reasonable excuse, intentionally accesses an information system by infringing a security measure shall be guilty of an offence.
Section 3	A person who, without lawful authority, intentionally hinders or interrupts the functioning of an information system by— (a) inputting data on the system, (b) transmitting, damaging, deleting, altering or suppressing, or causing the deterioration of, data on the system, or (c) rendering data on the system inaccessible, shall be guilty of an offence.
Section 4	A person who, without lawful authority, intentionally deletes, damages, alters or suppresses, or renders inaccessible, or causes the deterioration of, data on an information system shall be guilty of an offence.
Section 5	A person who, without lawful authority, intentionally intercepts any transmission (other than a public transmission) of data to, from or within an information system (including any electromagnetic emission from such an information system carrying such data), shall be guilty of an offence.
Section 6	A person who, without lawful authority, intentionally produces, sells, procures for use, imports, distributes, or otherwise makes available, for the purpose of the commission of an offence under section 2 , 3 , 4 or 5 — (a) any computer programme that is primarily designed or adapted for use in connection with the commission of such an offence, or

	(b) any device, computer password, unencryption key or code, or access code, or similar data, by which an information system is capable of being accessed, shall be guilty of an offence.
Section 10	[a] person may be tried in the State for a relevant offence in relation to an act, to which this subsection applies by virtue of subsection (2), committed, whether in whole or in part— (a) by the person in the State in relation to an information system outside the State, (b) by the person outside the State in relation to an information system in the State, or (c) by the person outside the State in relation to an information system outside the State if— (i) that person is a person to whom this subparagraph applies by virtue of subsection (3), and (ii) the act is an offence under the law of the place where the act was committed. (2) Subsection (1) applies to an act which, if it had been committed by a person in the State in relation to an information system in the State, would constitute a relevant offence. (3) Subsection (1)(c)(i) applies to each of the following persons: (a) an Irish citizen; (b) a person ordinarily resident in the State; (c) a body corporate established under the law of the State; (d) a company formed and registered under the Companies Act 2014; (e) an existing company within the meaning of the Companies Act 2014.

An interesting aspect of the Criminal Justice (Offences relating to Information Systems) Act is that the above sections have certain “extra-territorial effect”. This means that they can be applied not only to a person carrying out such activities within Ireland, but also to a person located outside Ireland who is accessing data/damaging digital property within Ireland, provided that such activities are an offence in that jurisdiction. This authority is provided in Section 10 of the Act. The legislation can also be applied to information systems outside the State. Those persons who can be prosecuted under this section is set out in subsection 3 of the Act described below.

Although this is a comprehensive Act, which provides much needed updates to legislation in this area, the Act should not be viewed in isolation. The Criminal Justice Act 2011 is also relevant, because it provides An Garda Síochána with more extensive powers to investigate and prosecute complex cases, often referred to as white collar crime/fraud cases, which includes cybercrime. Section 15 of the 2011 Act states that "for the purposes of the investigation of a relevant offence, a member of the Garda Síochána may apply to a judge of the District Court for an order under this section in relation to—

> (a) the making available by a person of any particular documents or documents of a particular description, or
>
> (b) the provision by a person of particular information by answering questions or making a statement containing the information, or both".

These additional powers are important in investigating cybercrime, since cybercrime is considered to be a complex crime and falls, in general, under this Act.

While the 2017 Act is welcomed, it does have its limitations. For one, scholars argue that the Act does not provide for the offence of Phishing. Phishing is not a specific offence in Ireland, per se (Harnett & Timon, 2018). However, such activities may be an offence under other legislation, depending on the specifics of the case. A representative from An Garda Síochána noted that such cases could be dealt with as a form of deception (Representative from An Garda Síochána, Interview, January 2020). Alternatively, activities related to identity theft or identity fraud that involve actions conducive to phishing may be covered under Section 6 of the Criminal Justice (Theft and Fraud Offences) Act 2001, which make it an offence of "making a gain or causing a loss by deception". It is worth noting that identity theft and identify fraud can be viewed as an aggravating factor when it comes to sentencing in relation to denial of service attacks and infection of IT systems offences, under Section 8 of the Criminal Justice (Offences relating to Information Systems) Act 2017. Section 25, 26 and 27 of the Criminal Justice (Theft and Fraud Offences) Act 2001 also provide for specific forgery offences, which may be appropriate in the area of cybercrime too, depending on the specifics of the case. The 2013 EU Directive on attacks against information systems further notes that setting up effective measures against identity theft and other identity related offences is another important part of an integrated approach against cybercrime (EU Directive 2013/40/EU (14)).

As noted by a representative of An Garda Síochána, while the 2017 Act is welcomed, the codification of cybercrime still remains scattered across many Acts (Interview, 2020). For example, the Offences against the State (Amendment) Act 1998 is pertinent in this cybercrime area. Section 8 states that it "shall be an offence for a person to collect, record or possess information which is of such a nature that it is likely to be useful in the commission by members of any unlawful organisation of serious offences generally or any particular kind of serious offence". Harnett & Timon (2018) suggest that any of the offences under the Criminal Justice (Offences relating to Information Systems) Act 2017 would constitute a serious offence for the purpose of Section 8 – in other words, cybercriminal activities against the State.

Despite the limitations of the Criminal Justice (Offences relating to Information Systems) Act 2017, it is positive that Ireland now has a dedicated law relating to cybercrime and that the powers of investigation for An Garda Síochána have been enhanced under the Criminal Justice Act 2011. However, given the fast pace and changing nature of cybercrime, legislation is likely to become outdated quickly, if not updated in a timely manner (Slevin & O'Reilly, 2017). The 2017 Act does not seem to provide for this inevitability, through for example technology neutral provisions, which may need to be addressed in future.

A good example is provided in the threat section above (Section 2) where from a criminal justice perspective, law enforcement notes that while 'cryptomining' is not illegal in some cases, it is still creating additional revenue and thus motivation for criminals to attack legitimate websites to exploit visitors' systems, possibly even breaking a victim's system as a result (EC3, 2018, p.19). Europol reports note that there is also "true cryptomining malware" delivered by a malicious payload like other malware which also uses the infected machines processing power to mine cryptocurrencies such as Bitcoin (which needs higher processing power) (EC3, 2018, p.19). Notably, law enforcement apparently finds this activity easier to detect, but there were no formal law enforcement reports of any cases in 2018 most likely because of its nature as an emerging threat and questionable legality (EC3, 2018, p.19). While a noteworthy incident did occur in Finland where healthcare systems were severely disrupted, it also seems that damages to victims are broadly speaking difficult to quantify and investigate (EC3, 2018, p.19 - Note that cryptocurrency depositories and any entity with significant amounts of cryptocurrencies is a likely target for cybercriminals). Again, this is a gap which must be addressed in the near future by legislators and law enforcement in Ireland.

Professor Wall, Professor of Criminology at the Centre for Criminal Justice Studies in the School of Law, University of Leeds also gave an example of how law enforcement can proceed in the absence of specifically designed legislation, purporting that law enforcement need to be more imaginative in how they apply existing legislation. Using the example of ‘crypto jacking’ to illustrate his point, Professor Wall stated that some countries do not have specific legislation to prosecute such cases, but one may be able to use old legislation relating to illegal abstraction of electricity, if available to prosecute such cases (D. Wall, interview, December 2019).

While the existence of effective legislation is desirable, it is not always feasible to have legislation in place to meet the changing face of cybercrimes. A representative from the UK’s National Crime Agency noted that it is difficult or impossible to keep pace legislatively with the pace of technological change (National Crime Agency, interview, December 2019). A representative from Europol echoed this and tried to provide some insights into why this is case. He noted that the lengthy process involved in legislative change is often for good reason. Legislation will be around for a long time, so it needs to be well thought out and debated. In order to prevent the need for regular legislative review and updates of the instruments, they should further be developed as technology-neutral as possible. Europol try to inform this process at the EU level, while not creating legislation, they are often consulted by the European Commission, the Council of the European Union and the European Parliament in relation to proposed legislation that might impact Europol’s work and the work of the law enforcement authorities combating cybercrimes within the Member States. Europol, in coordination with EU law enforcement partners and sometimes private sector partners, gives their opinion, informed by the casework, on the potential impact of the proposed legislation from the ground. An example relates to E-privacy Regulation where Europol identified potential problems with early drafts from an investigative but also broader cybersecurity perspective. Providing input at this early stage can help to address or remove the potential for issues that may hamper investigations after implementation (Europol representative, interview, December 2019). It is also worth noting that Europol works with law enforcement partners and the private sector to establish suitable agreement and agreed practices in the context of their Advisory Groups and through non-binding, strategic memorandums of understanding (MOUs) in order to inform and try to improve consistency prior to the implementation of legislation (Europol representative, interview, December 2019).

The fast pace of change, should also not be viewed as a reason to rush legislative change either. As noted by a representative from Europol, legislative change is a lengthy process for good reason. Changes, although perceived to be in the best interest may have negative impacts. For example, in Scotland the police had intended to roll out 41 ‘cyber-kiosks’ or laptop-sized machines which would allow them to bypass encryption to quickly read personal data from digital devices such as mobile phones or laptops (The Scottish Parliament website, 2019). However, in April 2019, members of the Scottish

Parliament's Justice Sub-Committee on Policing asked the police to stop the deployment of the cyber-kiosks until greater clarity was achieved as to the legal framework underpinning their use. It was noted that during the trials "police in Edinburgh and Stirling searched the mobile phones of suspects, witnesses and victims without undertaking the required governance, scrutiny and impact assessments [and that] members of the public whose phones were seized and searched were not made aware that their phones were to be searched using cyber kiosks as part of a trial, the implications of this, and were not provided with the option of giving their consent" (The Scottish Parliament website, 2019). The sub-committee stated that it "fully supports Police Scotland's ambition to transform to effectively tackle digital crime. However, prior to the introduction of any new technology to be used for policing purposes, an assessment of both the benefits and the risks should have been carried out" (The Scottish Parliament website, 2019). Concerns were also noted that the technology was used without consideration of human rights, equality, data protection and that there had been no public information campaign (The Scottish Parliament website, 2019). Many of these issues will be discussed further in the next section, but suffice to say, there should be no short cuts for legislative change, especially when such changes have the potential to breach other rights, such as the right to privacy.

More recently, the Law Enforcement Directive (LED), a piece of EU legislation, parallel to the EU General Data Protection Regulation (GDPR), came into effect from May 2018 through transposition at national level. LED deals with the processing of personal data by data controllers for law enforcement purposes, which falls outside the scope of the GDPR.[13] This also illustrates that law enforcement are not above reproach when it comes to the processing of personal data. As an EU Directive, it too requires transposition into Irish law to take effect and this transposition has been achieved through the Data Protection Act 2018, primarily through Part 5 – Processing of Personal Data for Law Enforcement Purposes. The Data Protection Commission is set out under Part 5 of the Act as the independent supervisory authority for the LED (Data Protection Commission website). This coupled with the GDPR illustrates the EU's commitment to protecting personal data. Now that the EU GDPR is fully in effect, with a package of financial penalties for organisations who do not comply, Irish organisations now face severe consequences for data loss or breach, due to a simple human error, a failure of process or falling victim to a cybercriminal (Amárach Research, 2019).

[13] https://www.dataprotection.ie/en/organisations/law-enforcement-directive

Statutory Instrument No. 360 of 2018 signed the EU Directive on security of network and information Systems (NIS Directive, 2016) into Irish law on 18 September 2018. It represents a “significant change in how countries in the EU approach cybersecurity, and involves a shift in approach towards a more formal type of regulatory relationship in certain key industries (NCSC Website, 2020). The Irish National Cyber Security Centre (NCSC) explains that the responsibilities that the NIS Directive places on the State and on businesses are wide ranging. More detail is provided on these changes in a section of the report below.

Given the global nature of the Internet and the need for international law enforcement cooperation to combat cybercrime effectively, Irish legislation should ideally continue to consider global legislative initiatives, and good practices. As a Member State of the EU, Ireland also has a number of compliance obligations like those instruments described above. Moreover, the EU has adopted a rather comprehensive approach to cyber-related matters, with much non-obligatory good practice available to EU Member States which is discussed in Section 4 of this report. The following section provides an overview of the most pertinent legislative initiatives.

3.3 International and EU instruments relevant to the Irish legislative landscape

The Council of Europe Convention on Cybercrime (CETS No. 185) of 2001, often referred to as the Budapest Convention was brought into force in November 2011. It is considered to be the legal framework of reference for combatting cybercrime, including attacks against information systems (Directive 2013/40/EU). The Convention was the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It contains a series of powers and procedures, such as the right to search computer networks and interception. Its main objective, set out in the preamble, is to pursue “a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation” (CETS No. 185, 2001, 2).

A noteworthy aspect of the Convention is that it extends its influence far outside of Europe. As of 5 February 2019, 62 countries are parties to the Convention, which includes 26 EU Member States - Ireland and Sweden excluded (European Commission website, Press Corner page, 2019). However, even though it is an international treaty, many non-EU states have expressed concern that it is broadly speaking a European or Western instrument with reservations for a number of reasons, including their lack of involvement in the initial creation of the treaty, sometimes even confusing the Council of

Europe with EU bodies. Nonetheless, the Convention continues to provide a global legal framework for combatting cybercrime, including attacks against information systems. In this respect, the Convention is important in that it defines a number of different types of crimes that can be committed online. This provides a common frame of reference for its members. The message in the preamble of the Convention signifies keys aspects of what has now become known as best practice in this area. It recognises the inherent benefits of the following;

- Fostering co-operation with the other States parties to this Convention;
- The need to pursue a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation
- Fostering international co-operation;
- Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies;
- Believing that an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters (CETS No. 185, 2001).

The Convention resulted from recognition by signatories that it was necessary “to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international co-operation”. The 2013 EU Directive on attacks against information systems builds on the Convention, and the EU Cybersecurity Strategy of 2017 specifies that the EU continues to see the value of the Budapest Convention. The 2017 strategy explains that due to the borderless nature of the Internet, the framework for international cooperation provided by the Council of Europe Budapest Convention on Cybercrime offers the opportunity amongst a diverse group of countries to use an optimal legal standard for the different national legislation addressing cybercrime (European Commission, Building strong cybersecurity in the EU, 2017).

A possible addition of a protocol to the Convention has been under exploration which could also provide a useful opportunity to address the issue of cross-border access to electronic evidence in an international context (Terms of Reference for the preparation of a draft 2nd Additional Protocol to the Budapest Convention on Cybercrime, T-CY (2017)3, and JOIN/2017/0450 final). Rather than the creation of new international legal instruments for cybercrime issues, the EU calls for all countries to design appropriate national legislation and pursue cooperation within this existing international framework. However, in late 2019, contrary to EU thinking, Russia submitted a proposal for the creation of a new international legal instrument for cybercrime issues by way of a cybercrime treaty proposal to the Third Committee of the United Nations on ‘countering the use of information and communications technologies for criminal purposes’ (UN General Assembly, A/74/401).

The Budapest Convention also recognises the need for cooperation between states and private industry in combatting cybercrime. It further promotes the need for better international police and judicial cooperation in the area of cybercrime, reinforced through the creation of a 24/7 network. The EU Directive similarly requires every signatory to: “designate a point of contact available on a twenty-four hour, seven-days-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence” (Directive 2013/40/EU, 20). However, An Garda Síochána, while acknowledging the positive aspects of having a 24/7 point of contact, also highlighted that this can place a considerable demand on small units, which can be challenging (Representatives from An Garda Síochána, interview, January 2020).

Article 13 of the 2013 EU Directive on attacks against information systems similarly requires that Member States ensure that they have an operational national point of contact for the purposes of exchanging information relating to offences referred to in Articles 3 to 8, and that they make use of the existing network of operational points of contact available 24 hours a day and seven days a week. Member States shall also ensure that they have procedures in place so that for urgent requests for assistance, the competent authority can indicate, within eight hours of receipt, at least whether the request will be answered, and the form and estimated time of such an answer (2013/40/EU Article 13). The Directive also aims to strengthen the importance of networks such as this Council of Europe network as well as the then G8 network. It calls for those points of contact to be in a position to deliver effective assistance thus, for example, facilitating the exchange of relevant information available and the provision of technical advice or legal information for the purpose of investigations or proceedings concerning criminal offences relating to information systems and associated data involving the requesting Member State (2013/40/EU (22)). In order to ensure the smooth operation of the networks, each contact point should have the capacity to communicate with the point of contact of another Member State on an expedited basis with the support, inter alia, of trained and equipped personnel (2013/40/EU (22)).

While Ireland became a signatory to the Convention in February 2002, as of 5 February 2019, the Irish government has yet to ratify the Convention (European Commission, 2019b). The EU Directive on attacks against information systems, which is a key instrument of the EU and builds on the Budapest Convention, provides that all EU Member States should complete ratification of the Convention as a priority (2013/40/EU (15)). While the majority of the Budapest Convention is already integrated within Irish legislation, at the time of writing a new cybercrime Bill is due to address the remainder of the provisions of the Convention – the Convention is also due to be formally ratified in the near future (Stanton D. T.D., 2019). Representatives from An Garda Síochána noted one specific limitation arising from the lack of ratification which presents an ongoing challenge relates to the lack of legal underpinning to enforce organisations to retain logs that might be required for investigations (Interview, January 2020).

Such EU and international endeavours are relevant to Irish efforts to combat cybercrime for a number of reasons. The safety and security of information systems in the EU is considered to be essential for the development of the internal market as well as a competitive and innovative economy which means that "ensuring an appropriate level of protection of information systems should form part of an effective comprehensive framework of prevention measures accompanying criminal law responses to cybercrime" (Directive 2013/40/EU (2)). Furthermore, it is commonly argued that significant differences in EU Member States' laws and criminal procedures in the area of attacks against information systems may hamper the fight against organised crime and terrorism, and hinder effective police and judicial cooperation in this area (Directive 2013/40/EU (27)). The "transnational and borderless nature of modern information systems means that attacks against such systems have a cross-border dimension, thus underlining the urgent need for further action to approximate criminal law in this area" (2013/40/EU (27)). Academics similarly note that domestic legislation alone is not enough, and cross-border harmonisation of such legislation is important (Picotti & Salvadori, 2008). This can help to reduce and prevent cybercrime havens and it is why transposing the EU NIS Directive is seen to be good practice for example. Given the cross-border dimension of cybercrime, (as a representative from Europol noted) cybercrime is truly an international crime.

ENISA (2013) provides some good practice recommendations in this area in relation to specific offences. For example, ENISA (2013) note that it is good practice to have coherence in relation to the "interpretation of unlawfulness of access attempts: especially in the absence of security measures" (9). It is recommended that it is good practice to have prosecution guidelines to assist both in interpretation and application of the law. The UK have such guidelines within the Crown Prosecution Services, while Portugal have similar guidelines for judges but do not have them for prosecutors (De Myynck, Graux and Robinson, 2013). De Myynck, Graux and Robinson (2013) further note that "collection and dissemination of such guidance at the EU level could also help to ensure homogenous application of the law" across Europe (10). Similar guidelines were suggested in relation to illegal interception (De Myynck, Graux and Robinson, 2013). In relation to the possession of tools for committing offences, ENISA (2013) makes the following recommendation for good practice, "implementing legislation should be clear and explicit, and include clear carve-outs of the applicability of the provision for the normal activities of CERTs, academic institutions, researchers, network operators and security service professionals, and any actions undertaken at the lawful request of businesses, governments and end users" (14).

Nonetheless, the EU Directive has its limitations such as limited definitions for the treatment and storage of investigation data which can result in a lack of consistency on the standards of storage between jurisdictions. In turn, this can result in the inadmissibility of evidence in investigations.

Moreover, while harmonisation of legislation is considered to be essential to effectively combat cross-border cybercrime, successful international cooperation relies on a range of additional factors. These include, but are not limited to, international relations with other countries, the hierarchy of standing of particular offences in different jurisdictions and the willingness or capacity of the police in other states to invest resources in investigations (Yar, 2013). These issues related to the hierarchy of standing of cases and the investment of resources were also highlighted as challenges by a number of interviewees (Representatives from Europol, An Garda Síochána and the NCA, interviews, December 2019 and January 2020), especially when dealing with law enforcement and government organisations outside the EU.

Christou (2016) argues that the EU should do more to support cybersecurity capacity and resilience of developing states, and to engage in more rigorous diplomatic efforts to secure cooperation of states reluctant to engage with cybercrime treaties or conventions. The United Nations Office of Drugs and Crime (UNODC) are particularly active in this area. It has developed the Global Programme on Cybercrime to assist UN Member States in their struggle against cyber-related crimes through capacity building and technical assistance. The main aims of the programme is to "increase efficiency and effectiveness in the investigation, prosecution and adjudication of cybercrime, especially online child sexual exploitation and abuse, within a strong human-rights framework; [to develop] efficient and effective long-term whole-of-government response to cybercrime, including national coordination, data collection and effective legal frameworks, leading to a sustainable response and greater deterrence; [and to] strengthened national and international communication between government, law enforcement and the private sector with increased public knowledge of cybercrime risks” (UNODC Website, 2020a). Moreover, the programme is designed in a manner to respond flexibly to identify needs in developing countries by supporting UN Member States to prevent and combat cybercrime in a holistic manner. The Irish National Cyber Security Strategy (2019-2024) also envisages Ireland having a role in helping improve capacity in developing states with respect to cybercrime. It notes that “[w]e will reinforce Ireland’s diplomatic commitment to cyber security, including by stationing cyber attachés in key diplomatic missions and by engaging in sustainable capacity building in third countries” (Department of Communications, Climate Action and Environment, 2019, p.44). It notes that Ireland will support international cooperation to combat cybercrime and promote formal and informal cooperation in cyberspace, including by engaging in sustainable capacity building in third countries” (Department of Communications, Climate Action and Environment, 2019, p.44).

Significant progress has thus been made at EU level in the field of cybercrime and wider cyber-related questions. While there is now a host of different policy documents and legislative initiatives related to cybersecurity and cybercrime, the NIS Directive and Directive 2013/40/EU on attacks against information systems form the EU’s core policy response so far (European Commission, 2016). An overview of additional key EU documents that specifically pertain to cybercrime are outlined in chronological order within Box 1 below, followed by further detail on each of the instruments (Heinl, 2019c).

Box 1: Overview of key EU documents that specifically pertain to cybercrime[14]

Council Framework Decision 2005/222/JHA on attacks against information systems, 24 February 2005: This Framework Decision is now replaced by the 2013 Directive on attacks against information systems which is discussed in greater detail below.

2008 Report on the Implementation of the 2003 European Security Strategy: This report first mentioned cyber as a potential challenge with an external dimension (most likely because of the incidents in Estonia (2007) and Georgia (2008), allegedly instigated by Russia.

The EU Internal Security Strategy in Action: Five steps towards a more secure Europe, 22 November 2010: Identified cybersecurity as one of five strategic objectives for the period 2010 to 2014.

Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, 7 February 2013: One of the five strategic priorities listed within the first EU Cybersecurity

[14] This is a non-exhaustive overview.

Strategy include combatting cybercrime. These priorities include: (1) Building cyber resilience; (2) Drastically reducing cybercrime; (3) Developing cyber defence policy and capabilities; (4) Developing the industrial and technological resources for cybersecurity; and (5) Establishing a coherent international cyberspace policy for the EU and promoting core EU values.

Directive 2013/40/EU of the European Parliament and of the Council on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, 12 August 2013: More detail provided below.

The European Agenda on Security, 28 April 2015: Prioritises terrorism, organised crime and cybercrime as interlinked areas with a strong cross-border dimension where EU action can make a difference.

Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, 5 July 2016: This policy document outlines the need to enhance cooperation for better preparedness and to deal with cyber incidents. It calls for existing cooperation mechanisms to be strengthened to increase EU resilience and preparedness, including for a possible pan-European cybersecurity crisis. In particular, it notes that these cooperation mechanisms should be comprehensive, spanning the life cycle of an incident from prevention to prosecution. It explains that effective cooperation among Member States and practical implementation of security requirements for critical operators will also demand robust technical solutions from the cybersecurity industry. The document further specifies that knowledge and expertise on cybersecurity is available at EU level but in an unstructured and dispersed way currently. Thus, in order to support NIS cooperation mechanisms, information should be pooled in an 'information hub' to make it easily available on request to all Member States. This 'hub' would become a central resource allowing the EU institutions and Member States to exchange information as appropriate. Easier access to better structured information on cybersecurity risks and potential remedies should help Member States to increase their capacities and align their practices, and thereby enhance overall resilience to attacks. The document includes a number of additional recommendations and suggestions for responses and measures that could be implemented.

Directive 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union ("NIS Directive"), 6 July 2016: More detail is provided in the report below.

Regulation (EU) 2016/794 on Europol, 11 May 2016: More detail is provided in the report below.

Joint Framework on countering hybrid threats: a European Union response, 6 April 2016: This Joint Framework recognises that the range of measures applied as part of a hybrid campaign may be very wide, including cyber attacks on critical information systems.

Cybersecurity package, "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU", 13 September 2017: More detail is provided in the report below.

3.3.1 DIRECTIVE 2013/40/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL ON ATTACKS AGAINST INFORMATION SYSTEMS AND REPLACING COUNCIL FRAMEWORK DECISION 2005/222/JHA, 12 AUGUST 2013

In accordance with Article 3 of the Protocol on the position of the United Kingdom and Ireland in respect of the Area of Freedom, Security and Justice annexed to the Lisbon Treaty (TEU and TFEU), Ireland notified its intent to take part in the application of the EU Directive on attacks against information systems (Directive 2013/40/EU (31)). EU Member States were thus expected to transpose the Directive into national law by 2015 by bringing into force the laws, regulations and administrative provisions needed to comply with the Directive (2013/40/EU (16)).

The 2013 Directive establishes minimum rules on the definition of criminal offences and provides operational measures for cooperation among authorities. It aims to facilitate cross-border cooperation and harmonisation of measures across EU Member States. The objectives of this Directive are to approximate the criminal law of the Member States in the area of attacks against information systems by establishing minimum rules concerning the definition of criminal offences and the relevant sanctions and to improve cooperation between competent authorities, including the police and other specialised law enforcement services of the Member States, as well as the competent specialised Union agencies and bodies, such as Eurojust, Europol and its European Cyber Crime Centre, and the European Network and Information Security Agency (ENISA) (2013/40/EU (1)).

The Directive’s preamble explains that there is evidence of a tendency towards increasingly dangerous and recurrent large-scale attacks conducted against information systems which can often be critical to Member States or to particular functions in the public or private sector. This tendency is accompanied by the development of increasingly sophisticated methods, such as the creation and use of so-called ‘botnets’, which involves several stages of a criminal act, where each stage alone could pose a serious risk to public interests. This Directive aims, inter alia, to introduce criminal penalties for the creation of botnets, namely, the act of establishing remote control over a significant number of computers by infecting them with malicious software through targeted cyber attacks. Once created, the infected network of computers that constitute the botnet can be activated without the computer users’ knowledge in order to launch a large-scale cyber attack, which usually has the capacity to cause serious damage, as referred to in this Directive. Member States may determine what constitutes serious damage according to their national law and practice, such as disrupting system services of significant public importance, or causing major financial cost or loss of personal data or sensitive information (2013/40/EU (5)).

The Directive provides that common definitions are necessary in the area of cybercrime to ensure a consistent approach in the EU Member States to the application of the Directive (2013/40/EU (7)). Moreover, it recognises the need to achieve a common approach to the constituent elements of criminal offences by introducing common offences of illegal access to an information system, illegal system interference, illegal data interference, and illegal interception (2013/40/EU (8)). A detailed outline of each of these common offences is laid out in Articles 3, 4, 5, and 6.

The Directive further indicates that Member States should provide for penalties in respect of attacks against information systems. Those penalties should be effective, proportionate and dissuasive and should include imprisonment and/or fines (2013/40/EU (10)). It provides for criminal penalties at least for cases which are not minor. Member States may determine what constitutes a minor case according to their national law and practice. A case may be considered minor, for example, where the damage caused by the offence and/or the risk to public or private interests, such as to the integrity of a computer system or to computer data, or to the integrity, rights or other interests of a person, is insignificant or is of such a nature that the imposition of a criminal penalty within the legal threshold or the imposition of criminal liability is not necessary (2013/40/EU (11)).

The Directive further notes that more severe penalties should be provided for where an attack against an information system is committed by a criminal organisation as defined in Council Framework Decision 2008/841/JHA where such a cyber attack is conducted on a large scale, which affects a significant number of information systems, including where it is intended to create a botnet or where a cyber attack causes serious damage, including where it is conducted through a botnet. It is also appropriate to provide for more severe penalties where an attack is conducted against a CI of the Member States or of the Union (2013/40/EU (13)).

The Directive is lauded by the 2017 EU Cyber Strategy as a progressive step towards improving the criminal law response to cyber attacks. According to the 2017 Strategy, this Directive has led to substantive progress in criminalising cyber attacks at a comparable level across the Member States, which facilitates the cross-border cooperation of law enforcement authorities investigating these types of offences. However, there is still scope for the Directive to reach its full potential if Member States were to implement all of its provisions fully (COM(2017)474). The Commission will continue to provide support to the Member States in their implementation of the 2013 Directive and at the time of the 2017 Strategy's publication saw no need to propose amendments to it.

3.3.2 DIRECTIVE 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL CONCERNING MEASURES FOR A HIGH COMMON LEVEL OF SECURITY OF NETWORK AND INFORMATION SYSTEMS ACROSS THE UNION ("NIS DIRECTIVE"), 6 JULY 2016

The aim of the NIS Directive is to enhance cybersecurity across the EU by laying down measures with a view to achieving a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market. The NIS directive was published on 6 July 2016. EU Member States were due to transpose the Directive into national law by 9 May 2018 and identify Operators of Essential Services (OES) by 9 November 2018. The Directive provides legal measures to boost the overall level of cybersecurity in the EU. It suggests that

> [B]uilding upon the significant progress within the European Forum of Member States in fostering discussions and exchanges on good policy practices, including the development of principles for European cyber-crisis cooperation, a Cooperation Group, composed of representatives of Member States, the Commission, and the European Union Agency for Network and Information Security ('ENISA'), should be established to support and facilitate strategic cooperation between the Member States regarding the security of network and information systems. For that group to be effective and inclusive, it is essential that all Member States have minimum capabilities and a strategy ensuring a high level of security of network and information systems in their territory. In addition, security and notification requirements should apply to operators of essential services and to digital service providers to promote a culture of risk management and ensure that the most serious incidents are reported (Directive (EU) 2016/1148, 194/1-194/2).

There are number of elements worth noting in the NIS Directive specifically. For example, Chapter II, Article 7, which relates to National strategy on the security of network and information systems. This articles states that

> Each Member State shall adopt a national strategy on the security of network and information systems defining the strategic objectives and appropriate policy and regulatory measures with a view to achieving and maintaining a high level of security of network and information systems (Directive (EU) 2016/1148, 194/15).

Similar to the 24/7 point of contact in respect to the Budapest Convention, Article 8 of the Directive relates to the appointment of national competent authorities and single points of contact. Article 9 relates to the establishment of computer security incident response teams (CSIRTs). It states that "Each Member State shall designate one or more CSIRTs" (Directive (EU) 2016/1148, 194/17). Article 12 relates to the establishment of a CSIRT network. Article 10 relates to cooperation at national level. Chapter III also relates to cooperation, more specifically to the establishment of an EU Cooperation Group to help "and facilitate strategic cooperation and the exchange of information among Member States and to develop trust and confidence" (Directive (EU) 2016/1148, 194/17). Similar to the Budapest Convention Article 13 provides for international cooperation.

Chapter IV relates to security of the network and information systems of operators of essential services. It sets out requirements Member States should ensure are in place in relation to such services. These include security requirements and incident notification (Article 14) as well as implementation and enforcement (Article 15). Chapter V sets out similar requirements in relation to Digital Service Providers (DSPs), requirements relating to security requirements and incident notification (Article 16), implementation and enforcement (Article 17) and jurisdiction and territoriality (Article 18).

The Directive was signed into Irish law on 18 September 2018 by way of Statutory Instrument No. 360 of 2018, mentioned above. The Irish NCSC explains that the responsibilities that the Directive places on the State and on businesses are wide ranging, but, among other things:

- Involve the application of a set of binding security obligations to a wide range of critical infrastructure operators, i.e. OES. These include energy, healthcare, financial services, transport, drinking water supply and digital infrastructure and telecommunications.
- Require the State to apply and police a new regulatory regime on so called DSPs. These include cloud computing providers, search engines providers and providers of online market places.
- Critically, and in a similar manner to that for data protection, the State has responsibility for dealing with the security of services provided by multinational companies across the EU that have their European headquarters located in Ireland. The majority of these multinational companies are from the United States.

The NCSC further explains that in relation to OES, in order to realise the Directive and its objectives, Member States' must identify the OES within its jurisdiction, ensure that such entities have security measures in place and that they report significant incidents. Security Guidelines are now published by NCSC to assist OES in meeting their network and information system security and incident reporting obligations under the Directive (transposed into Irish legislation under Regulations 17 and 18 of S.I. 360 of 2018: European Union (Measures For A High Common Level Of Security Of Network And Information Systems)). They represent a sample approach that can be adopted by OES to manage the risks posed to the security of the network and information systems used in their operations, and to minimise the impact of incidents affecting those systems. They are both technology neutral and non-sector specific to allow OES in different sectors adapt these to meet their needs, and to evolve their sector specific response along with technological advances and business requirements. Draft Security Measures were published for public consultation in January 2019 and the final version can be found on the NCSC website.[15]

In relation to DSPs, companies providing digital services specified in Annex III of the Directive are categorised as Digital Service Providers and are to meet requirements set by the European Commission through the EU legal mechanism known as implementing acts. Incident reporting forms are available for both OES and DSPs on the NCSC website. The strategy on strengthening Europe's cyber resilience system highlights that a key part of national capabilities required by the NIS Directive are CSIRTs responsible for rapid reaction to cyber threats and cyber incidents. They will form the CSIRTs Network to promote effective operational cooperation on specific cybersecurity incidents and sharing information about risks.

3.3.3 REGULATION (EU) 2016/794 ON EUROPOL, 11 MAY 2016

Regulation (EU) 2016/794 on the European Union Agency for Law Enforcement Cooperation (Europol) replaces and repeals Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA. The 'Stockholm programme — An open and secure Europe serving and protecting citizens' calls for Europol to evolve and become a hub for information exchange between the law enforcement authorities of the Member States, a service provider and a platform for law enforcement services. On the basis of an assessment of Europol's functioning, it has previously been recognised that further enhancement of its operational effectiveness is needed to meet that objective (Regulation (EU) 2016/794 (3)).

Article 8 of the Regulation specifies that attacks against information systems affecting Union bodies or two or more Member States are a growing menace in the Union, in particular in view of their speed and impact and the difficulty in identifying their sources. When considering requests by Europol to initiate an investigation into a serious attack of suspected criminal origin against information systems affecting Union bodies or two or more Member States, Member States should respond to Europol without delay, taking into account the fact that the rapidity of the response is a key factor in successfully tackling computer crime (Regulation (EU) 2016/794 Article 8). Article 30 provides that in order to ensure operational effectiveness, Europol should be able to exchange all

[15] (https://www.ncsc.gov.ie/nis/).

relevant information, with the exception of personal data, with other Union bodies, authorities of third countries and international organisations, to the extent necessary for the performance of its tasks. Since companies, firms, business associations, non-governmental organisations and other private parties hold expertise and information of direct relevance to the prevention and combatting of serious crime and terrorism, the Regulation provides that Europol should also be able to exchange such information with private parties. To prevent and combat cybercrime, as related to network and information security incidents, Europol should, pursuant to the NIS Directive, cooperate and exchange information, with the exception of personal data, with national authorities competent for the security of network and information systems.

In short, the NIS Directive is the first EU-wide cybersecurity law. The EU 2017 Cyber Strategy explains that the NIS Directive is designed to build resilience by improving national cybersecurity capabilities; fostering better cooperation between the Member States; and requiring undertakings in important economic sectors to adopt effective risk management practices and to report serious incidents to the national authorities. These obligations also apply to three types of providers of key Internet services: cloud computing, search engines and online marketplaces, as described above. It aims for a stronger and more systematic approach and a better information flow. Full implementation of the Directive is considered essential to EU cyber resilience by increasing harmonisation across the EU, especially in relation to OES.

As part of the 2017 Cybersecurity package, the Commission was also due to issue a Communication to support their efforts by providing best practice from the Member States relevant to the implementation of the Directive and guidance on how the Directive should be operating in practice. The 2017 strategy notes that an area where the Directive will need to be supplemented is information flow. For example, it recognises that the Directive only covers key strategic sectors – but logically a similar approach by all stakeholders hit by cyberattacks would be necessary to have a systematic assessment of vulnerabilities and entry points for cyber attackers.

3.3.4 CYBERSECURITY PACKAGE "RESILIENCE, DETERRENCE AND DEFENCE: BUILDING STRONG CYBERSECURITY FOR THE EU", 13 SEPTEMBER 2017, JOIN/2017/0450 FINAL

The 2017 EU Cybersecurity strategy builds on the review of the 2013 EU Cybersecurity Strategy. The Strategy addresses concepts of deterrence – explaining that effective deterrence means putting in place a framework of measures that are both credible and dissuasive for would-be cyber criminals and attackers. As long as the perpetrators of cyber attacks – both non-state and state – have nothing to fear besides failure, they will have little incentive to stop trying. It argues that a more effective law enforcement response focusing on detection, traceability and prosecution of cyber criminals is central to building effective deterrence.

However, it is worth noting that the extensive research on deterrence and the effectiveness of criminal sanctions, one of the most researched areas of criminology, has shown that the extent to which punitive policies can meaningfully address or impact crime rates is limited (although some deterrent effect is not disputed). The question is rather what kind of punitive measures, and how to establish the certainty of punishment? These are difficult questions to answer in the context of cybercrime, especially cyber-dependent offending, as research in this area is in its infancy, due to factors such as, among others, limited prosecutions, or limited access to offenders. Care should thus be taken in pursuing any increased punitive measures without an investment in research in this area. It is essential that states explore or invest in research on cyber-dependent offenders' movement in and out of offending and what were the conditions that led them to offend to begin with before implementing increased punitive measures. Policing alone will never be enough. Greater consideration of prevention measures that are oriented towards addressing the underlying causes of offending to begin with – and not at 'controlling' through deterrence is required where this latter approach may be a costly and ineffective venture.

3.3.5 ADDITIONAL LEGISLATIVE INITIATIVES

Beyond EU measures among Member States, a number of countries are considering agreements that can surmount the difficulties associated with the Mutual Legal Assistance Treaties that many stakeholders argue are broken so that more efficient channels of data sharing with law enforcement authorities can be facilitated while being mindful of privacy and data protection standards. The passage of the Clarifying Lawful Overseas Use of Data Act or CLOUD Act by U.S. Congress in 2018 has apparently opened diplomatic avenues that could facilitate such a transition. Moreover, a number of third countries such as India are exploring data sharing agreements with the United States along the same lines as the U.S.-UK bilateral agreement following the CLOUD Act.

While deliberations on a UN framework for responsible state behaviour in cyberspace are ongoing, the 2015 UN GGE consensus report notes that States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats as well as consider whether new measures may need to be developed in this respect (7-8). The experts further find that States should take appropriate measures to protect their CI from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures (8).

While there is clearly much legislative progress at EU and national level in Ireland, the existence of legislation, policies and strategies alone is rarely enough. They are redundant if they are not effective. The next section will therefore examine how effective these legislative measures are in the context of combatting cybercrime in terms of prevention, prosecution, convictions or other measures.

3.4 Effectiveness of legislation in combatting cybercrime in terms of prevention, prosecutions, convictions or other measures

Cybercrime presents numerous challenges for traditional criminal law and the criminal justice system in general (Calderoni, 2010). A number of these challenges are highlighted below. They include (1) obstacles associated with unclear definitions; (2) the impact of complex cybercrime on effective detection, investigation and prosecution of cybercrimes by law enforcement; and (3) jurisdiction challenges.

The first challenge, which is already highlighted at the beginning of this report, is the lack of clear and consistent definitions. In respect to legislation, many of the definitions of cybercrime are not conducive to legal interpretation and legislators do not always do a good job at defining terms (Shinder, 2002; See also Clough 2012 for an expanded and internationally situated discussion on this.). Sometimes legislators do not even define key terms, as evident in the Criminal Damage Act 1991, leaving the court to interpret such terms (Chawki, 2005). Many of the terms used within the Criminal Damage Act 1991, such as ‘operate’ and ‘computer’ were not defined, leading Murray (1995) to argue that the Act may be unconstitutionally vague. This issue has been somewhat alleviated by the Criminal Justice (Offences relating to Information Systems) Act 2017 as well as the 2013 EU Directive on attacks against information systems which aims to harmonise definitional understanding across EU Member States to aid cross-border cooperation. However, there are some terms within the Criminal Justice (Offences relating to Information Systems) 2017 Act that remain undefined. For example, the offence of hacking requires the ingredient of ‘reasonable excuse’, yet ‘reasonable excuse’ is not defined in this legislation (Harnett & Timon, 2018). While this may be positive if courts take a broad view, equally it can be significantly limiting if narrow interpretations are taken. By working to more deeply address such legislative vagueness in the Irish legal system, some of the problems identified could be alleviated.

A second challenge relates to the nature of cybercrimes given that they are often complex and can be unfamiliar to those within the criminal justice field. Holt & Bossler (2015), albeit in the context of sex offenders and content-offences, questioned the extent to which forms of offending fit into the services of organisations such as probation and social workers. Similar questions are likely to be relevant in respect to cyber-dependent crime. This can directly impact the ability to effectively implement legislation and criminal justice related responses. Two key elements are required to respond to this challenge. The first relates directly to legislation. Law enforcement require extensive powers to investigate and prosecute complex cases, and legislation needs to provide for this, including by aligning with data protection and privacy rights. In the Irish context, the Criminal Justice Act 2011 provides for these powers, as mentioned above. However, such powers are only effective if properly resourced as highlighted by McIntyre (2015).

The issue of resourcing with An Garda Síochána specifically relating to cybercrime was highlighted in the Future of Policing in Ireland report (2018). It stated “the capacity and expertise of the existing Garda National Cyber Crime Bureau should be substantially expanded as a matter of urgency, and personnel appointments in that field should be fast tracked” (27). It further notes that “An Garda Síochána should further develop its cybercrime and cyber security capabilities, including digital forensics. These should be centrally led, but with response capacity at appropriate geographical locations” (Future of Policing in Ireland report, 2018, 80).

Investigation and prosecution of cybercrimes require well-trained and knowledgeable personnel in the investigation phase, during prosecution, and in courts, coupled with effective legislation. Without significant additional resources provided to An Garda Síochána, an organisation often reported as having limited resources, the ability to take advantage and exercise these additional powers is often limited (Slevin & O’Reilly, 2017).

A third challenge worth highlighting relates to staff and skills retention and upskilling, as highlighted by Whelan and Harkin (2019) and Harkin et al (2018). They identified the challenge for the police to retain staff. They noted that when the police train officers in digital forensics and cybercrime investigation, they tend to experience significant challenges in keeping them in the police, given the opportunities in the private sector. Standardised courses like Certified Information Security Professional (CISP) and other accreditations are expensive and costly to the state, and the police cannot afford to provide such training and then have officers leave. Yet, they find it difficult, if not impossible, to match conditions, pay and opportunities in the private sector.

Whelan and Harkin (2019) and Harkin et al (2018) identified the possibility of bridging this gap with the use of volunteers and partnerships to support skills gaps within the police.

Interestingly, this was also identified as a good practice worth exploring with respect to An Garda Síochána. A representative from An Garda Síochána noted the use of special police officers in the UK who have specific IT skills, and who can be called in as and when they are required (Interview, 2020). Another option may be to work with private sector professionals to back fill the skills gap, but this too is not without its problems. For example, potential clashes between occupational cultures, such as being profit driven, management styles, or levels of innovation to privacy issues, and many more. However, such challenges illustrate that the nature of the work in this area fundamentally challenges the notion of routine police work and police occupational culture.

The reference to digital forensics by the Commission is worth further noting. The volatility of digital evidence is a great challenge in relation to prosecution. Retrieving and ensuring integrity of the evidence requires expertise. Furthermore, the nature of electronic data "requires sophisticated forensic techniques to ensure its retrieval, preservation and validity for use in a criminal trial" (Clough, 2015; 8). As a result, the necessary resources of people, technology and training need to be commensurate with the evolution and advancement of criminality in this area, coupled with regular legislative updates to ensure countries have the necessary authority and skill set to respond to the ever-evolving range of cybercrimes that emerge and to bring evidence to court (Clough, 2011). This rapid pace of change within this sector presents challenges. The use of the cyber-kiosks in Scotland, as discussed above, was implemented as a direct response to this challenge and the process of digital evidence, more generally. As a result, it would be prudent to ensure such developments are made mindful of human rights, transparency, coupled with public consultation and deliberative democracy.

As noted by Brenner & Clarke (2005), cybercrimes often occur in a fraction of a second, and spread with astonishing speed, never mind the fast pace of technological development. Both factors makes it difficult to police and prosecute. As a result, and as mentioned above, this is highly likely to require investment of considerable resources for An Garda Síochána, prosecutors and the courts to ensure they have the capacity necessary to bring cases effectively through the criminal justice system.

In addition, given that better cooperation between law enforcement bodies and judicial authorities across the EU is considered necessary to effectively combat cybercrime, the 2013 EU Directive on attacks against information systems notes that even more adequate training is needed for authorities to enhance their understanding of cybercrime and its impact, and to foster cooperation and the exchange of best practices (2013/40/EU (28)). In particular, such training should be aimed at raising awareness about the different national legal systems, the possible legal and technical challenges of criminal investigations, and the distribution of competences between relevant national authorities

(2013/40/EU (28)). Representatives from An Garda Síochána noted that positive progress was being made in this regard in Ireland. They noted that considerable improvements were noticeable in how the courts in Ireland now deal with cybercrime cases (Interview, 2020). It was stated that court staff had received training and improved their expertise in this area. They also reported that An Garda Síochána and the Director of Public Prosecution office now work closer together to better understand this area. This has been helped by participating in joint training. Coupled with the improved learning of each other's activities, requirements and needs, such opportunities were highlighted as important for building positive relationships between both organisations (Representatives from An Garda Síochána, interview, January 2020).

The 2013 EU Directive on attacks against information systems also provides that the cybercrime investigative capabilities of Member States' law enforcement authorities need to be improved too, as well as the understanding of cyber-enabled crimes and investigative options by prosecutors and the judiciary. Eurojust and Europol contribute to this objective and to enhanced coordination, in close cooperation with specialised advisory groups within EC3 and with the networks of chiefs of cybercrime units and of prosecutors specialised in cybercrime. The Commission has been due to dedicate EUR 10.5 million funding to fight cybercrime, primarily under its Internal Security Fund-Police Programme. Training is an important element and a number of useful materials have been developed by the European Cybercrime Training and Education Group. These should now be widely rolled out for law enforcement professionals with the support of the European Union Agency for Law Enforcement Training (CEPOL).

A fourth challenge relates to jurisdiction. Jurisdiction in the area of cybercrime is described by some experts as having two distinct components, virtual and geographical, both of which present challenges to the effectiveness of legislation. That said, neither are mutually exclusive, given that virtual environments are still embedded in physical infrastructure. Firstly, the virtual nature of many of the environments in which cybercrimes often occur, can result in a direct clash between the "main operational criteria of the criminal justice systems, namely sovereignty and the territoriality principle" (Calderoni, 2010, 3). This requires countries to establish jurisdiction over virtual environments, which often requires specific legislation. The second component, geographical, poses similar problems, given the cross-border dimension of much of this crime. This makes some traditional legislation ineffective. As Clough (2015) notes "criminal law is traditionally regarded as local in nature, being restricted to the territorial jurisdiction in which the offence occurred. Modern computer networks have challenged that paradigm" (p. 8). This negatively impacts the effectiveness of law enforcement and highlights the impediment caused by the lack of harmonisation of legislation, at least in respect to the geographical dimension (Clough, 2015).

In the Irish context, the Criminal Justice (Offences relating to Information Systems) Act 2017, aims to reduce this challenge by ensuring that the legislation provides for "extra-territorial effect" for the sections mentioned above. This means that they can be applied not only to a person carrying out such activities within Ireland, but also to a person located outside Ireland who is accessing data/damaging digital property within Ireland, provided that they have been convicted or acquitted abroad in respect to the same offence and meet the Act's requirements. Clough (2011) notes how important it is that a country's jurisdiction over cybercrime is as wide as possible, to ensure no country or region becomes a 'safe haven' for such activities. However, inconsistency in definitions across jurisdictions can make prosecution outside national boundaries difficult (Chawki, 2005). This is one reason why the EU seeks to harmonise law in this area. The 2013 EU Directive on attacks against information systems does not govern conditions for exercising jurisdiction over any of the offences referred to in the Directive, such as a report by the victim in the place where the offence was committed, a denunciation from the State of the place where the offence was committed, or the non-prosecution of the offender in the place where the offence was committed (2013/40/EU (20)). That said, the Directive does recommend that in the EU the coordination of prosecution of cases of attacks against information systems should be facilitated by the adequate implementation and application of Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflict of jurisdiction in criminal proceedings (2013/40/EU (27)).[16]

These factors all present significant challenges for the criminal justice system, from law enforcement to the courts, whilst also impacting the effectiveness of legislation. The next piece will examine a number of other challenges as they pertain specifically to prevention, prosecution, convictions and other measures.

3.4.1 PREVENTION

Reliance on criminal sanctions should only be one approach to combatting cybercrime. While the best form of defence is often prevention, it is often easier said than done. Furthermore, such a focus is important given the limited amount of research available

[16] Beyond the EU, the operability of legislation can be contingent on the willingness of nation states to engage, along with private companies whose services were used to facilitate the crime.

with regard to the effectiveness of legal instruments, due to the fact that research in this area is in its infancy. That said, research in the area of crime prevention more generally is better researched, the learnings of which may be transferable to the area of cybercrime. A recent publication by Brewer et al (2019), considers how longstanding, traditional crime prevention techniques can be reimagined and applied for an increasingly digital world, and it explores how criminology can apply to the digital realm.

Prevention measures are often achieved through education, training and awareness raising rather than through legislation in order to enhance individual and overall cybersecurity and resilience. This is the case in Ireland at present as there is little in the way of legislation that mandates prevention measures in this area. The UK Government has taken a more proactive approach, starting with Internet companies. The government introduced an Online Harms white paper, which extended responsibilities for companies whose services are used for illegal activity (HM Government, 2019). The white paper recommends that Internet companies that allow “users to share or discover user-generated content or interact with each other” should be held responsible for illegal, harmful, or otherwise disreputable content appearing on their platforms (HM Government, 2019, p11). The white paper states that an independent regulator will create ‘codes of practice’ detailing how companies should best deal with each of those harms. Those who do not comply, will face fines. These fines will be similar to GDPR fines, in that they will be in proportion to their revenues. The paper also goes as far as suggesting that the companies may be taken offline, at least in the UK and their executives might be prosecuted in civil or criminal court (HM Government, 2019). While this does not directly relate to cyber-dependent crimes, it does demonstrate that increased responsibility is being expected of Internet companies.

In a slightly similar vein, the transposition into Irish law of both the NIS Directive and GDPR means that Irish individuals and entities will now be held accountable under Irish legislation for not meeting their compliance obligations. The introduction of such legislative measures may now mean that preventative measures are now more likely to be introduced by organisations, thus driving better resilience in the wake of cybercrimes. It may be too soon to gauge the effectiveness of these new legislative initiatives on prevention.

There is, however, no specific criminal offence in Ireland for failing to implement cybersecurity measures within an organisation or as an individual, at this time. However, Section 71 of the Data Protection Act 2018 places a legal obligation on data controllers to take the necessary steps to ensure the security of data. It explicitly states

> [T}hat the data shall be processed in a manner that ensures appropriate security of the data, including, by the implementation of appropriate technical or organisational measures, protection against—(i) unauthorised or unlawful processing, and (ii) accidental loss, destruction or damage (64).

This places a legal imperative on data controllers to prevent data breaches. This should thus help to enhance cyber resilience by reducing cybercriminals' success rate while also acting as a deterrent to their future activities because their chances of success may be lessened or detection may be higher. While the measures and guidelines that have been introduced as a result of the NIS Directive primarily apply to OES and DSP, the 2017 EU cybersecurity strategy in recognising that the NIS Directive only covers key strategic sectors, considers that logically a similar approach by all stakeholders hit by cyberattacks would be necessary to have a systematic assessment of vulnerabilities and entry points for cyber attackers.

The 2013 EU Directive similarly specifies that

> [I]n order to fight cybercrime effectively, it is necessary to increase the resilience of information systems by taking appropriate measures to protect them more effectively against cyber attacks. Member States should take the necessary measures to protect their critical infrastructure from cyber attacks, as part of which they should consider the protection of their information systems and associated data. Ensuring an adequate level of protection and security of information systems by legal persons, for example in connection with the provision of publicly available electronic communications services in accordance with existing Union legislation on privacy and electronic communication and data protection, forms an essential part of a comprehensive approach to effectively counteracting cybercrime. Appropriate levels of protection should be provided against reasonably identifiable threats and vulnerabilities in accordance with the state of the art for specific sectors and the specific data processing situations. The cost and burden of such protection should be proportionate to the likely damage a cyber attack would cause to those affected. Member States are encouraged to provide for relevant measures incurring liabilities in the context of their national law in cases where a legal person has clearly not provided an appropriate level of protection against cyber attacks (2013/40/EU (26)).

3.4.2 PROSECUTION

Several challenges have impacted prosecutions in Ireland. The first offence of hacking was successfully prosecuted in July 2013, under the provisions of the Criminal Damage Act, 1991. This prosecution was the result of a combined investigation between the Garda Bureau of Fraud Investigation and the Federal Bureau of Investigation, and pertained to the hacking of a political party's website during the run up to an election. There are a number of investigations into denial of service attacks on high profile targets, but as of October 2018 these had yet to result in prosecutions. Furthermore, as of October 2018, there has been few if any prosecutions under the Criminal Justice (Offences relating to Information Systems) Act 2017 (Harnett & Timon, 2018). The representatives from An Garda Síochána highlighted that the lack of convictions under the (Offences relating to Information Systems) Act 2017 to date, makes it difficult to assess the suitability of the Act (Interview, 2020). Media reports find that those few prosecutions which have been successful have been through criminal damage legislation (Gallagher, 2019). A number of these challenges in relation to successful prosecution of cybercrime are described in more detail below. They include the following: (1) Legislation (2) Reporting of cybercrime; and (3) Crime Statistics.

3.4.2.1 ANALYSIS ON THE IMPORTANCE OF LEGISLATION

Proper legislation is the cornerstone for the investigation and prosecution of cybercrime. However, similar to Ireland, many countries use a combination of old legislation (or at least not specifically developed to target cyber activities) and specific legislation. This approach offers both advantages and disadvantages but is somewhat understandable, given that it can take significant periods of time to update national criminal law to prosecute new forms of cybercrime.

This process often involves three phases, which include adjustment to national law, identification of gaps in the penal code, and drafting of new legislation (ITU, 2012). Existing laws often provide sufficient jurisdiction for traditional crimes perpetrated using new cyber tools, reducing the impetus for change. Furthermore, given that this law is often familiar territory for both law enforcement and the prosecution, they may find it more comfortable to navigate. However, if there is an absence of specific legislation relevant to new cybercrimes, criminals can exploit traditional legislation to conduct their activities with impunity – for example where crimes that are IoT dependent and new, non-specific legislation is often limited (Chawki, 2005). Irish policy-makers should ideally continue to focus their attention on addressing such gaps that arise in relation to new cybercrimes where non-specific legislation is sometimes limited.

This is exemplified in the Irish context with the Criminal Damage Act, 1991, which it should be noted was the first piece of Irish legislation that dealt with crimes against computers. It addresses hacking and does so as an act of vandalism. However, this is quite a narrow view and fails to account for the more complex collection of activities that illicit hacking often involves (Manning, 2016). Furthermore, other crimes involving new technologies would have, mostly likely, fallen outside of the scope of this Act; those now dealt with under the Criminal Justice (Offences relating to Information Systems) Act

2017. Maner highlighted the need for specific legislation as early as 1996, arguing that cyber technology is "uniquely malleable", "uniquely complex", "uniquely fast" and "uniquely cheap" and thus required special and separate consideration. In this case, legislators in Ireland should ideally analyse which new technologies and cybercrimes are not currently addressed by existing non-specific or specific legislation, and how legislation can be implemented in a technology-neutral manner where necessary.

Specific legislation often has its problems too. For example, each of the offences set out in the Criminal Justice (Offences relating to Information Systems) Act 2017 include the element that the offence was committed without ‘lawful authority’. Therefore, to achieve a prosecution it must be proven that such authority or lawful permission was not given. Like any crime where the actus reus must be proven, if this cannot be proven, it can be difficult to prosecute. This is one of the reasons to explain why law enforcement tend to emphasise the high importance of preventative measures and the development of innovative means to prevent this type of cybercrime.

The 2013 Directive on attacks against information systems explains that it does not impose criminal liability where the objective criteria of the offences laid down in this Directive are met but the acts are committed without criminal intent, for instance where a person does not know that access was unauthorised or in the case of mandated testing or protection of information systems, such as where a person is assigned by a company or vendor to test the strength of its security system. Legislation should ensure that it facilitates this type of work and that of security researchers to enhance the security of information systems and networks. The Ministry of Justice in the UK provides a good resource and guidance around vulnerability disclosures, in their Vulnerability Disclosure Policy. Something of this nature may be helpful in an Irish context, but there are different interpretations on how this should be best achieved. Brown, Edwards and Marsden (2009) highlight that vendors and major organisations like Google and Microsoft take the view that it is best practice for those who identify software vulnerabilities in their systems to immediately report them directly to these organisations, so that corrective action can be taken. Others argue, however, that they should first be reported to CSIRTs.

In the context of the 2013 Directive, contractual obligations or agreements to restrict access to information systems by way of a user policy or terms of service, as well as labour disputes as regards the access to and use of information systems of an employer for private purposes, should not incur criminal liability where the access under such circumstances would be deemed unauthorised and thus would constitute the sole basis for criminal proceedings. This Directive is without prejudice to the right of access to information as laid down in national and Union law, while at the same time it may not serve as a justification for unlawful or arbitrary access to information (2013/40/EU (17)).

In addition, the 2013 Directive specifies that given the different ways in which attacks can be conducted, and given the rapid developments in hardware and software, it refers to tools that can be used in order to commit the offences laid down in this Directive (2013/40/EU (16)). Such tools could include malicious software, including those able to create botnets, used to commit cyber attacks. Even where such a tool is suitable or particularly suitable for carrying out one of the offences laid down in this Directive, it is possible that it was produced for a legitimate purpose. Motivated by the need to avoid criminalisation where such tools are produced and put on the market for legitimate purposes, such as to test the reliability of information technology products or the security of information systems, a direct intent requirement that those tools be used to commit one or more of the offences laid down in this Directive must be also fulfilled.

The 2017 EU Cyber strategy explains that effective investigation and prosecution of cyber-enabled crime is a key deterrent to cyber attacks. It finds, however, that today's procedural framework is not fit for purpose where, for instance, the speed of cyber attacks can overwhelm our procedures, as well as creating particular needs for swift cooperation across borders. To this end, as announced under the European Agenda on Security, the Commission published draft legislation to facilitate cross-border access to electronic evidence on 17 April 2018 (Jeppesen & Nojiem, 2018). In February 2019, the European Commission proposed to start international negotiations on cross-border access to electronic evidence, necessary to track down dangerous criminals and terrorists (European Commission, website – following European Council Conclusions from October 2018).[17] If agreement is reached, an amendment to the Budapest Convention would be required (European Commission, 2019b). In parallel, the Commission is implementing practical measures to improve cross-border access to electronic evidence for criminal investigations, including funding for training on cross-border cooperation, the development of an electronic platform to exchange information within the EU, and the standardisation of judicial cooperation forms used between Member States.

Establishing intent and challenges in evidence sharing make it very difficult to attribute blame to offenders, which in turn impacts the ability to prosecute and convict individuals. As Brenner (2012) notes “the elimination of physical constraints and the alteration or

[17] https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en

elimination of identity combine to erode the efficacy of the traditional law enforcement model, which nation-states use to enforce their criminal laws” (139).

Another obstacle to effective prosecution, which is specified within the 2017 EU Cyber Strategy, is the different forensic procedures for the gathering of digital evidence in cybercrime investigations across Member States. Representatives from An Garda Síochána noted such challenges, and also highlighted that the borderless nature of cybercrime and the use of cloud storage can make it difficult to access data, even if companies reside within the nation, but hold their data elsewhere. This was also experienced by the representative from the corporate consultancy firm, who noted the challenges that the jurisdiction and cloud storage can have on investigations. Such issues have also been highlighted in the research of Koops & Goodwin (2014), who noted that the cloud reinforces challenges in relation to gathering digital evidence for criminal investigations. They, like the representatives of An Garda Síochána noted that mutual legal assistance can be inadequate in this area. As a result, their research looked at “legality of cross-border access to data under international law under the core principles of territorial integrity and non-interference” (abstract). They suggest that the widely accepted interpretation of international law is that accessing data stored on a foreign server without the prior consent of that state is a breach of territorial integrity of that state. Furthermore, they note that it is not a defence to state that the location of data was unclear or unknown. As a result, Koops & Goodwin (2014) argue that substantial work is required to develop shared basis of common understanding in this area, an observation also made by the representative from a corporate consultancy firm (Interview, February, 2020).

Koops & Goodwin (2014) note that framing cyberspace as a more abstract ‘space’, rather than as a physical ‘place’ that is controlled like territory, may be helpful. They suggest that this might look like “a new international or widely shared multilateral legal instrument that allows narrowly defined and strongly safeguarded forms of cross-border cyber-investigations” (abstract). Given that this is likely to take time, they also offered a shorter term alternative, whereby “some states — early adopters — could start creating and enhancing the legitimacy of unilateral actions that are narrowly defined, transparently conducted, and strongly safeguarded, by advancing an alternative account of sovereignty in cyberspace” (abstract). Interestingly, they identified the principle of open skies as a possible example and suggested that states might consider a new, and similar, principle of ‘open cyberspace’ in the context of cross-border access to data. This is a highly contestable approach, which is far from certain and much work needs to be conducted on these gaps.

3.4.2.1 *REPORTING OF CYBERCRIME*

Another aspect that negatively impacts the effectiveness of legislation in this area, relates to reporting. Manning (2016), amongst others, notes that cybercrime is under-reported and under-recorded. If cases are not reported, then prosecutions are unlikely, if at all possible. Kabay (2001) noted, as far back as 2001, but still relevant today, that

> [E]ven if attacks are detected, it seems that few are reported in a way that allows systematic data collection. This belief is based in part on the unquantified experience of information security professionals who have conducted interviews of their clients; it turns out that only about ten percent of the attacks against computer systems revealed in such interviews were ever reported to any kind of authority or to the public"(3).

Such a lack of reporting is still an issue of concern in the Irish context, and one highlighted in the Future of Policing in Ireland report. It notes that cybercrimes often go unreported, and that the crime statistics in Ireland do not reflect the rapid development of Internet crimes. The result being that there is no full picture on the degree or extent of the problem. Representatives from An Garda Síochána also confirmed this issue, noting that cybercrimes may be underreported to a greater degree than other crimes (Interview, 2020). This is in line with the findings of McGuire & Dowling (2013), who note a similar pattern in the UK. However, this is hard to prove without research. It was highlighted that reporting cybercrime to the GNCCB is largely based on knowledge of the work of the unit, or a personal contact with a member of the unit (Representatives from An Garda Síochána, interview, January 2020). It was suggested that reporting at the local or district level is less common.

Representatives from An Garda Síochána purported that if more people reported such crimes, there would be a knock-on effect whereby more cases would be investigated; more learning would be achieved from reviewing increased cases; more cases would likely go towards prosecution; more convictions would be achieved; more public attention would be received, which would serve to influence further reporting and greater awareness, and the circle would begin again (Representatives from An Garda Síochána, interview, January 2020). It was explained, however, that this would require greater resources, but the benefits would outweigh the costs, as it would ideally help reduce cases due to greater awareness. One of the first key steps to overcome this challenge does however relate to improving citizens awareness that they have been a victim of crime in the first place (Representatives from An Garda Síochána, interview, January 2020). They also noted that SMEs do not often understand that a crime has occurred against them (Interview, 2020).

It should be noted that this is not unique to Ireland. The National Crime Agency in the UK have identified underreporting as a ‘serious problem’, noting that it negatively impacts prosecution. Moreover, Hull, Eze and Speakman’s (2018) research supports the need for increased awareness to improve reporting, noting that they found that the issue of underreporting can be influenced by businesses’ lack of awareness of the attack or due to a fear of reputational damage if they report. McGuire & Dowling (2013) also found similar patterns in relation to individuals, finding that underreporting was also due, in part, to individuals not understanding the nature of cybercrime. Another but related issue in this regard, emerged from the British government’s paper titled ‘A Call to Action: The Cyber Aware Perception Gap. This was produced in conjunction with BritainThinks and Cyber Aware. The report summarised key research and identified “a large and growing gap between the nature of the threat, and public perceptions” (HM Government, 2018, p 5). They found that both the public and SMEs vastly underestimate the risk of cybercrime, whilst also feeling powerless to protect themselves against it.   The representatives from An Garda Síochána noted that SMEs do not report such crimes because their main priority is to keep their businesses up and running when such crimes occur. Furthermore, those that do, often only do so because they want to comply with internal or regulatory reporting requirements (Representatives of An Garda Síochána, interview, January 2020).

In the Irish context, organisations are encouraged by the NCSC and An Garda Síochána to report both cybercrime incidents and cybersecurity issues. The NCSC recommends that those who think they have been victim of a cybercrime should report it to An Garda Síochána. This can be done by reporting said crime to a local Garda Station or to the GNCCB. Interestingly, representatives from the financial institutions noted that reporting can be difficult, and burdensome. A more streamlined, easier process would be likely to improve reporting, which in turn would improve national statistics, which in turn would provide more insights and information about patterns and trends (Representatives from the financial sector, interview, January 2020). An Garda Síochána echoed this, and identified the Action Fraud Online Reporting Platform in the UK, which is available to businesses for reporting cybercrimes. It was noted that if a similar platform were to be implemented in Ireland, reporting would likely increase as the system of reporting would be streamlined and made easier (Representatives from An Garda Síochána, interview, January 2020). Australia has a similar model, called the Australian Cybercrime Online Reporting Network (ACORN). This is a national online facility that receives cybercrime reports from members of the public. It also acts as a repository for information for Australian law enforcement agencies and provides crime prevention advice to the public, which is believed to have been effective in improving law enforcement response to cybercrime (Morgan et al, 2016).

To centralise the reporting of cybersecurity related issues, the Government established a CSIRT. However, the CSIRT currently provides “incident response services to Government bodies and Critical National Infrastructure providers across Ireland”, rather than to individuals and non-designated CI such as other businesses. The importance of extending domain CSIRTs was highlighted by the representative from the Banking & Payments Federation Ireland (BPFI), who said it may be worth considering the development of a Financial Services CSIRT, and even going as far as embedding representatives from the financial sector in the NCSC (Representative from BPFI, interview, January 2020).

CSIRT-IE also acts as a national point of contact for international partners who wish to inform Irish-based entities of cybersecurity matters which may affect them” (National Cyber Security Centre, 2019). The scope of CSIRT-IE’s activities covers prevention, detection, response and mitigation services to Government departments and core state agencies. Its responsibilities include:

- Monitoring incidents at a national level;
- Providing early warning, alerts, announcements and dissemination of information to relevant stakeholders about risks and incidents;
- Responding to incidents;
- Providing dynamic risk and incident analysis and situational awareness;
- Participating in the CSIRTs network.
- Prosecution (National Cyber Security Centre, 2019).

Reporting cybersecurity incidents and cybercrimes when they occur or are detected, means that CSIRTs can provide warnings and alerts to other potential victims and in some way help to prevent further victimisation. Greater insights can also help link crimes and in so doing help direct investigations towards prosecution. The identification and reporting of threats and risks posed by cyber attacks and the related vulnerability of information systems is a pertinent element of effective prevention of, and response to, cyber attacks and to improving the security of information systems (2013/40/EU (12)). Providing incentives to report security gaps could add to that effect. Member States should endeavour to provide possibilities for the legal detection and reporting of security gaps (2013/40/EU (12)). Consideration of introducing a formal bug bounty programme, whereby individuals are compensated and recognised for reporting bugs, especially those related to security exploits and vulnerabilities, could be made, either within recognised government vendors or contractors or more widely – this would be one way to develop this. However, this too should be well thought through in respect to what is legally possible. For example, the Ministry of Justice in the UK cannot offer a paid bug bounty programme. However, they do try to show “appreciation to security researchers who take the time and effort to investigate and report security vulnerabilities to us according to this policy wherever we can” (Gov.UK, 2020).

3.4.2.3 CRIME STATISTICS

There is, in addition, a need to collect comparable data on the offences laid down in the 2013 EU Directive (24). Relevant data should be made available to the competent specialised Union agencies and bodies, such as Europol and ENISA, in line with their tasks and information needs, in order to gain a more complete picture of the problem of cybercrime and network and information security at Union level and thereby to contribute to formulating a more effective response. Member States should submit information on the modus operandi of the offenders to Europol and EC3 for the purpose of conducting threat assessments and strategic analyses of cybercrime in accordance with Council Decision 2009/371/JHA of 6 April 2009 establishing Europol.

An Garda Síochána provide input to Europol’s annual Internet Organised Crime Threat Assessment (IOCTA) report (Representative from An Garda Síochána, Interview January 2020). Providing information can facilitate a better understanding of present and future threats and thus contribute to more appropriate and targeted decision-making on combating and preventing attacks against information systems. Article 14 of the 2013 EU Directive does in fact require Member States to have a system in place for the recording, production and provision of statistical data on offences referred to in the Directive, including data on the existing number of offences, and the number of persons prosecuted for and convicted of these offences. Member States shall transmit the data collected pursuant to this Article to the Commission.

However, it was highlighted by the Representative from the Central Statistics Office that it can be very difficult to harmonise data across jurisdictions and to meet the reporting requirements in relation to EU Directives and other bodies, because no one organisation can really supply all the figures. For example, the data is usually held by organisations from both the private and public sector, and there is often no compulsion or legal obligation on the private sector to supply it. It was noted that this is not only a problem for Ireland. In short, there does not currently seem to be a complete picture on the level of cybercrimes and no one agency seems to have a complete data set.

Despite these challenges, it is the role of the European Commission to ensure that a consolidated review of the statistical reports is published and submitted to the competent specialised Union agencies and bodies. For similar reasons, there could be value in publishing the data that is collected and recorded at national level in Ireland by An Garda Síochána in order to drive the development of better solutions based on informed statistics (if other government entities possess additional data on cybercrimes, this might also need to be considered in this instance). Over the past number of years, the UK has worked considerably hard to introduce questions that measure cybercrime rates on the Crime Survey for England and Wales. These have been trialled and are running for a couple of years now. This process is one that the Irish government - if including the collection of this data is within its priorities - could learn from and simplify the process. Crime surveys have now long replaced police recorded crime as being the most accurate measure of crime rates given that they provide insights into unreported crimes (Lohr, 2019). It should be noted that is dependent, of course, on a good quality survey. Applying a similar approach may be a step in the right direction. The Scottish Household survey under its digital section has introduced questions on cybersecurity behaviours to establish the prevalence of these behaviours across the population. The UK's NCSC has also commissioned work of this nature. The introduction of questions like these into nationally representative services could go a long way towards informing the development of efficient and effective cybersecurity in Ireland.

In more recent times, Europol's EC3 reports explain that, from a law enforcement perspective, the most pertinent steps that OES and DSP are obliged to take because of the NIS Directive is the obligation to notify the relevant CSIRT of any security incident having a significant impact on service continuity without undue delay. Whether or not this means that more complaints will reach law enforcement remains to be seen (EC3, 2018). Moreover, there is a chance that with tighter controls on data and less data available, this will make what data can be obtained by criminals even more valuable (EC3, 2018). With the EU GDPR coming into effect in May 2018, the reporting of data breaches is now also a legal requirement across the EU, bringing with it significant fines.

Such statistical data should ideally assist better future analyses of the effectiveness of legislative initiatives such as those outlined at national level in Ireland and beyond by providing metrics that examine, for example, whether the introduction of penalties for criminals has led to sufficient deterrence of cybercrime, or obligations to enhance cybersecurity and resilience have in fact led to a reduction in cybercrime activities.

The way in which cybercrime statistics are arrived at in Ireland is useful to examine. Official figures are based on those reported to An Garda Síochána, and subsequently recorded by them. The CSO has the responsibility for coordinating the official statistics of public authorities, so it provides the official figures. Its role is to impartially collect, analyse and make available statistics about Ireland’s people, society and economy. In relation to crime statistics, much of the information originates from an extract of data from An Garda Síochána’s PULSE data. This is provided to the CSO on a quarterly basis (Representative from the CSO, Interview December 2019). The data provided within this extract is a subset of what is available on PUSLE. The information provided has three key variables: incident type; date reported; and the station where the crime is reported or has taken place. The incident type is the classification of the incident by An Garda Síochána. The CSO have no input into this. However, it was highlighted by the CSO Representative that it is evident that those within AGS who are now creating these categorisations are looking internationally, to ensure their classifications align with international best practices (Interview, December 2019). This is welcomed by the CSO, as they plan to move to the International Crime classification system in the medium to long term. Currently, the CSO use the Irish model.

Once the incidents are received from AGS they are mapped against their own criminal classification systems. The incident type does not specifically link to a specific piece of legislation, albeit on occasion, the data provided may contain information on charges or summons, which in turn often contain information on offence code or offence description if charged (Representative from the CSO, Interview December 2019). Therefore, in the majority of cases, it is currently not be possible to answer questions relating to breaches of specific legislation. It is worth noting that the categorisation of fraud has recently changed, with additional sub-types added, which has impacted the recording of cybercrime cases. A number of new incidents types were added, including for example, assessing interference in IT systems (Representative from the CSO, Interview December 2019). That said, the CSO never provide a breakdown of fraud offences because it is difficult to provide an objective breakdown, as the information needed is not often there to drill down to that level of specificity. Furthermore, they are also not in a position to provide statistics in relation to all technology related cybercrime affecting businesses here or the number of convictions in respect of same, as the CSO do not compile or publish any statistics using the description ‘cybercrime’ at present. A question of this nature was asked in PQ 26508/17. The response noted that the relevant categories of recorded crime are not disaggregated along these lines and therefore the information in question is not displayed in the official CSO crime statistics publications. It was also noted that AGS were also not in a position to provide specific information in respect to cyber-enabled and cyber-dependent crime, because as mentioned above, incidents are recorded on a Pulse basis on the type or category of crime committed, not on the offence breached. An example was presented in the response to illustrate this point. They noted that some cybercrimes were recorded, at least at that time, on PULSE under the general heading of 'Criminal Damage' using the sub-heading 'Unauthorised Accessing of Data'.

Other challenges that negatively impact the reporting and recording of cybercrime incidents will be further discussed in the next section. It is evident that the legislation in Ireland, while improved, is not sufficient in of itself to tackle cybercrime because it is only one tool in the toolkit, which includes several non-legislative measures to combat cybercrime. Given that legislation alone is not sufficient to responding to the threats posed by cybercrime, the next section will consider additional non-legislative models of best practice for responding to the threat of cybercrime nationally and internationally.

Section 4: What are the models of best practice for responding to the threat of cybercrime nationally and internationally?

4.1 Non-Legislative Models of Best or Good Practice

Reliance alone on the deterrent effect of criminal legislation is not a sufficient response to cybercrime. Effective and appropriate policies and practices are needed to help in safeguarding against risk and related harms. Similar to traditional crime prevention, such responses can be broken down into three categories: (1) Raising Awareness; (2) Target Hardening; and (3) Situational Prevention. This section of the report is structured around these three categories. The section then ends with a discussion on finding a balance between tackling cybercrime, while protecting human rights.

4.1.1 MEASURING SUCCESS

There is evident dissent about the nature of best or good practice in the area of cybercrime. Generally speaking, best or good practice is a method or technique that is widely accepted as superior to other alternatives because the results it produces are more impactful in a positive sense to those achieved by other methods. In so doing, the best or good practice becomes the standard way of doing things. In more scientific environments, best or good practices are determined based on rigorous evaluation. However, such standard practices are not widespread in this area of cybercrime. As noted by Professor David Wall, University of Leeds, there is a problem with finding agreement as to what constitutes good practice in this field (Prof. Wall, interview December 2020). He notes some key factors that influence this situation, namely a lack of awareness of what and how things might work; the lack of funding to experiment, review and evaluate existing practices; and the lack of willingness of some organisations to make themselves and their practices open to external scrutiny because of a desire to be seen to be on top of things. A representative from Europol echoed this lack of systemised best practices (Europol representative, interview, December, 2019). Notwithstanding, he purported that Europol continuously tries to develop and test practices and build on those that are found to be effective. This is conducted through a constant process of review (Europol representative, interview, December 2020). Europol strives to build on effective actions and develop their practices as they pertain to their support for EU Member States and requirements. The example provided here of Europol's processes to identify and build upon known good practices could be further examined and possibly implemented at national level by Irish law enforcement and policymakers, if such stream-lined procedures are not already in place.

Despite little formal agreement of what constitutes good practice in this field, this section of the report reviews a range of activities at the individual, organisational, national and international level that academics and/or practitioners often consider to be good practice. This is based both on a literature review and through interviews conducted for the purpose of this report. Few of the models mentioned in this report have been rigorously assessed with regard to success and therefore it can be difficult to determine which models are successful without using an arbitrary assessment. Unfortunately it is beyond the scope of this review to evaluate the merits of categorisation for good practice given to the examples discussed, but the report does try to present the negative as well as positive aspects of these activities. In addition, it is worth noting that local and contextual contingencies usually need to be considered when evaluating a model, as these factors often play an influential role. As a result, importing a model from one area to another directly is rarely effective, without proper consideration of these underlying and potentially influencing factors.

PWC (2019) in the Global Technology Risk Management Study questions what ‘good’ looks like, which is echoed in academia, in this area, where there is a gap in the research as to what works. However, Brewer et al (2019) in their recent publication, Cybercrime Prevention Theory and Applications, try to address this question. This is an important contribution to the field given that the sociological/criminological study of cybercrime is still quite small. Much of the research dedicated to cybersecurity has related to the purely technical and there are few, if any, studies that focus on offenders and recidivism. Moreover, studies of punishment and penology more generally has yet to get to grips with cyber-dependent offending, but undoubtedly has something to offer. Increased research in this area may be timely.

The lack of ability to measure success, or the absence of evaluation mechanisms with strategies is noted by ENISA. The agency now recommends as good practice, that nations include mechanisms on evaluation in their strategies, and adjust them to ensure continuous improvement. ENISA has also published an evaluation framework in 2014. The UK national cybersecurity strategy for the period out to 2021, for example, includes references to metrics and the Scottish Cyber-resilience strategy also contains useful performance indicators and outcomes against which progress can be measured.

That said, reviews of organisations, bodies, or companies often take place, whether they are conducted internally or externally. This can be illustrated in the Irish context by the Comptroller and Auditor General (C&AG) review of the NCSC. However, while such reviews are important, they are often not measuring success at the granular level that is needed to determine whether core activities have been a success. Many only assess the overall outcome achieved. This is a further limitation in assessing what works well and what does not.

Another significant factor for why there is limited evaluation at the required level of granularity, therefore making success hard to measure, is the lack of reliable and consistent statistics in this area, as discussed in the previous section. It is difficult to conduct effective research if the data is not available. In addition, there is often a lack of consistency in methodologies used when research is actually conducted, which makes it difficult to compare findings across studies, which further impacts the ability to measure the prevalence of cybercrime effectively (McIntyre, 2015).

That said, some have tried to provide structured mechanisms to measure success in relation to crime more generally. For example, the report titled ‘Improving the Criminal Justice System – lessons from local change projects’ jointly published in the UK by the Prosecution Service Inspectorate, the Inspectorate of Constabulary, Inspectorate of Probation and the National Audit Office. This report “draws out good practice lessons from three such projects. In order to provide a degree of focus, all of the projects cover the ‘front-end’ of the CJS – that is to say, crime reduction or, where a crime has been committed, the process from arrest to sentencing in court. The projects were chosen because they had achieved some combination of: cost reductions; improvements in efficiency and overall performance; and a better service for witnesses and victims of crime” (UK Government Publication, 2011, p 6). To determine these good practices, they used a standardised framework of management principles drawn from the UK’s National Audit Office December 2011 Guide to Initiating Successful Projects and more general guidance on project delivery, which ensure consistency across evaluations. Such an approach could potentially be applied specifically to cybercrime.

Currently, An Garda Síochána and other interviewees reported a range of different methods used to measure success. For example, developing mechanisms to record figures such as the increase in incidents, the number of people impacted, and speed of time with which incidents were dealt with and contained. However, for the most part, the measurements have more to do with performance and recording, rather than directly focused on crime prevention (Interviews, December 2019 and January 2020).

4.2 Raising Awareness

Raising awareness of crime is important in the prevention of it. If people understand what constitutes a crime, they can take action to prevent them falling victim to such a crime. This holds true in reference to cybercrime. Practices that help in this regard include awareness campaigns and increased education, training and upskilling. Good practice models in these areas are discussed below.

4.2.1 AWARENESS CAMPAIGNS

The NIS Directive specifically highlights the need for campaigns relating to awareness of cybercrime, across a number of areas. The Directive notes ENISA's key role in respect to awareness-raising and training, while also recommending that awareness raising should be a key element of national strategies. It further highlights that EU Cooperation Groups should exchange information on awareness raising to share others' best practice. Europol's annual cybercrime threat assessment (EC3, 2018) similarly echoes the benefits of such initiatives. In the European context, examples of awareness raising activities include Safer Internet Day, International Youth Day, and European Cyber Security Month (ENISA, 2016). Many of these initiatives also take place in Ireland. Furthermore, the National Cyber Security Strategy includes a measure relating specifically to Public Awareness (Government of Ireland, 2019).

ENISA (2016) highlights the importance of awareness raising specifically as it relates to security threats and vulnerabilities, and their impact on society. This is relevant in relation to fighting cybercrime, as increased information and knowledge should help inform both individuals and businesses on how to behave and protect themselves against online risks. However, a central challenge with this perspective, if viewed in isolation is that it assumes simply knowing more will change people's behaviour, which fails to account for the other pressures, pleasures and demands people may prioritise (e.g. streaming a show illegally, saving passwords in plain text files, using the same password for everything). There are limits to what people will do in the name of security. Essentially, more knowledge and awareness may not necessarily mean a safer population.

That said, there is a significant logic to believing such approaches work. For example, Chatterjee, Kar, Dwivedi and Kizgin (2019) research in India found that awareness of cybercrimes positively influences the use of technology to prevent cybercrime. Sarre, Lau & Chang (2018) found similar results, noting that education in this area with those who are most vulnerable is deemed effective. However, it is worth noting that this research related to campaigns targeted at specific groups of people. In contrast, the current approach in many of the aforementioned activities appear to use a one size fits all model, believing the same message fits everyone. As mentioned above, this approach fails to take into account that people think differently about these things, and interpret these messages in different ways. Bada and Sasse (2014) argue that campaigns need to resonate with target groups, and that the intended message needs to resonate locally, socially and culturally. This will require greater investment in understanding the current predominant cybersecurity practices across the population, and targeting core groups with messages that meet their needs. However, a more targeted approach will ensure there is less wasted money on generic campaigns and messages directly targeted at the ‘general public’. The lack of impact of general campaigns may be evident in the Irish context, as, representatives from financial institutions note that despite the increase in campaigns, people seem more willing to respond to requests for personal information by email, phone, or messaging services (Representatives from Financial Institutions, interviews, January 2019). This might suggest similar patterns to the research that generic campaigns are not working as intended, but this would require further analysis to properly assess.

Nonetheless, the benefits of providing training to help develop awareness of cybercrime issues is highlighted in the research of Singh et al (2013) and Chen et al (2015). This is similar to research in the context of behavioural change, where it has been found that effectively influencing individuals and changing behaviour requires more than simple dictating what they should and should not do. As highlighted by Bada, Sasse and Nurse (2019), the “‘provide information and they will use it’ approach does not appear to be effective in spreading the message fully or widely enough” in the context of cybersecurity (14). They note that people need to accept that the information is relevant to them and then understand how they should respond. They then need to want to respond accordingly given competing demands, rather than circumventing the security protocols. This illustrates that awareness campaigns, although good practice, may not be as effective as imagined if not designed in a way that is cognisant of its limitations.

Furthermore, there is little understanding of the length of time people persist with secure behaviours. This is due to a lack of longitudinal data in this area. Yet, in the case of risk perceptions, it is known that these are time sensitive, which might suggest that security behaviours motivated by increased awareness may be a short term manifestation too. Therefore, research with a longitudinal element would be informative and useful.

There is also a risk that the information provided can act to escalate fear without influencing a positive response (Coventry, Briggs, Blythe, & Tran, 2014). As a result, researchers have argued that such campaigns should be developed cognisant not to create a climate where victims become the blamed and the environment becomes hostile to them, lessening their ability to seek support or to report (Button and Cross, 2017; Horgan, 2019). Messages need to be designed to be sensitive and nurture a supportive security culture, rather than one that creates a sense of scapegoating and stigma. Horgan (2019) in his research notes that cybersecurity messages that focus on individuals, and fail to build communities of supportive local social networks who can share better knowledge and practices are likely to be limited. Rather they should be designed to offer support and create an atmosphere where people are safe to report. He

(Horgan) also purports that by promoting this kind of social context and culture of empathy, vulnerable users may be less put off or alienated by security messages they struggle to understand, citing older users for instance.

Interestingly, it was noted in the interviews with the financial institutions that cybercrime and related cybersecurity measures are routinely framed with a technical focus, thereby alienating people from the discussion, potentially further victimising them. The financial institutions highlighted the importance of using simple and plain language when speaking about threats and risks to help people engage more with the issue. The representative from a corporate consultancy firm also highlighted the need to use language which people can relate to and understand (Interview, February, 2020). The merits of such an approach is reinforced in the research literature that calls for a non-technical approach to fighting cybercrime, and one that looks at the human factor in cybercrime and cybersecurity (Leukfeldt, 2017). While this agenda does not dismiss the role of the technical sciences in answering the research questions in this area, it rather looks to complement this approach by adding the perspective that cybercrime remains a human activity, and therefore warrants greater examination of this human element.

Briggs, Blythe, & Tran (2014) state that “knowledge and awareness is a prerequisite to change but not necessarily sufficient and must be implemented in conjunction with other influencing strategies” (19). The UK’s Government Office for Science conducted research in this area, more specifically researching into ‘Using behavioural insights to improve the public’s use of cyber security best practices’ (Coventry, Briggs, Blythe, & Tran, 2014). Coventry, Briggs, Blythe, & Tran (2014) found that in this context “the vast majority of messages are general and do not target a particular behaviour or group but attempt to address all simultaneously” (14). They state that research suggests that the success of awareness campaigns are more likely if they are multifaceted and supplemented with (1) Concurrent community programmes; (2) Policy and law changes; (3) Readily available products and services to support the target behaviours; (4) Tailored messages for specific audiences; (5) Messages being built-in to many different delivery mechanisms; and (5) Role models and champions exhibiting the behaviour (14).

The National Cyber Security Strategy (2019-2024) of Ireland does include a number of activities relating to information and awareness campaigns. It states that the Government will “develop a national cyber security information campaign which will use information provided by the NCSC and the Garda National Cyber Crime Bureau and be delivered by entities which are directly engaged in information provision” (Government of Ireland, 2019; p. 48). The aim of the campaign is to improve societal awareness around common cyber risks and will also include more targeted awareness campaigns aimed at vulnerable groups such as children and the elderly. This approach of having such targeted campaigns is in line with Coventry, Briggs, Blythe, and Tran (2014) recommendation that messages should be tailored for specific audiences. Two specific actions to achieve this that have been highlighted within the new NCSS include (1) supporting the continued inclusion of cybersecurity elements in Webwise programmes and (2) developing a public awareness campaign to include information on cybersecurity and cybercrime prevention.

This is likely to require a challenge of the status quo as general awareness campaigns have been commonly used in this space for some time. A representative from Europol explains that although Europol's role relates largely to the support of investigations in the EU Member States, the agency does try to help in the areas of cybercrime prevention and awareness raising. They do this through awareness raising campaigns, and working in conjunction with their network of law enforcement and private sector partners to ensure the campaign reaches the widest possible audience (Europol Representative, interview, December 2019). These campaigns are also available in multiple languages, which is EU funded and promoted by private sector partners in order to further enhance the reach of such campaigns. The BPFI have been one of these contributors and supporters (Representative from BPFI, interview, January 2020). Europol awareness campaigns were cited in a positive light by other experts interviewed for this report. One specific campaign that was highlighted as a good example is the Europol 'Say No' campaign related to raising awareness on online sexual coercion and extortion affecting minors. An Garda Síochána noted that they contribute content into these campaigns and in turn use the materials to supplement their own material (Interview, 2020), as did the BPFI (Representative of BPFI, interview, January 2020). By way of further examples, the United Kingdom's National Crime Agency also actively uses information campaigns. One very effective campaign has been their campaign to raise awareness of Sextortion. While such praise is welcomed, the important element of any campaign is that it resonates with the target audience and brings about change, as identified in the research above – even though there are challenges with reaching such audiences.

The findings in the interviews very much echoed the academic literature in this area with respect to the need for targeted campaigns and challenges such campaigns can pose. While the benefits of general campaigns such as those conducted by EC3, at the national level, or through the BPFI's own 'Fraud Smart' campaign, were acknowledged, there was agreement that more targeted campaigns are needed (Representative from the BPFI and An Garda Síochána, Interviews, January 2019). Money mules were highlighted as an example of a group who may benefit from a targeted campaign, as they are often found to use the excuse that they did not know that what they were doing was a crime (Representatives from financial institution, interview, December 2019). The interviewed representative from the National Crime Agency noted that while such campaigns should be public facing, unless conducted directly, he remarked that it is difficult to engage with the public, as they often do not see the relevance which can reduce campaigns' impact. He noted that one important question that needs to be asked from the outset in making campaigns effective is 'how to keep people engaged'? Furthermore, he noted that there needs to be a strategy of engagement and re-engagement over time to ensure relevance is maintained, which can be hard to do. This may confirm that integrating longitudinal elements, as noted above, has been limited.

4.2.1.1 Supporting Reporting

Increased awareness should ideally result in less crime, but also in more reporting. However, people will only report when they feel safe to do so. Creating such an environment is a pivotal element in awareness raising. Despite the obstacles identified above, some campaigns have been successful. The representative from the NCA highlighted areas within the criminal justice system where campaigns have been effective and played a role in changing the culture around the topics in the campaign. For example, drink driving. He noted the need for a cultural change in how cybercrime is perceived, suggesting that being victimised by cybercrime is often blamed on the victim and not taken as seriously as other more traditional crime. This echoes the research of Horgan (2019) and Button and Cross (2017) about victim blaming. For these reasons, reviewing the campaigns that have had a last impacting, even if they are in another field, could provide learning and ideas for effective campaigns in this area of the fight against cybercrime. Furthermore, as awareness campaigns are an integral part of both Irish and EU cyber strategies and recommended good practice, behavioural change strategies should ideally be an integral part of any awareness campaign in order to increase the likelihood that individuals and businesses will in fact act on the advice. One emerging area that may indicate that there is also a shift in how messages are framed is illustrated by a move towards constructing or considering cybersecurity from a public health perspective, and drawing on insights from that domain to enhance public cybersecurity more generally.

4.2.2 EDUCATION, TRAINING AND UPSKILLING

As noted earlier in the report, education is a key element of best practice in this area and is also a mechanism for raising awareness. ENISA (2016) identifies investment in cybersecurity related education and more general education in information security threats as key to decreasing the risk for businesses and society at large. In this regard, under the framework of the Commission on Crime Prevention and Criminal Justice (CCPCJ), the UNODC launched a cybercrime repository in 2015. This repository is a central database of legislation, case law and lessons learned on cybercrime and electronic evidence (UNODC Website, 2020b). It acts to assist countries in their efforts to prevent and effectively prosecute cybercriminals. This is an excellent resource given that many countries are not producing enough trained personnel in this field to meet the markets' demands (ENISA, 2016). That said, this should not be mistaken for the absence of good programmes.

There are examples of universities that offer programmes in this regard. For example, University College Dublin (UCD) has developed the Centre for Cybersecurity and Cybercrime Investigations which has a strong reputation for its work on training law enforcement from across Europe (rather than education for businesses and individuals). That said, it also provides training to non-law enforcement individuals, promoting the principles of good practice in forensic analysis in this area. Most non-police students comes from organisations that have a remit to enforce legislation, for example the NCSC, the Revenue Commissioners or the Central Bank. The centre also works with UNODC, OSCE, and Interpol in relation to building capacity across the globe (Representative from UCD, interview, January 2020). Not only does the centre provide training, but they also offer train the trainer programmes to ensure they leave people with the soft skills to develop and train others, in their absence (Representative from UCD, interview, January 2020).

Notably, the development of the Masters programme at UCD stemmed from a proactive approach from An Garda Síochána when they initially formed a cybercrime capacity in the 1990s. The programme initially started as a diploma course but grew into what it is today. In the early 2000s, An Garda Síochána with UCD, supported by EU Commission funding, conducted a study on the state of play of cybercrime across Europe. The report had three key findings, namely the need for increased training resources, formal qualifications and Continuous Professional Development, which influenced the evolution of the work of the Centre (Representative from UCD, interview, January 2020). The European Cyber Crime Training and Education group emerged from this review, with An Garda Síochána and UCD founding partners. An Garda Síochána speak very highly of the UCD centre, in terms of their training. The benefits in terms of skill and expertise development is clear but other benefits are also appreciated. For example, a practical benefit of having such formal qualifications helps present someone as an expert witness. Secondly, having a dedicated programme for law enforcement means that it is fit for purpose and in line with what is needed to investigate and bring a case to court (Representatives from An Garda Síochána, interview, January 2020). Whilst having a stream for non-law enforcement means the standards are similar across all graduates.

The centre works to ensure strong relationships between law enforcement and industry, and works in the area of education, training, research and tool development. This approach and the centre's collaboration with NCSC is in line with ENISA's (2016) guide which states that it is good practice to "establish cooperation with leading academic and R&D institutions on new digital forensic techniques" (33). It is believed to be a much needed element in developing "new tools for deterring, protecting, detecting, and adapting to and against new kinds of cyber attacks" (38). A number of police forces are applying this recommendation to their own organisations, and developing internal R&D units, such as in Latvia. A representative from UCD noted that the introduction of an R&D component within An Garda Síochána would assist them in being more forward thinking, bring new ideas and expertise to the organisation, while also benefiting from researchers embedded within the organisation (Representative from UCD, interview, January 2020). The EU's Horizon2020 programme offers opportunities to access funding to support such developments (Representative from UCD, interview, January 2020).

Another example in the Irish context is the work by the Cork Institute of Technology (CIT), supported by the IDA, to develop a programme to establish and grow a Cyber Security Cluster in Ireland. The cluster aims to include "stakeholders from industry, academia and government and will seek to encourage cooperation, raise awareness of education and career opportunities, drive innovation and stimulate new business in the Cyber Security field" (Government of Ireland, 2019, 4). The NCSC has supported the CIT in building and managing the cluster from inception, resulting in the establishment of 'Cyber Ireland' in 2018. Cyber Ireland brings together, industry, academia, and government to represent the needs of the cybersecurity ecosystem in Ireland, aiming "to enhance the innovation, growth and competitiveness of the companies and organisations which are part of the cluster" (Cyber Ireland, 2019).

In terms of additional examples of training and education in Ireland, at the time of writing, Irish universities offer four undergraduate courses in cybersecurity, sixteen postgraduate courses with modules in cybersecurity, and eight postgraduate degree courses in cybersecurity. A more applied post-graduate education initiative is the 'Cyber Security Skills Initiative', which was launched by Skillnet Ireland in partnership with the NCSC, GNCCB, other agencies and third level institutions in October 2018. As set out in the NCSS Consultation document "the core aims of the initiative are to develop awareness, bridge the skills gap and to set standards for skills and competencies for Cyber Security roles. The three year plan will focus on building training and accreditation in the field to address skills gaps, attracting more young people, and in particular women into the sector and promoting Continuous Professional Development. Skillnet Ireland estimates that the initiative will deliver Cyber Security training to in excess of 5,000 people in the industry over the next three years" (Government of Ireland, 2019, 4). This is a good practice activity to increase the much needed talent pool in this area.

Prof. Wall highlighted that the relationship between academia and law enforcement should move beyond training to greater collaboration in regard to joint, mutually beneficial research. While there are some examples of this already, Wall noted that this has not fully happened yet. A number of challenges are evident that impact this area. For one, he suggests that such research has to fit into the strategic overview of the police force and be useful to them. However, they often have conflicting ideas about what may be useful and/or what should be prioritised. There is also the historical tension between academia and police research more generally that needs to be overcome.

Secondly, he reported that from his experience, law enforcement and analysts can be fearful if their data is passed outside of their control, as if they are fearful of being caught out through external criticism. Thirdly, he also found from personal experience that demands for data usually mean additional work for the person tasked to retrieve it, which added to their normal workload and could make them reluctant to cooperate fully with the request. Finally, he highlighted that police data, often seen as the holy grail of data, is not usually fit for purpose for academic researchers. The data demands of practitioners do not always map onto the needs of social scientists, so it should not be seen as the key to answering all the questions (Prof. Wall, interview, December 2019).

4.2.3 UPSKILLING AND TRAINING FOR LAW ENFORCEMENT

Specifically in the context of law enforcement, raising awareness through training and upskilling, beyond formal education, is critical. This is hugely relevant in the Irish context where An Garda Síochána have a lead role in respect to preventing, investigating and prosecuting cybercrime. The first dedicated unit to cybercrime, the Computer Crime Investigation Unit was established in 1991 and re-developed in 2017 into the GNCCB. The GNCCB is a national unit and is "tasked with the forensic examination of computer media seized during the course of any criminal investigations" (An Garda Síochána website, 2020). The unit is also responsible for investigating cyber dependent crime. It is now made up of all sworn officers, supported by Higher Executives Officers (HEO) and Clerical Officers (COs) who coordinate the administrative element of the unit. These non-sworn officers all have specialised training as they often take the first complaint if a victim contacts the unit (Representatives from An Garda Síochána, interview, January 2020). At the time of writing, approval has also been given, as part of the ongoing expansion plan to recruit four, of the six, approved civilian forensic analysts. The introduction of this skill set will be an asset to the unit (Representatives from An Garda Síochána, interview, January 2020).

Over the last number of years, the unit has invested in developing capacity in the regions across Ireland. Two pilot regional cyber units were established in the Southern and South-Eastern Regions in 2017 (An Garda Síochána website, 2020). These regional units operate a triage model, which provide tiered response and capability for computer forensic services on a Regional basis. These units are staffed by locally-based and trained first-responders and cyber triage specialists. In 2019, the Garda Commissioner highlighted the additional roll out of satellite hubs across other regions. The organisation is now in the latter stages of the development of these satellite hubs. They will be centrally managed, and will be tasked and resourced by GNCCB, but will provide specialists services out in the regions. To start with, the units will work at a low base rate but skills and expertise will build and grow over time and experience (Representatives from An Garda Síochána, interview, January 2020). These hubs will triage cases, deal with cases they are capable of, and send the more difficult cases to the HQ. This is an interesting development as some interviews in the financial sector report that if incidents are reported at the local level, the expertise is not always present (Representatives from the financial sector, interview, January 2020). That said, training is provided to all members, through the Garda Training College, as all members need to be able to take a complaint in this area. However, despite this training not all members may feel competent to take such reports (Representatives from An Garda Síochána, interview, January 2020). Holt and Bossler (2015) find that there is often some police cultural resistance, due to the fact that cybercrime in the UK and U.S. at least, may not fit easily into the image of policing, nor is it routine everyday police work. It would require further analysis to see if this is the case in An Garda Síochána. Online training is available to members within the organisation (Representatives from An Garda Síochána, interview, January 2020).

ENISA (2016) highlights the need for constant upskilling and training for law enforcement, especially for digital forensics. This need was echoed by Europol, where the interviewed representative noted that training is a main element in EC3 activities in close cooperation with CEPOL and the European Cybercrime Training and Education Group. Their partners provide some training opportunities which helps to upgrade skills and further develop relationships. In return, the existence of EC3 has helped enhance the capabilities and effectiveness of law enforcement across Europe (ENISA, 2016). However, their existence, does not replace the need for a dedicated capacity at the national level which applies to Irish stakeholders involved in this space. ENISA (2016) states that it is good practice to “create national cybercrime units (law enforcement and judicial authorities)” (33). The establishment of specialised law enforcement units for conducting cybercrime investigations/forensics was also highlighted at the Council of Europe (COE) Octopus Conference and Budapest Convention 10th anniversary meeting on ‘Cooperation against cybercrime’ (2011) as good practice.

A EUROPOL and EUROJUST (2019) report also highlights that developing and maintaining specialised expertise across these different stakeholders must occur at the same rate. In addition to these units, “countries [should] develop official guidelines for the work of those agencies, especially regarding the collection, preservation, examination and presentation of digital evidence, in order to have standards and procedures compatible with the best practices recognized internationally” (COE, 2011, 109). Furthermore, it is good practice to “create a harmonised set of rules for police and judicial record-keeping and appropriate tools for statistical analysis of computer crime” (ENISA, 2016, 33). The lack of such records is a major challenge and barrier to the organisation or redistribution of resources effectively.

Notably, ENISA states the same need in respect to judicial authority staff. For example, the agency suggests that it would be beneficial to conduct comparative analysis of the requirements for digital evidence at the national level, identify “what mechanisms (digital signature) are present or used within each Member State to verify authenticity of evidence” (75). They further note that this type of information would be beneficial in establishing good practice mechanisms that ensure the usability of such information by CSIRTs in legal proceedings (ENISA, 2012). The agency also notes the need for training between law enforcement and CSIRTs, including modules on how these stakeholders could work better together, where enhanced cooperation between these parties can lead to improved outcomes for both agencies. The cooperation between GovCERT.nl and the High Tech Crime Unit on the Taurus Botnet Monitoring Project has been provided as an example, albeit from 2012 (ENISA, 2012b). The importance of these relationships is noted in the National Cyber Security Strategy 2019-2024. In particular, the NCSC and GNCCB currently share training and use a co-location model where Garda members are seconded to the NCSC. However, it should be noted such aspirations as set out in the strategy require resources and funding. Without these the impact will be limited (Yar and Steinmetz, 2019; Wall, 2007). As it is, the representatives from An Garda Síochána noted that it will be a significant resource burden on An Garda Síochána to second an officer to the NCSC (Representatives from An Garda Síochána, interview, January 2020).

4.2.4 Diversion

Knowledge of alternative paths away from crime can be key to making the right choices. The UK’s National Crime Agency (NCA) reviewed pathways into and out of cybercrime based on their database of offenders, with the aim of diverting younger people to more productive avenues in which they can develop and explore their interest in computing. Although their sample was limited, as it could only use the data from those caught and available to them, they presented some interesting points and recommendations around cease and desist visits. However, there are a number of limitations in relation to this piece of work and similar work. Firstly, the NCA reportedly paid particular focus on autism, without a significant empirical basis for the claims they made about or the allusions to predispositions, which is potentially harmful in itself. This is likely to be linked to the lack of external scrutiny and/or academic oversight of the project. Secondly, it is framed around a prevent model that mimics the ideals of prevent proposed in the Counter terrorism strategy, which is a highly critiqued and controversial policy in the UK. This approach is often criticised for lack of objectivity or scrutiny. Consideration of joint research between academics and operational organisations may have helped reduce the impact of such criticism. Academic insights can help in increasing rigour and objectivity. It might be beneficial in the case of Ireland to look to joint research projects to mitigate such criticism if research in this area is considered.

4.3 Target Hardening

In contrast to raising awareness, target hardening is largely about strengthening security to protect against a crime. In terms of cybercrime, target hardening is often referred to as cyber resilience. Such models include those which involve enhancing cybersecurity measures and raising cyber resilience. This section considers good practice cybersecurity efforts from the perspective of fighting cybercrime. As defined by Coventry, Briggs, Blythe & Tran (2012) cybersecurity is “the protection of globally connected electronic data or equipment against criminal, unauthorized or accidental use and the technology and processes required to achieve this protection prevent cybercrime” (p 4).

4.3.1 ENHANCING CYBERSECURITY AND CYBER RESILIENCE TO COMBAT CYBERCRIME

At the individual level, much of the research in relation to good practice prevention measures relates to individual or organisational routine practices. By way of example, resilience building efforts of the NCSC also help to ensure cybercrimes are prevented and cybercrime actors are thwarted in their activities at a structural level in order to ensure a national level of resilience to mitigate against risk and enhance cyber resilience. Removing the opportunity for cyber criminals significantly inhibits their ability to operate effectively, thereby reducing the overall risk.

In the context of individual and organisational measures, Coventry, Briggs, Blythe, & Tran (2014) used behavioural insights to advise of ten best practices everyone should know and follow, namely (i) Use strong passwords and manage them securely; (ii) Use anti-virus software and firewalls; (iii) Always run the latest version of software; (iv) Log out of sites after you have finished and shut down your computer; (v) Use only trusted and secure connections, computers and devices (including Wi-Fi); (vi) Use only trusted and secure, sites and services; (vii) Try to avoid scams and phishing; (viii) Always opt to provide the minimal amount of personal information needed for any online interaction and keep your identity protected; (ix) Be aware of your physical surroundings when online; and (x) Report cybercrimes and criminals to the authorities. These examples solely provide an indication of the types of cyber safety measures that individuals can often pursue to enhance their own personal cybersecurity, thus enhancing overall cyber resilience which can partially help to prevent cybercrime. Two-factor authentication is also another highly recommended practice that individuals can take to increase their resilience.

Law enforcement and policy-makers in Ireland can thus continue their ongoing efforts to raise the level of cyber hygiene, as part of the response and mitigation efforts in the fight against cybercrime. However, as exemplified by more proactive steps taken by the UK Government, there is a shift in also moving the burden of responsibility towards Internet companies. For example, a recent Online Harms White Paper extends responsibilities for companies whose services are used for illegal activity. While this does not directly relate to cyber-dependent crimes, it shows that increased responsibility is likely to be expected of Internet companies.

From an organisational perspective, Epps (2017) states that organisations must move beyond simple password protection to stronger authentication, such as using a combination of cards, tokens and biometrics. Epps (2017) suggests that organisations “take advantage of the improved convenience of a mobile strong authentication model” (14). He also recommends that organisations “employ a layered IT security strategy that ensures appropriate risk mitigation levels” (Epps, 2017, 14). Ross (2018) echoes similar advice, especially in the context of increased remote working, noting that in such an environment risks are inevitable.[18] In that vein, Ross (2018) highlights as a good practice the need to educate to ensure people do not work around the security measures in place, but rather understand and adhere to them. Therefore, he contends that all employees should know and understand the potential threat they could be exposed to, and know what to do if they are exposed. Ross (2018) frames this good practice under the theme of developing a security culture within organisations. He suggests that organisations develop a strong security culture that defines how security influences the work conducted by the organisation, its products and services (Ross, 2018).

[18] This has been exemplified of late, in the context of COVID 19 and increased remote working.

However, Stanton et al (2016) highlighted a recognised problem of security fatigue, where employee’s work lives are negatively impacted by enhanced security measures, resulting in reduced compliance, thereby increasing the risk. As a result, it is important to understand how staff members may perceive and interact with polices and processes in this area. A representative from a corporate consultancy firm, based on experience working directly with clients, noted that it was beneficial to make the content resonate personally with employees, as much of the same lessons they learn to protect themselves are transferable to their workplace. Furthermore, they added that it was important to offer awareness training and support, at the department level, not just the organisational level, as a department risk exposure can differ greatly from one to another even within the same company. Departments such as Human Resources and Finance, and Board Members are often more actively targeted (Representative from a corporate consultancy firm, interview, February, 2020). In having a multi-layered approach, employees can better understand the relevance of mitigation measures discussed, increasing the likelihood of compliance (Representative from a corporate consultancy firm, interview, February, 2020).

Ross (2018) argues that education alone is not enough. He suggests the need for a technical component, to ensure a layered approach, which includes elements such as device authentication, data encryption and the ability to remotely wipe data from devices, if they are lost or stolen. Ross (2018) also highlights the importance of backing up data regularly. That said, Shah, Jones, & Choudrie (2019) find that even though cybercrime is quickly evolving and increasing, businesses have been slow to implement such prevention strategies. This is echoed in an Irish context, where, for instance, research conducted on behalf of Microsoft finds that poor, inconsistent security polices, practices and procedures were reported by employees across large and medium organisations in the country (Amárach Research, 2019). This lack of implementation of good practice is occurring despite an increase in cybercrimes in Ireland. The National Cyber Strategy states that “despite an increased level of awareness, Cyber Crime incidents in Ireland are increasing with 61% of Irish organisations reported to have suffered cybercrime such as Fraud in the last two years with an estimated loss on average of €3.1m” (Government of Ireland, 2019, p 18) – note that fraud is not considered to be a cyber-dependent crime for the purposes of this report. Further research would be beneficial to determine why this is the case, and to what extent it cuts across the public, private and voluntary sectors.

Nonetheless, many companies in Ireland do take prevention seriously, driven largely by two motivations. The first being compliance or regulatory related and the second prevention related. While many companies are mindful of audits by organisations such as the Data Protection Commission, the Central Bank and/or the NCSC, in line with the NIS

Directive, they also go to extraordinary lengths to prevent against attacks to ensure they can maintain their services and protect their customers (Representative from a corporate consultancy firm, interview, February, 2020).

Implementing such high standards of security from the bottom up level of individuals and organisations, right up to the state level, help in reducing the collective risk. The NIS Directive notes, for example, the inconsistencies across Member States' level of security of network and information systems, and states that "an unequal level of protection of consumers and businesses…undermines the overall level of security of network and information systems within the Union". Support is needed to ensure a minimum level of cybersecurity. One example of how Ireland is trying to increase the level of protection across Irish business, is evident in the NCSC's document titled '12 Steps to Cyber Security - Guidance on Cyber Security for Irish Business'. This document sets out a suggested activity plan that business can implement on a month-by-month basis over a 12 month period to improve their cyber resilience (NCSC, 2018).

Two further examples of this are evident in the UK. The British Government has developed the Cyber Essentials and Cyber Essential Certification schemes to provide such support. These schemes are provided online by the UK's National Cyber Security Centre. The Cyber Essentials scheme provides advice under five controls that can be immediately put in place to take the first steps to implement cybersecurity (UK NCSC Website). While the Cyber Essential Certification is the next step under this scheme, businesses are informed about the protections they need to have in place. Once these are in place, an independent body assesses the company's cyber security systems and provides independent verification (UK NCSC Website). All organisations who want to be government contractors must have this certification. Furthermore, the companies who complete this scheme get public recognition for the standard of security they achieve. This complements the Cyber Growth Partnership, which is a joint industry and Government group, co-chaired by the Minister for Culture and The Digital Economy and the CEO of BT Group. The partnership was established to support the growth of the UK cybersecurity industry (Cyber Essentials Website, 2020).

The ENISA's report on 'NCSS Good Practice Guide, Designing and Implementing National Cyber Security Strategies' (2016) also analyses good practice in the area of prevention at these levels. For instance, good practice recommendations that specifically relate to providing "incentives for the private sector to invest in security measures" (39). In addition to legislative solutions such as the GDPR that mandates businesses to maintain certain standards in relation to data protection, ENISA (2016) notes that countries can also apply softer approaches to incentivise industry to invest in security measures. Two examples of this are evident in the UK. In Scotland the Scottish Council for Voluntary Organisations (SCVO), with support from the Government, provides a small grant scheme to enable third sector organisations to achieve the Cyber Essentials accreditation, discussed above. While Innovate UK, with equal funding from the Department for Culture, Media and Sport, provide businesses with Cyber Security Innovation Vouchers worth up to £5,000 to implement the required cybersecurity and resilience measures. Other schemes may come in the form of tax breaks or financial subsidies. ENISA highlights Finnish solutions as examples of good practice in this area, where direct action by industry against computer-related crime is encouraged. However, such approaches also have to be managed and well thought through given the potential risks associated with promoting vigilantism.

Other good practices suggested by ENISA include risk assessments, which should ideally be included under national cybersecurity strategies and conducted at the national state level (ENISA, 2016). ENISA (2016) states that "risk assessments can provide valuable information for developing, executing and evaluating a strategy. The assessment can be conducted on different levels. Risks assessment on a national level allows gaining a holistic understanding about risks to the nation as a whole" (15). The EU agency identifies models in Switzerland and Spain which exemplify good practice in this area. ENISA suggests that typical tasks to consider when conducting risk assessments include:

- Agree on a risk assessment methodology to use; if this is not possible, tailor an existing one to the specific needs of national and to specific sector risks.
- Task a national authority or sector-specific authorities with conducting risk assessment.
- Design and follow an approach to risk identification and assessment (e.g. all-hazard approach).
- Develop a method for the identification of critical (information) infrastructure (ENISA, 2016, 16).

The results of such assessments provide insights into key areas that need to be targeted to reduce the level of risk exposure, thereby prioritising areas where preventative activities may be worthwhile. A higher level response is then required to respond to the issues raised in such assessment, especially if carried out at the national level.

4.4 Situational Prevention

Situational crime prevention aims to reduce the harms caused by crime by changing situational factors in the environments where such crime occurs. In the context of cybercrime, this involves creating an environment less conducive to cybercrime. Good practices in this context that are considered in this report include the introduction of dedicated strategies, investment and improvement in detection and related forensics, and cross collaborative effort. These will be discussed in detail below.

4.4.1 NATIONAL CYBERCRIME STRATEGY

In broad terms, the existence of a national cybersecurity strategy alone may not be enough in the context of cybercrime specifically, including the Irish National Cyber Security Strategy of 2019. A national cybersecurity strategy does not necessarily replace the need for a cybercrime strategy. As asserted by Seger (2012), cybercrime strategies can instead outline activities to directly and indirectly deal with cybercrime, such as crime prevention and criminal justice policies, programmes, and practices.

The United Kingdom's Home Office Cybercrime Strategy (2010) is an example of this approach. The cybercrime strategy was published in 2010 - the year after the first UK Cyber Security Strategy was published. As the lead government department in the United Kingdom responsible for developing policies to counter cybercrime, the Home Office developed the Cyber Crime Strategy, which sets out the Department's plan for coordinating and delivering that policy (Home Office Cybercrime Strategy, 2010). The logic of having a strategy or plan is recognised good practice for governments and organisations as they provide a roadmap for activities that help achieve the goals set by them. They guide discussions and decision making, as well as help to establish the resources and budgets that may be required. Having such a structured approach to cybercrime is hugely important, where, for instance, Prof. Wall notes that a good practice in and of itself is to have a clear methodological approach that could be laid out in a strategy. He highlights the '4Ps' approach used in the UK Counter Terrorism Strategy, namely, 'Prevent, Pursue, Protect and Prepare' as a good example of a methodological approach which specifically highlights different approaches to a problem. While this strategy has been highly criticised, it is the strategy's methodological approach that Prof. Wall suggests could have value if applied to cybercrime because it targets multiple phases (before, during and after the crime happens) and also helps to mitigate cybercrime in the first place.

A contrasting approach is evident in Scotland. The Scottish Government opted to develop strategies across different areas of cybersecurity to address different sectors and activities required, including a strategy to address the necessary learning required to foster a successful cybersecurity ecosystem and promote business. At the heart of these strategies is the ideal of creating a safe and prosperous digital economy. The representatives from An Garda Síochána highlighted the benefits of having a dedicated strategy in this area, but noted the importance of having a whole of government approach to the activities contained within. Notably, while the UK has published a number of cybersecurity strategies, the 2010 cybercrime strategy has been since updated.

4.4.2 INCREASE DETECTION AND FORENSIC CAPABILITIES

Creating an environment less conducive to cybercrime requires the capabilities to respond if and when such crimes occur. In the context of responding to and prosecuting cybercrime strong capabilities in the area of digital forensics are important. However, cases may not even get this far, due to the nature of cybercrime. For example, IoT and other new technologies and tactics that often offer anonymity to users, are very advantageous for criminals, and a significant challenge for prosecution. As noted by Clough (2015), offenders may deliberately conceal their identity online by the use of proxy servers, spoofed email or Internet protocol (IP) addresses. Simply opening an email account which does not require identity verification provides a false identity. Confidentiality may be protected by the use of readily available encryption technology, while traces of digital evidence may be removed using commercially available software. The networked nature of modern communications means that data will routinely be routed through a number of jurisdictions before reaching its destination, making tracing of communications extremely difficult and time sensitive. Accessing wireless networks, with or without authorisation, may conceal the identity of the actual user even if the location can be identified. Data may be stored deliberately in jurisdictions where regulation and oversight is lax.

The 2017 EU Cyber Strategy notes this ongoing challenge, raising the concern that in order to increase the chances of bringing perpetrators to justice, there is an urgent need to improve capacity to identify those responsible for cyber attacks. Finding useful information for cybercrime investigations, mostly in the form of digital traces, is a major challenge for law enforcement authorities. The strategy therefore recommends increasing technological capability to investigate effectively including by reinforcing Europol's cybercrime unit with cyber experts. All those interviewed highlighted the exceptional work carried out by Europol, more specifically EC3, in this area. (Interviews, December 2019 and January 2020).

Europe has become a key actor in supporting Member States' multi-jurisdictional investigations. The strategy calls for EC3 to become a centre of expertise for Member States' law enforcement on online investigations and cyber forensics. The widespread practice of placing multiple of users – sometimes thousands of them – behind one IP address makes it technically very difficult to investigate malicious online behaviour. It also makes it sometimes necessary, for example for serious crime such as child sexual abuse, to investigate large number of users in order to identify one malicious actor. The EU will therefore encourage the uptake of the new protocol (IPv6) as it allows the allocation of a single user per IP address, thus bringing clear benefits to law enforcement and cybersecurity investigations. As a first step to encourage uptake, the Commission will mainstream the requirement to move to IPv6 throughout its policies, including requirements in procurement, project and research funding as well as supporting the necessary training materials. In addition, it advises that Member States should consider voluntary agreements with Internet Service Providers to drive the take up of IPv6.

The Commission also included the results of reflections on the role of encryption in criminal investigations in October 2017 in the 'Eleventh progress report towards an effective and genuine Security Union'. This set out actions to support both law enforcement and judicial authorities when encryption is encountered in criminal investigations. Lastly, the NIS Directive notes that "[u]niversities and research centres have a decisive role to play in spurring research, development and innovation in those areas" (Directive (EU) 2016/1148, 194/2).

4.4.3 CROSS COLLABORATION

The development of collaborative partnerships between many actors and communities both nationally and internationally is key to developing resilience against cybercrime (ENISA, 2016). As a result, they can plan a significant role in situational prevention. EU law enforcement equally highlight how such partnerships are important especially in the context of cybercrime (EUROPOL & EUROJUST, 2019). Beyond owning the infrastructure as is the case in the Irish context, EUROPOL & EUROJUST (2019) specify that these entities also hold much of the evidence that may be required in prosecutions. Given the range of actors this may involve, ENISA (2012) notes that it is good practice to build a common consensus as to what constitutes a cyber-incident given the range of stakeholders involved. Furthermore, ENISA documents state that it is good practice to "establish cooperation between public and private sector stakeholders to quickly identify and respond to cybercrime related issues" (33). To develop this further, ENISA (2012) states that countries should establish "core competencies and indications of each stakeholder's competencies, capabilities and procedures" (3). This assists in understanding the range of competencies and capabilities available within stakeholder groups. This resonates with the suggestion of the representative from the corporate consultancy firm who, as discussed above, made the suggestion of building a reserve body construct, where all available skills and experience of stakeholders are mapped out

(Interview, February 2020) ENISA further highlights in respect to cybercrime specifically, the need for stakeholders to "develop knowledge and expertise on emerging cybercrime-related threats and vulnerabilities but also attack methods through information sharing at national and international levels" (ENISA, 2016, 33). This clearly illustrates that in order to be able to respond to cybercrime effectively, a high degree of knowledge about the broader cybersecurity environment is required. Two keys areas of collaboration discussed below include: (1) Law Enforcement Collaboration with Government Stakeholders; and (2) International cooperation between law enforcement agencies.

4.4.3.1 Law enforcement collaboration with non-governmental stakeholders

Europol, through the EC3, works very hard in this area, and the EU law enforcement agency has actively created a multifaceted approach, built around public and private resources. Despite the fact that much of their work deals with investigations, they are cognisant of the need to look beyond this in relation to their connections and network (Europol representative, interview, December 2019). Through their public private partnerships, Europol is setting standards, in the context of best practices, as evident in their three Advisory Groups for Internet Security, Financial Services, and Communication Providers.

EC3 hosts the Joint Cybercrime Action Taskforce (J-CAT)[19]. Its mission is to proactively drive intelligence-led, coordinated action against key cybercrime threats and top targets through cross-border investigations and operations by its partners. J-CAT facilitates the joint identification, prioritisation, preparation, initiation and execution of cross-border investigations by its partners. While such groups and networks help on a day to day basis, they also help in ensuring a more hostile environment for cybercriminals. The establishment of such networks is also in line with ENISA's (2016) advice that there is a need develop such forums, to improve and enhance cooperation between various stakeholders dealing with cybercrime, that goes beyond official stakeholders.

Much effort has gone into making these groups effective and efficient by Europol and partners. In an interview, a Europol representative suggested that the success of these groups is probably on account of Europol acting as the coordinating body within the established framework both legally and in terms of secure infrastructure and partnership networks but also due to the effectiveness of the joint approach which is clearly evident to all involved. Interestingly, some of the representatives of financial institutions noted

[19] See https://www.europol.europa.eu/activities-services/services-support/joint-cybercrime-action-taskforce

that they believed their lack of brand strength, in this area, limited their ability to gain traction on some of their own campaign material thereby reducing their reach (Representatives from financial institutions, interview, January 2020).

The strength of the partnership between EC3 and stakeholders is not by chance. All partners within the Europol advisory groups have clearly defined roles, work plans are agreed and collectively set, which require input by all. The majority of partners are reportedly very active, which is welcomed by Europol. Cooperation is also based around a high degree of trust between partners which is paramount in areas of security and crime that are traditionally dealt with in a more closed and secretive manner given sensitivities and security concerns. One example of a worthwhile campaign illustrating the value of this partnership is the ‘No More Ransom’ campaign. This is a collaboration between Dutch police, Europol and private security companies, which provides information on how mitigate the risk of being targeted and how to report such cases, if they occur. Where possible, they also provide victims who have been targeted with decryption keys for ransomware. A competent, speedy response to ransomware demands is critical for businesses, as an attack can be detrimental to their business (Representative from a corporate consultancy firm, interview, February 2020).

Building a high level of trust has provided an environment where partners are willing to talk about important issues as they feel comfortable to exchange relevant information (Europol representative, interview, December 2019). The importance of trust was also highlighted in all the interviews in Ireland, in relation to such partnerships (Interviews, December-February 2020). Establishing confidentiality for businesses has also been a key activity for the UK NCSC, which views this as a method of bringing business on board in relation to their work. Interestingly, the representative from Europol highlighted that while for many companies the relationships may start out due to corporate social responsibility and the positive PR, the majority of these stakeholders quickly see greater benefits in sharing experience, training and expertise.The experience of enhanced benefits of such partnerships is in line with the literature. For example, IPerez-Gonzalez, Trigueros Preciado and Solana-Gonzalez (2014) interestingly in their research that information security knowledge sharing has a positive impact on management performance.

Another beneficial aspect of these relationships, while not good practice itself but could help to enable good practice, is that such networks provide quick access to skills and expertise that may not be available to an organisation. This was confirmed by representatives from An Garda Síochána, the NCA and the financial institutions in the interviews. It was suggested that investigators while experts in their own right, are rarely as proficient as dedicated IT experts, which means that building relationships and knowledge exchange is very effective (Europol representative, interview, December

2019). This observation was also highlighted by a representative from the United Kingdom's National Crime Agency, who noted that training - while important - dates quickly, and therefore the most important thing for investigators is to have access to a network of people that they can reach out to when needed (Interview, 2019).

Nonetheless, there is much literature on the difficulties associated with developing public private partnerships in this space. For example, Carr (2016) noted that despite the central positioning of public–private partnership in both UK and USA strategies, such agreement are often nebulous. Carr's (2016) research found that there is often a serious disjuncture in expectations from governments and the private sector. She (Carr) noted that governments often view privately owned and operated critical infrastructure as a key element of national security, while at the same time can be reluctant to exert a mandate to ensure and oversee network security. In contrast, the private sector often does not want to see or accept their potential role or liability for national cybersecurity. Therefore, there is a real need to manage expectations, balance public versus private interests and navigate different understandings of the same threat. The representatives from BPFI, the financial institutions and An Garda Síochána all noted that this was a problem they had, on occasion, encountered. When such crimes happen the priority for businesses is largely remediation and recovery, then compliance. It is only afterwards that investigation for the purpose of criminal investigation becomes important. This illustrates some of the competing interests that can occur during and after such a crime such as concerns about getting a business back up and running, or a fear of fines where regulations are not complied with. Competing obligations are also evident in relation to reporting. For example, the need to report certain incidents both to the NCSC and An Garda Síochána. The former to ensure corrective action can be taken and to reduce the risk, and the latter to ensure the incident is criminally investigated.

Unlike traditional crime where the majority of crimes are investigated solely by law enforcement agencies, cybercrime is slightly different. Investigations are often conducted by private sector bodies initially to assess whether a crime has happened at all, prior to reporting to law enforcement. For example, the representative from a corporate consultancy firm noted that when they are doing incident response for a client, or where a client may be unsure as to whether an attack has occurred, they are often called in to investigate (Interview, February 2020). In doing so, they look to see what type of incident it might be, a simple, non-issue, or criminal, to name a few. At this point, their investigation is largely focused on the source of attack, stopping it, and getting business back up and running and protected. If, during this process, a potential crime is detected, it is reported to law enforcement. Law enforcement often approve the organisation to continue with their investigation, so they can protect their client from further attack (Representative from the corporate consultancy firm, Interview 2020).

Furthermore, developing relationships with Internet service providers, as currently undertaken by An Garda Síochána, may be beneficial, as law enforcement are often hugely dependent on ISPs for their work. Such relationships have proved effective for Europol in the investigation into Imminent Monitor Remote Access Trojan (IM-RAT) as noted above. That said, as noted in the interviews this would be most beneficial if enhanced by the development of a clear legal framework within which all parties can work with and cooperate around. Having this in place would be essential for ensuring investigative success, and clear boundaries for all involved. The importance of these relationships is highlighted in the research by Boes & Leukfeldt (2017). Their work explores the need for such partnerships in the context of overcoming the difficulties the police have in fighting cybercrime. Therefore, greater cooperation and collaboration between the ISPs and other private organisations should also be encouraged in the Irish context. That said, and as highlighted by the financial institutions, BPFI, and An Garda Síochána representative, relationships with the ISPs in Ireland are improving (Interviews, December 2019 and January 2020). One example of this is evident in the bi-annual meeting between BPFI and the Irish Telecommunications Security Fraud Forum (Representative from BPFI, interview, January 2020). It was highlighted in some of the interviews that such relationships were much more robust in the UK (Representatives from the Financial Institutions, interviews, January 2020). It might be worth exploring further why this is the case, for potential lessons to be learned for further development of these relationships in Ireland. The importance of public private partnerships and relationship building will be discussed in more detail later in this section.

In short, the representatives from An Garda Síochána (from the perspective of law enforcement tasked to counter cybercrime) noted that more formal and coordinated approaches to cyber in Ireland are badly needed, as there are currently none in place, while at the same time stating that people are just doing their best. In this regard, they (An Garda Síochána) highlighted the need for a whole of government approach, one that is fully resourced and has a multi-agency approach, between government departments and key stakeholders.

4.4.3.2 International cooperation between law enforcement agencies

In terms of international cooperation among LEAs, Europol's structure is such that it includes representatives from all EU Member States, which makes cooperation at this level more accessible. However, this is further enhanced by the co-location of representatives from third-party countries that have an operational or strategic agreement with Europol such as, among others, the U.S., New Zealand, Australia, and Canada at

Europol's HQ (Europol representative, interview, December 2019). Responses should be coordinated between relevant stakeholders (ENISA, 2016). An example of this recommendation in practice is EC3, which was established in 2013 to strengthen the law enforcement responses to cybercrime in the EU. EC3 has two forensic teams, namely digital forensics and document forensics. Each provides operational support as well as research and development. The unit also includes two strategic teams. The forensics team conducts outreach and provides support, "which establishes partnerships and coordinates prevention and awareness measures" and the second conducts "strategy and development, which is responsible for: strategic analysis; the formulation of policy and legislative measures; [and] the development of standardised training" (European Cyber Crime Centre, 2019).

The UK's NCA is also highlighted as a very good model of law enforcement collaboration which links broader national policing investigations (such as with cybercrime) with local forces via a Regional Organised Crime Unit (ROCU) (Prof. Wall, interview, December 2019). The agency not only works closely with UK police and regional organised crime units, but it also works with international law enforcement such as Europol and the FBI, both in sharing intelligence and coordinated action. (NCA, 2020). This was also confirmed by An Garda Síochána in the interviews. The agency also actively works to develop effective partnerships and work closely with private industry to share information and technical expertise. The representative from the NCA also noted the very good relationships between law enforcement within the EU. Responses are quick and competent for the most part, especially where there are lives at stake. For example, a number of cases of suicide have been associated with cybercrime, and there has been good cooperation in these instances.

However, the NCA representative noted that cooperation can be difficult outside the EU. As a result, the NCA takes on an active role to educate lead officers that the infrastructure they have at their disposal may not be the same elsewhere, and they therefore need to manage expectation. In short, responses can differ access jurisdictions, resources can differ, and even issues of concern that are pertinent in one jurisdiction may not be the same in another (NCA representative, interview, December 2019). For these reasons, cyber capacity building on different measures in the fight against cybercrime is important for national and collective cyber resilience in relation to growing cybercrime levels. In the context of Ireland, the National Cyber Security Strategy released in 2019 states that Government goals now include "engaging in sustainable capacity building in third countries". With specific reference to cybercrime, the Irish government will "support international cooperation to combat cybercrime and promote formal and informal cooperation in cyberspace, including by engaging in sustainable capacity building in third countries” (p.4). While this is a step in the right direction as well as in Ireland’s national interest to reduce the impact of cybercrime in the country, government stakeholders must either establish or support programmes that will certainly have impact by drawing on past lessons and good practice for effective cyber capacity building related to cybercrime questions. A number of global initiatives are already making progress on cyber capacity building questions specifically related to cybercrime such as the Global Forum on Cyber Expertise (GFCE).

In an interview in Eolas Magazine in 2017, Detective Superintendent Gubbins (then head of the GNCCB), noted that An Garda Síochána follow these practices of collaboration with international law enforcement. He then explained that “EC3, for us as a small country, is a valuable entity. We send them a lot of information and intelligence which they then analyse for us within a bigger picture”, thus acknowledging the value that international cooperation provides for the Irish cybercrime unit and An Garda Síochána. He also noted in the same interview that, in line with good practices mentioned above, senior Gardaí engage with a wide range of stakeholders in this area. In particular, “our main business partner would be Banking and Payments Federation Ireland (BPFI) and once a month we meet under what’s known as the High-Tech Crime Forum. We meet with all the banks, our colleagues in the Police Service of Northern Ireland (PSNI), the Internet Service Providers Association of Ireland and others from the UCD Centre for Cybersecurity and Cybercrime Investigation and exchange information about what trends we observe in the cybercrime sphere. It’s been quite successful” (Eolas, 2017). He also noted that through “the European Cybercrime Centre, the Garda also have relationships with Europol, Interpol and other law enforcement partners across the world. The Modernisation and Renewal Programme outlined that “specialist units will be set up to liaise with international partners on current and emerging threats, and to provide cyber and forensic tools to support frontline policing and State security” (Eolas, 2017).

4.4.4 CONDUCTING EXERCISES

Another good practice referenced within the NIS Directive that can help strengthen the capacity of those involved in the fight against cybercrime relates to exercises. The Directive states that “exercises which simulate real-time incident scenarios are essential for testing Member States' preparedness and cooperation regarding the security of network and information systems. The CyberEurope cycle of exercises coordinated by ENISA with the participation of the Member States is a useful tool for testing and drawing up recommendations on how incident-handling at Union level should improve over time” (194/7). ENISA’s (2016) states that such “exercises enable competent authorities to test existing emergency plans, targets specific weaknesses, increase cooperation between different sectors, identify inter-dependents, stimulate improvements in continuity planning” (25).

4.4.5 PREVENTION BY DESIGN

Implementation of a code of ‘security by design’ has been implemented by some technology companies in their design and innovation strategies to ensure products come to market with a basic standard of in-built security. The UK government's Code of Practice for Consumer Internet of Things (IoT) Security for manufacturers, with guidance for consumers on smart devices at home is a good example of what this could look like. It also supports increasing the responsibility of tech and Internet companies for building security into their products.

4.5 The ‘balance’ between tackling cybercrime and protecting individual rights

The Budapest Convention acknowledges that achieving the right balance between tackling cybercrime and protecting individual rights is an important factor (Preamble). It further recognises the need to be mindful of ensuring a proper balance between the interests of law enforcement and respect for fundamental human rights. These rights are important given that they include, but are not limited to, the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, as well as rights concerning the respect for privacy and the right to the protection of personal data. The NIS Directive similarly includes reference to rights, stating that it “respects the fundamental rights, and observes the principles, recognised by the Charter of Fundamental Rights of the European Union, in particular the right to respect for private life and communications, the protection of personal data, the freedom to conduct a business, the right to property, the right to an effective remedy before a court and the right to be heard” (Directive (EU) 2016/1148, 194/11). It further notes that the Directive should be implemented at national level in accordance with those rights and principles.

Despite inclusion of safeguards provided under national and international laws, early critics of the Budapest Convention stated that it was not properly balanced between the fight against cybercrime vis-à-vis respecting fundamental rights (Taylor, 2001). In fact, Taylor purports that the Convention is fundamentally imbalanced, providing considerable detail on powers of search and surveillance, with no detailed description of how countries should go about protecting rights and restricting government authority. A suggestion of how this could have been overcome was the inclusion of limitations on the use of certain techniques in each section referencing to powers and authority (Taylor, 2001). One specific example of where the Convention illustrates imbalance, as Taylor suggests, relates to encryption. Taylor notes that countries like Singapore, Malaysia, India and the UK transposed Clause 4 of Article 19, Search and Seizure of stored computer data, into law - this provides for the power to force users to provide encryption keys (in some cases, with the power to fine or imprison those who do not). Taylor (2001) highlights one specific concern in this regard, contending that this application raises issues about the right against self-incrimination in certain jurisdictions.

While many of Taylor's criticisms remain, some additional protections have been implemented since the Convention was agreed, especially in the EU. For example, the overturning of the Data Retention Directive (DRD) by the European Court of Justice clearly demonstrated that the EU was not afraid to step in to ensure balance, albeit knowing that in doing so it would make it difficult for law enforcement and prosecutors to obtain data from private companies (EUROPOL & EUROJUST, 2019). Secondly, GDPR has provided much needed protection relating to personal data.

Drewer and Ellermann (2012) note that full compliance with data protection regulations and principles is an asset in regard to preventing and responding to cybercrime. A tangible example of how the EU is trying to implement this and move beyond safeguards in the Convention to operational activities is illustrated by the work of EC3. The approach of Europol includes protocols for independent data protection supervision, secure information exchange capabilities, data protection, compliant outreach to the private sector and clearly defined purpose specifications for processing personal data on their data sets (Drewer & Ellermann, 2012). This allows EC3 to support EU Member States in tackling cybercrime, while protecting individuals' rights. This approach has been implemented in the Europol Platform for Experts, which was launched to facilitate the exchange of best practice and to share tools, tactics and techniques. The success of this approach is demonstrated regularly. For example, in November 2017, where EC3, the FBI, Joint Cybercrime Action Taskforce (J-CAT), EUROJUST and private sector partners dismantled one of the longest running botnets, the Andremeda botnet. While, more recently, in November 2019, an international investigation into Imminent Monitor Remote Access Trojan (IM-RAT) spyware took place, led by the Australian Federal Police (AFP), with international activity coordinated by Europol and Eurojust. This operation involved numerous judicial and law enforcement agencies in Europe, Colombia and Australia. The cross-border interaction was supported on law enforcement level through the J-CAT and on judicial level through the European Judicial Cybercrime Network (EJCN).The operation ended the availability of this tool, which was being use by actors in 124 countries.

There is a perception that perfect privacy may provide offenders with the ability to commit crime undetected as it will not allow law enforcement fully investigate cases. However, providing backdoors in encryption for law enforcement may push offenders to services without such backdoors, making them harder to reach, whilst potentially weakening the security on systems that do have the backdoors. Raab et al (2015), although writing in the context of surveillance, claim that if introduced in the name of greater security, surveillance may have the opposite effect, and in fact erode social freedoms and public goods such as privacy. Therefore, it is important to have these discussions when new legislation is being proposed in order to work towards an appropriate balance between privacy, security and safety discussions (Europol Representative, interview, December 2019).

Supported by the literature, Hildebrant (2013) contends that balancing these two complex issues does not have to involve a sacrifice of liberties for the sake of increased security. He notes that where security measures are implemented that violate our liberties and rights, extra safeguards must be put in place to ensure balance. This requires specificity, not just a statement of intent, as is the criticism of Taylor (2001) on the Convention. To further address the need for balance, Hildebrant (2013) claims that a more generic understanding of the right to privacy is required. He presents Rothenberg's definition as a step in the right direction. Rothenberg defines the right to privacy as 'the freedom from unreasonable constraints on the construction of ones identities" (Taylor, 2012, 377). In this context, Hildebrant (2012) suggests that it is not a question of a trade-off between security and privacy, although this notion along with balance are integrated into the Convention, rather he contends that there can be "no trade off without balance" (357). Moreover, Drewer and Ellermann (2012) argue that "high data protection standards lead to high quality of data which itself is a precondition for high quality crime analysis" (394). Therefore, better adherence to protection of rights can only help in tackling cybercrime.

ENISA (2016) echoes such sentiments that it is good practice to balance security with privacy and data protection. It notes that any national cybersecurity strategy should try to achieve a good balance between these two goals, identifying a number of specific tasks to consider, such as:

- "Take into account national legal requirements for data protection when drafting cyber security relevant regulatory texts.
- Take the advice of the data protection authority(ies) on regulatory texts related to cyber security.

- Consider data protection law compliance measures when consulting the minimum security measures
- Make data protection supervisory authority(ies) part of information security compliance audits to the most critical stakeholders.
- Support and brand, together with the national data protection authority(ies), the European Data Protection Day (January 28).
- Involve national data protection authority(ies) in national cyber exercises, if the scenario is relevant to data protection issues" (ENISA, 2016, 36-37).

The Irish national cybersecurity strategy includes the need to achieve such a balance and sets out in its Vision the need to "[p]rotect the State, its people and critical national infrastructure from threats in the cyber security realm in a dynamic and flexible manner, and in a way that fully respects the rights of individuals and proportionately balances risks and costs" (p.11). The first Irish cyber strategy notes the need for "open, free and safe access to cyberspace, and confidence that their personal data will be processed in accordance with data protection principles enshrined in law, notably national legislation, the European Union Treaties and the European Convention on Human Rights" (Department of Communication, Energy & Natural Resources, p.4).

An Garda Síochána also are mindful of the need to balance tackling cybercrime and protecting individual rights. This starts at the top of the organisation, set out in organisational HQ circulars, which set out the organisation policy, coupled with the organisational ethics code (Representative from An Garda Síochána, Interview, January 2020). Moreover, the GNCCB actively strive to protect privacy, especially as it pertains to understanding rights of access.

CONCLUSION: Key findings and reflections for policy and practice

This study examined the existing research literature on cybercrime (focusing in particular on cyber-dependent crime) including current and emerging threats, the Irish anti-cybercrime landscape and models of best practice for combatting cybercrime in order to inform both policy and practice across the criminal justice system in Ireland.

The report finds that there is no consensus for the term ‘cybercrime’. Rather, it is largely used to encompass a range of criminal activities that use ICTs. The lack of an agreed definition is not solely an academic disagreement or debate. In fact, many now concede that a definition is less important given the saturation of Internet-connected technologies in everyday life, and that as a result, much of all crime exists on a technological spectrum. Many nations do not adopt a statutory or case law definition of cybercrime, because requirements of definitions change depending on the purpose in which the definition is used. That said, given the EU’s desire to harmonise legislation, responses and standards in this area across Member States, any government policies should be mindful of using, at the very least, a shared understanding of terms within particular use cases.

Section Two notes that while contemporary cybercrime threats present new challenges, the perception that cybercrime activities are an entirely new problem is misplaced. Nonetheless, the threat landscape continues to evolve requiring a constant revision of responses at national and international level. The prevalence of cybercrime activity will likely often correlate with opportunities for these crimes to be conducted – and these opportunities are growing because of an increasing attack surface brought about by the growth of ICTs and new technologies. Wealthier nations with more Internet users per capita are also traditionally found to be subject to higher cybercrime activity, and in Ireland’s case, it is among the leading ranks of EU Member States in terms of the use of digital technologies.

Another factor for developed countries like Ireland is the impact of cross-border cybercrime activity from other countries that often account for more of the variation in cybercrime activity than others. UN experts note that different levels of capacity for ICT security among States can increase vulnerability in an interconnected world, especially where a lack of capacity can make the citizens and CI of a State vulnerable or make it an unwitting haven for malicious actors. This is one of the reasons why sustainable capacity building efforts in other parts of the world (as now identified in Ireland’s national cyber security strategy) are essential to reduce cybercrime activity in Ireland. This is particularly important for Ireland given that it may not only suffer the direct consequences of cybercrime, but because of its status as a location of choice for many global technology companies and other multinationals. This means that the country must have top-tier advanced cyber readiness capabilities and avoid the indirect consequences of cybercrime such as loss of confidence from outside investors.

Yet, it is difficult to measure both the direct and indirect consequences of cybercrime. And while cybercrime-related activities occur daily, they are often not reported to law enforcement for several reasons including broad uncertainty about the actual nature of cybercrime. Such under-reporting will likely limit the ability to create effective policy solutions, which means that efforts to increase the level of reporting in Ireland are likely needed as a first step. Of the few reports on cybercrime in Ireland, it is found that the numbers of those companies experiencing cybercrime has apparently grown in Ireland and it is double global levels despite increased levels of awareness and more resources being allocated to address risks. These increases in crime are explained to not only be a reflection of better detection methods, but also because more cybercrime is in fact being conducted.

The most significant cybercrime trends and threats in Europe currently include: (1) Ransomware; (2) Other malware threats; (3) Data breaches and network attacks; (4) Spearphishing; and (5) Attacks against critical infrastructure. In particular, the fallout from both the WannaCry and NotPetya ransomware attacks showed the ability of ransomware to spread globally at great speed, affecting targets indiscriminately. A second growing threat is mobile malware aided by the growing use of mobile phones and tablets. While mobile malware has not so far been extensively reported in Europe, there seems to be an ongoing lack of awareness in the general population about how to deal with mobile phone cyber incidents. Victims of mobile malware in Europe are more inclined to approach their provider rather than make police reports, and few will report to the police at all. This means that already low levels of reporting of cybercrime in Ireland is likely to be exacerbated by under-reporting in relation to mobile malware incidents.

Cryptomining presents new challenges because it is not illegal in some cases but it is still creating additional revenue and thus motivation for criminals to attack legitimate websites. It seems that damages to victims are broadly speaking difficult to quantify and investigate. This is a gap that should ideally be addressed in Ireland. Other trends that should ideally be considered by law enforcement and policy-makers involved in the fight against cybercrime include the growing connections between cybercrime and malevolent state activity; IoT/future cities and smart meters; cloud security; emerging technologies; third party vendor risks and supply chain attacks; wide public and commercial availability of tools and techniques as well as “Darknet” concerns; poor security cultures; the terrorist-cybercrime nexus; and pervasive anonymisation tools. From a criminal justice perspective, for example, countries like the United States are increasingly using criminal indictments for cases that involve state actors or state proxies as a deterrent for the perpetration of cybercrimes by state actors. Irish authorities may also need to assess the applicability and effectiveness of the domestic legal framework for state-sponsored cybercrime. In addition, there are concerns about the growing availability and use of publicly and commercially available cyber tools, exacerbated by the leaking and release of states’ tools and techniques. The entry barrier for criminals has apparently never been so low where many criminals are using legitimate and off-the-shelf tools or techniques. Anonymity provided through legitimate tools such as Bitcoin and cryptocurrencies that allow untraceable payments as well as Tor-like networks allowing communication and trade of both information and technologies is also described as one of the most important developments behind the recent “tectonic shift” in the threat landscape.

Lastly, cybercriminals will use simplistic methods, including targeting victims and countries with poor cybersecurity protections. This is why cybersecurity agencies like the NCSC in Ireland, through their advisories, and the NCSC in the United Kingdom are publicly communicating the risks so that there is a better level of security awareness and basic protections on an individual and entity level, thus enabling individuals to be better empowered to act on the information they are given in ways that they could not previously. This signals a shift in how cybercrime is approached in the United Kingdom through a culture of increasing openness – the extent of public advisories provided by the NCSC in the UK has been relatively more than most countries so far. The UK’s NCSC is releasing unprecedented levels of information and it has ambitions to continue declassifying much more information in a well-managed way to help the general public to be better prepared. These are the types of steps that could be considered in Ireland in order to more effectively combat modern cybercrime.

The third section of the report identifies key legislation including an assessment on its effectiveness. The key piece of Irish legislation is the Criminal Justice (Offences relating to Information Systems) Act of 2017 which amends previous Acts and gives effect to EU Directive 2013/40/EU on attacks against information systems. However, the codification of cybercrime still remains scattered across many Acts. Statutory Instrument No. 360 of 2018 signed the EU NIS Directive into Irish law and it represents a significant shift in approach towards a more formal type of regulatory relationship in certain key industries. The transposition into Irish law of regulatory instruments like the NIS Directive and GDPR means that Irish individuals and entities will now be accountable for not meeting compliance obligations. This means that preventative measures are now more likely to be introduced by organisations, thus driving better resilience in the wake of cybercrime - even though it may be too soon to gauge their effectiveness on crime prevention. While these measures primarily apply to OES and DSP, the 2017 EU cybersecurity strategy considers that a similar approach by all stakeholders hit by cyberattacks would be necessary to have a systematic assessment of vulnerabilities and entry points for cyber attackers. There is no specific criminal offence in Ireland for failing to implement cybersecurity measures within an organisation or as an individual.

Many countries, including Ireland, use a combination of old legislation (or at least not specifically developed to target cyber activities) and specific legislation. Irish policy-makers should ideally address gaps that arise in relation to new cybercrimes where non-specific legislation is sometimes limited. The 2017 EU Cyber strategy notes that today's procedural framework is not fit for purpose where, for instance, the speed of cyber attacks can overwhelm our procedures, as well as creating particular needs for swift cooperation across borders. For example, the EU Directive has limited definitions for the treatment and storage of investigation data which can result in a lack of consistency on the standards of storage between jurisdictions and this can result in the inadmissibility of evidence in investigations. To this end, the European Commission published draft legislation to facilitate cross-border access to electronic evidence in 2018 and proposed international negotiations on cross-border access to electronic evidence. It is also implementing practical measures to improve cross-border access to electronic evidence for criminal investigations, including funding for training on cross-border cooperation, the development of an electronic platform to exchange information within the EU, and the standardisation of judicial cooperation forms used between Member States.

While the majority of the Budapest Convention is already integrated within Irish legislation, a new cybercrime Bill is due to address the remainder of the provisions of the Convention, which is due to be formally ratified in the near future. The Convention continues to provide a global legal framework for combatting cybercrime, and a possible addition of a protocol has been under exploration to address cross-border access to electronic evidence in an international context. Rather than the creation of new international legal instruments for cybercrime issues, the EU calls for the designing of appropriate national legislation and for Member States to pursue cooperation within this existing international framework. However, a proposal for a cybercrime treaty was submitted by Russia to the Third Committee of the United Nations in 2019 and Irish policy-makers working in criminal justice and foreign affairs should ideally analyse the implications of this proposal for Irish and EU interests in terms of cybercrime and broader diplomacy questions.

The report finds that while effective legislation is desirable, it is not always feasible to have legislation in place to meet the pace of technological change. Legislative change can be a lengthy process for good reason, and this report finds that input provided by law enforcement at an early stage of the legislative process can help to surmount fundamental issues that may hamper investigations after implementation. For example, Europol works with the private sector to establish agreed practices and non-binding agreements to improve consistency prior to the implementation of legislation. The report further highlights the issue of resourcing for An Garda Síochána in relation to cybercrime. While the Future of Policing in Ireland report (2018) notes this challenge and some progress has been made, there is still a constant demand on small investigative teams given that cases increasingly have an IT component. Investigation and prosecution of cybercrimes require well-trained and knowledgeable personnel in the investigation phase, during prosecution, and in courts, coupled with effective legislation. Another challenge relates to staff and skills retention and it may be timely to consider how officers can be retained or whether there is value in the use of volunteers or partnerships with the private sector to support skills gaps within the police.

In addition, there is limited research on the effectiveness of these legal instruments, but research in the area of crime prevention more generally is better researched. These learnings on traditional crime prevention and criminology could be transferable to the area of cybercrime. Moreover, prevention measures are often achieved through education, training and awareness raising rather than through legislation.

Another aspect that negatively impacts the effectiveness of legislation relates to under-reporting which means prosecutions are less likely. Improving citizens' and SMEs' awareness that they have been a victim of crime is found again in the report to be a key first step. While organisations are encouraged to report cybercrime incidents, reporting is found to be difficult and burdensome. Creating an easier process would likely improve reporting, which in turn would improve national statistics and provide better insights. In terms of statistical data, it can also be difficult to harmonise data across jurisdictions and to meet the reporting requirements of EU Directives and other bodies because no one organisation can supply all the figures. The UK has started to introduce questions that measure cybercrime rates on the Crime Survey for England and Wales and this could be a good practice to consider in Ireland given that crime surveys have long replaced police recorded crime as the most accurate measure of crime rates.

Other examples of non-legislative good practice are discussed in Section Four. A key finding is the lack of systematic reviews of practices responding to the threat of cybercrime, both from an academic and operational perspective. That said, this research shows that there is an increasing and evolving array of research into what is or is not effective in this area. This may result in improved mechanisms to measure success in the near future. The impact of a lack of systematic reviews means that the findings contained within this report provide food for thought in regard to policy consideration for Ireland and the Department of Justice and Equality. Greater analysis will be required to substantiate many of the aforementioned policy suggestions and good practices. Nonetheless, the approach taken in the report has been to identify perceived good practice in academic writings and through interviews with key stakeholders to better inform the direction of further analysis and policy development in Ireland. For the most part, many of these findings align closely.

A large number of areas were discussed in section four of the report, all of which offer areas for further analysis and research. Firstly, local and contextual conditions should be assessed and researched before importing a model into a new area. Secondly, any new policy practice should include mechanisms for evaluating success or lack thereof. However, this requires reliable and consistent statistics, which has been shown to be a challenge. In this regard, it would be prudent, in an Irish context, to explore mechanisms to ensure the availability and accessibility of more reliable and relevant statistics. Thirdly, any policy should be risk assessed to ensure a balance between human rights and privacy. This should be conducted cognisant of the need to have both a short and long term perspective of positive and unintended consequences. Fourthly, the findings suggest that any course of action should take on a methodological approach when defining a roadmap for activities, and where possible include a whole of government approach, and also incorporate non-governmental stakeholders.

Such collaborative partnerships are often a central part of crime strategies and essential to the work of EC3 at Europol, and while not beyond challenges as shown in the report, they have the potential to be very effective if developed correctly. As a result, an area worth further analysis is how Ireland can enhance its existing, highly prized, partnerships in this area. Improvements could place Ireland in a good position to develop a systematic means of establishing best practice, and build on the rich eco-systems of universities, tech companies, law enforcement and other relevant stakeholders. One area that would benefit from further enhancement is to explore the development of a more formal mechanism of collaboration. This may require a review of the interpretation of regulations and legislation such as GDPR, to see if there are opportunities for greater exchange of data, without infringing on privacy. Interestingly, Europol in the interest of moving forward and maximising existing relationships, while not breaching any law or regulations on data privacy, is looking at the potential of exchanging open source intelligence.

Another area that often takes a central part of such strategies is the use of awareness raising campaigns. The research shows a shift from general campaigns is needed. Therefore, more precise efforts to bring about change that will help to raise cybersecurity levels and resilience in the wake of cybercrime should ideally be considered, mindful also of the need to reduce the risk of creating a culture of fear, or a culture where victims are blamed.

REFERENCE SECTION

Ablon L, Libicki M, and Golay A. 2014. *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar*. The RAND Corporation.

Amárach Research. (2019). *Securing the Future: The Cyber Security Climate in Ireland*. Commissioned by Microsoft.

An Garda Síochána Website (2020) Garda National Cyber Crime Bureau (GNCCB) https://www.garda.ie/en/about-us/specialist-units/garda-national-cyber-crime-bureau-gnccb-/

An Garda Síochána. (ongoing). *Monthly Reports to the Policing Authority*. Accessible at: https://www.garda.ie/en/Information-Centre/Commissioner-s-Monthly-Reports-to-Policing-Authority/.

Arthur C. (2018). *Cyber Wars: Hacks that shocked the business world*. Kogan Page Limited.

Bada, M. and Nurse, J. (2019). *Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs*). Information and Computer Security.

Bada, M. and Sasse, A; (2014) Cyber Security Awareness Campaigns: Why do they fail to change behaviour? Global Cyber Security Capacity Centre, University of Oxford: Oxford, UK.

BH Consulting. (2019). *Security Roundup: September 2019* [online]. Available at: https://bhconsulting.ie/security-roundup/.

Blinderman E. and Din M. 2017. *Hidden by Sovereign Shadows: Improving the Domestic Framework for Deterring State-Sponsored Cybercrime*. Vanderbilt journal of transnational law.

Bossong R. & Wagner B. (2018) A Typology of Cybersecurity and Public–Private Partnerships in the Context of the European Union. In: Bures O., Carrapico H. (eds) Security Privatization. Springer, Cham

Brenner, S. (2012) *Cybercrime and the Law: Challenges, Issues, and Outcomes,* Northeastern University Press, 2012.

Brewer et al (2019) *Cybercrime Prevention - Theory and Applications,* Palgrave Macmillan.

Button, M & Cross, C 2017, Cyber Frauds, Scams and their Victims. Routledge.

Cahill. K (2018). *GCHQ offers help to embryonic Irish cyber security organisation*. Computer Weekly. Accessible at: https://www.computerweekly.com/opinion/GCHQ-offers-help-to-embryonic-Irish-cyber-security-organisation.

Calderoni, F. (2010) The European legal framework on cybercrime: Striving for an effective implementation. *Crime, Law and Social Change* **54**(5), 339-357.

Carr, M. (2016) Public–private partnerships in national cyber-security strategies, 92(1), 43-62.

Central Statistics Office (CSO) (2018). Information Society Statistics – Households: https://www.cso.ie/en/releasesandpublications/er/isshh/informationsocietystatistics-households2018/

CETs No. 185 (2001). Council of Council of Europe Convention on Cybercrime (CETS No. 185) of 2001, Accessed from https://rm.coe.int/1680081561 19 August 2019.

Chang, L. and Grabosky, P. (2017). *The governance of cyberspace*. Drahos, P. (ed) in *Regulatory Theory: Foundations and Applications*. Canberra: ANU Press.

Chatterjee S, Kar AK, Dwivedi YK et al (2019) Prevention of cybercrimes in smart cities of India: from a citizen's perspective. *Information Technology & People*. **32**(5): 1153-1183.

Chawki, M. (2005) A Critical Look at the Regulation of Cybercrime: A Comparative Analysis with Suggestions for Legal Policy, *DROIT-TIC*, 11 April 2005.

Clough, J. (2015) *Principles of Cybercrime*. Cambridge: Cambridge University Press.

Clough, J. (2011). Cybercrime. *Commonwealth Law Bulletin*. **37**(4), 671-680.

Commission on the Future of Policing (2018). *'The Future of Policing in Ireland'* Report. Retrieved from http://www.policereform.ie/en/POLREF/The%20Future%20of%20Policing%20in%20Ireland(web).pdf/Files/The%20Future%20of%20Policing%20in%20Ireland(web).pdf on 3 September 2019

Coventry, Briggs, Blythe, & Tran, (2014). Using behavioural insights to improve the public's use of cyber security best practices, Summary Report. Government Office for Science.

Coventry L. and Branley D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas. Volume 113.

Crowdstrike. (2019). *2019 Global Threat Report: Adversary Tradecraft and the Importance of Speed*. United States.

Cyber Essentials website (2020). Protect your organisation against cyber attack, Accessible at https://www.cyberessentials.ncsc.gov.uk/

Cyber Ireland (2019) Cyber Ireland Website, Retrieved on https://cyberireland.ie/ 14 October 2019

Day, G. (2019). *Ireland's commitment to cybersecurity* [online]. Paloalto networks blog. Accessible at: https://blog.paloaltonetworks.com/2019/08/irelands-commitment-cybersecurity/.

Décary-Hétu, D. and Giommoni, L. (2016). *Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous. Crime, Law and Social Change*.

Dempster, M. (2003) ‘Systematic Reviews’, in R. Miller and J. Brewer (eds) The A to Z of Social Research (London: Sage).

De Myynck, J., Graux, H., and Robinson, N. (2013) The Directive on attacks against information systems, *A Good Practice Collection for CERTs on the Directive on attacks against information systems,* ENISA P/28/12/TCD, Version: 1.5, 24 October, 2013.

Department of Communications, Climate Action & Environment. (2019). *National Cyber Security Strategy Draft Public Consultation*. Government of Ireland.

Department of Communications, Energy & Natural Resources. (2015-2017). *National Cyber Security Strategy: Securing our Digital Future*. Government of Ireland.

Department of Communications, Energy & Natural Resources. (2019-2024). *National Cyber Security Strategy*. Government of Ireland.

Department for Digital, Culture, Media and Sport. (2019). *Cyber Security Breaches Survey 2019: Statistical Release*. HM Government.

Department of Justice and Equality (2019), *Cybercrime*, Government of Ireland, Accessible at: http://www.justice.ie/en/JELR/Pages/Cybercrime [Accessed 18 September 2019].

Directive 2002/58/EC of the European Parliament and of the Council of the European Union, 12 July 2002, [2002] OJ L 201/37 279.

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, [2013] OJ L 218/8.

Directive 2016/1148/EU. ENISA Website, NIS Directive, Retrieved from https://www.enisa.europa.eu/topics/nis-directive 15 August 2019. on 01 September 2019.

Director of National Intelligence. (2019). *Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community*. Office of the Director of National Intelligence. United States government.

Doolan, (2011). *An Introduction to Irish Criminal Law*, Gill Education.

Drewer, D. & Ellermann, J. (2012). *‘Europol’s data protection framework as an asset in the fight against cybercrime*’. ERA Forum (2012) 13:381–395. This article is based on a contribution given at the conference “Making Europe Safer: Europol at the Heart of European Security”, organised by ERA in cooperation with Europol on 18–19 June 2012 in The Hague.

ENISA (2012a) *‘Give and Take, Good Practice Guide for Addressing Network and Information Security Aspects of Cybercrime Legal, Regulatory and Operational Factors Affecting CERT Co-operation with Other Stakeholders’,* Retrieved from https://www.enisa.europa.eu/publications/good-practice-guide-for-addressing-network-and-information-security-aspects-of-cybercrime/at_download/fullReport on 27 September 2019.

ENISA (2012b) *'The Fight against Cybercrime, Cooperation between CERTs and Law Enforcement Agencies in the fight against cybercrime, A first collection of practices'*, Retrieved from https://www.enisa.europa.eu/publications/cooperation-between-certs-and-law-enforcement-agencies-in-the-fight-against-cybercrime-a-first-collection-of-practices on 27 September 2019.

ENISA (2014) '*National-level Risk Assessments, An Analysis Report',* Retrieved from https://www.enisa.europa.eu/publications/nlra-analysis-report on 27 September 2019.

ENISA (2016) '*NCSS Good Practice Guide, Designing and Implementing National Cyber Security Strategies'*, Retrieved from https://www.enisa.europa.eu/publications/ncss-good-practice-guide on 27 September 2019.

ENISA (2018). ENISA Threat Landscape Report 2017: 15 Top Cyber-Threats and Trends, Heraklion, Greece: ENISA: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017.

Eolas Magazine (2018). Combatting cybercrime. https://www.eolasmagazine.ie/combatting-cybercrime/Home Office Cybercrime Strategy (2010) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228826/7842.pdf

Epps, C. (2017) *Best practices to deal with top cybercrime activities*, Computer Fraud & Security April 2017.

EU DESI index (2020). '*Digital Economy and Society Index (DESI) 2020 -Thematic chapters*'. European Commission.

European Commission (2016) '*Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry'.* Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions.

European Commission (2013). Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the European Union: , An Open, Safe and Secure Cyberspace, Brussels JOIN(2013) 1 final.

European Commission. (2017a). *Joint Communication to the European Parliament and the Council – Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*. Brussels. JOIN(2017) 450 final.

European Commission (2017b) *Annex 1, Annex to the Communication from the Commission to the European Parliament and the Council, Making the most of NIS-towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union*, Retrieved from https://eur-lex.europa.eu/resource.html?uri=cellar:d829f91d-9859-11e7-b92d-01aa75ed71a1.0001.02/DOC_4&format=PDF on 12 October 2019

European Commission. (2019a). *Digital Economy and Society Index (DESI). 2019 Country*

Report: Ireland.

European Commission (2019b). 'Questions and Answers: Mandate for the Second Additional Protocol to the Budapest Convention', European Commission Press Release Database, Brussels, Retrieved from https://europa.eu/rapid/press-release_MEMO-19-865_en.htm 13 October 2019 on 12 October 2019

European Commission (2019) *'E-evidence - cross-border access to electronic evidence, Improving cross-border access to electronic evidence',* Retrieved from https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en on 15 October 201

European Commission. (2015). *Special Eurobarometer 423: CYBER SECURITY*. http://ec.europa.eu/public_opinion/index_en.htm.

EUROPOL & EUROJUST (2019) '*Common challenges in combating cybercrime, As identified by Eurojust and Europol',* JOINT REPORT, Europol and Eurojust Public Information. Retrieved from http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/Casework/Joint%20report%20of%20Eurojust%20and%20Europol%20on%20Common%20challenges%20in%20combating%20cybercrime%20(June%202019)/2019-06_Joint-Eurojust-Europol-report_Common-challenges-in-combating-cybercrime_EN.PDF on 13 October 2019

European Cyber Crime Centre (EC3). (2018). *Internet Organised Crime Threat Assessment (IOCTA).* Europol.

Eurostat (2019). Digital economy and society statistics - households and individuals: https://ec.europa.eu/eurostat/statistics-explained/index.php/Digital_economy_and_society_statistics_-_households_and_individuals#Internet_access

Gallagher. C. (2019) Gardaí receive intelligence on thousands of hackers from Europol. Irish Times. Accessible at: https://www.irishtimes.com/news/crime-and-law/garda%C3%AD-receive-intelligence-on-thousands-of-hackers-from-europol-1.3776452.

Grabosky, P. (2004) The Global Dimension of Cybercrime, *Global Crime*, **6**(1) 146-157.

Gordon, S. & Ford, R. (2006). On the definition and classification of cybercrimeJournal in Computer Virology, 2(1), 13–20.

Government of Ireland (1991) *Criminal Damage Ac*t. Retrieved from http://www.irishstatutebook.ie/eli/1991/act/31/enacted/en/print.html on 1 September 2019

Government of Ireland (1997) *Bail Act.* Retrieved from_Government of Ireland (1998) *Offences Against the State (Amendment) Act.* Retrieved from http://www.irishstatutebook.ie/eli/1998/act/39/enacted/en/print.html on 23 September 2019

Government of Ireland (2001) *Criminal Justice (Theft and Fraud Offences) Act.* Retrieved from http://www.irishstatutebook.ie/eli/2001/act/50/enacted/en/print.html on 1 September 2019

Government of Ireland (2011) *Criminal Justice Act*. Retrieved from http://www.irishstatutebook.ie/eli/2011/act/22/enacted/en/print on 1 September 2019

Government of Ireland (2017) *Criminal Justice (Offences relating to Information Systems) Act*. Retrieved from http://www.irishstatutebook.ie/eli/2017/act/11/enacted/en/print on 1 September 2019

Government of Ireland (2019) *National Cyber Security Strategy 2019-2024.*

Harkin, D., Whelan, C. and Chang, L. (2018). *The challenges facing specialist police cyber-crime units: an empirical analysis*. Police Practice and Research: An International Journal. Taylor & Francis.

Harkin, D. and Whelan, C. (2019). *Civilianising specialist units: Reflections on the policing of cyber-crime*. Criminology & Criminal Justice.

Harris, M. and Singla, R. (2014). *Cybercrime costs*. Accountancy Ireland. Institute of Chartered Accountants in Ireland.

Heinl C. (2019a). *Russia and China – Their impact on Irish security from a cyber perspective* [online].

Heinl C. (2019b). *Enhancing national cyber deterrence and the Irish Defence Forces' contribution*. Defence Forces Review.

Heinl, C. (2019c) An overview of the European Union's current strategies, policies and concepts on cyber. Retrieved from https://observatoire-fic.com/en/an-overview-of-the-european-unions-current-strategies-policies-and-concepts-on-cyber-by-caitriona-heinl/ on 25 August 2019.

Heinl, C. (2019d). *Peace and Security in Cyberspace: Issues, Actors and Practice*. United Nations HQ Training Session organised by Permanent Missions of Estonia, Kenya, Mexico, Singapore and the European Union. Author observations.

Heinl (2019e). *Conference on Building Global Cyberspace Peace Regime 2019 (GCPR 2019).* Republic of Korea. Author observations.

Harnett, Kevin & Timon, Victor (2018). Ireland: Cybersecurity 2019. ICLG. Retrieved from https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/ireland, published 16 October 2018.

Hildebrant, M. (2013) Balance or Trade-off? Online Security Technologies and Fundamental Rights, *Philosophy & Technology*, **26**(4), 357–379.

Hilliard, M. (2018). *Less fear and more transparency key to fighting cybercrime*. Irish Times. Accessible at: https://www.irishtimes.com/business/technology/less-fear-and-more-transparency-key-to-fighting-cybercrime-1.3692135.

Holt, T. & Bossler, A. (2015). *Cybercrime in Progress Theory and prevention of technology-enabled offenses*, Routledge, London.

Home Office. (2018). *Understanding the costs of cyber crime: A report of key findings from the Costs of Cyber Crime Working Group*. Research Report 96. Home Office Science Advisory Council. HM Government.

Honan. B. (2015). *Cybercrime statistics for Ireland* [online]. BHConsulting blog. Accessible at: https://bhconsulting.ie/cybercrime-statistics-for-ireland/.

Horgan, S. (2019) Cybercrime and everyday life: exploring public sensibilities towards the digital dimensions of crime and disorder, Forthcoming at: https://era.ed.ac.uk/handle/1842/35869

Hull, M., Eze, T. & Speakman, L. (2018) Policing the Cyber Threat: Exploring the Threat from Cyber Crime and the Ability of Local Law Enforcement to Respond. European *Intelligence and Security Informatics Conference*. 24-25 Oct. 2018

Irish Times. (2019). *Republic could get direct link to new undersea fibre optic cable*. Accessible at: https://www.irishtimes.com/business/technology/republic-could-get-direct-link-to-new-undersea-fibre-optic-cable-1.3777402.

Kabay, M (2001) Studies and Surveys of Computer Crime. Retrieved from

http://www.securitystats.com/reports/Studies_and_Surveys_of_Computer_Crime.pdf#search='studies%20and%20surveys%20of%20computer%20crime' on 20 September 2019

Keane J. (2018). *Dublin has ranked as one of Europe's top tech clusters – ahead of Paris and Copenhagen*. Fora. Accessible at: https://fora.ie/dublin-tech-cbre-4219755-Sep2018/.

Kaspersky Lab. (2018). *Reality vs Delusion: A Guide to the Modern Threat Landscape.* Moscow. Retrieved from www.kaspersky.com.

Kaspersky Lab. (2019). *Kaspersky Security Bulletin: Threat predictions for 2019*.

Keane, A. (2007). Computer Forensics and Irish Law, *The ITB Journal* **8**(2), Article 3. Retrieved from https://arrow.dit.ie/cgi/viewcontent.cgi?article=1106&context=itbj

Kennedy, J. (2018). *Cybercrime growing faster in Ireland than anywhere else*. Accessible at: https://www.siliconrepublic.com/enterprise/cybercrime-ireland-pwc.

Kigerl, A. (2011). *Routine Activity Theory and the Determinants of High Cybercrime Countries*. Social Science Computer Review.

Koops, Bert-Jaap and Goodwin, Morag, Cyberspace, the Cloud, and Cross-Border Criminal Investigation. The Limits and Possibilities of International Law (December 20, 2014). Tilburg Institute for Law, Technology, and Society CTLD – Center for Transboundary Legal Development, December 2014; Tilburg Law School Research Paper No. 5/2016.

Lessig, L. (1999) *Code and Other Laws of Cyberspace*, Basic Books, New York, 85-99.

Engineering Ethics **2**(137).

Leukfeldt, R. (2017). *The Human Factor in Cybercrime and Cybersecurity: Research Agenda,* Eleven International Publishing, 2017.

Levi, M. and Williams, M. (2013). *MULTI-AGENCY PARTNERSHIPS IN CYBERCRIME REDUCTION: Mapping the UK Information Assurance Network Cooperation Space*. Information Management & Computer Security.

Lohr, S. (2019). *Measuring Crime – Behind the Statistics*. CRC Press, Taylor and Francis Group.

Manning, C. (2016) Old Laws, New Crimes: Challenges of Prosecuting Cybercrime in Ireland. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2729204 on 13 August 2019.

Maurer, T. 2018. *Cyber Mercenaries: The State, Hackers, and Power*. Cambridge University Press.

McEnroe, J. (2019) Harris promises faster investigation of crimes and more frontline gardaí Retrieved from https://www.irishexaminer.com/breakingnews/ireland/harris-promises-faster-investigation-of-crimes-and-more-frontline-gardai-951327.html 17 September 2019 on 10 October 2019

McGuire, M. & Dowling, S. (2013). *'Cyber crime: A review of the evidence'*. Home Office, London.

McIntyrne, TJ (2015) Cybercrime: Towards a Research Agenda. In *Routledge Handbook of Irish Criminology.* (Healy, D., Hamilton, C., Daly, Y. & Butler, M. eds.), London: Routledge. Post Print Retrieved from https://researchrepository.ucd.ie/bitstream/10197/7281/1/TJ_McIntyre_-_Cybercrime_in_Ireland.pdf on 02 September 2019

McLaughlin, G. (2018). *Cybercrime rise is threat to Ireland Inc – Flanagan*. Independent.ie. Accessible at: https://www.independent.ie/business/technology/news/cybercrime-rise-is-threat-to-ireland-inc-flanagan-37422540.html.

Microsoft (2016) The Budapest Convention on Cybercrime – 15th Anniversary, *Microsoft Secure Blog Staff*, Retrieved from https://www.microsoft.com/security/blog/2016/11/17/the-budapest-convention-on-cybercrime-15th-anniversary/ on 14 Oct 2019.

Murray, K. (1995) Computer Misuse Law in Ireland. *Irish Law Times* 13(114).

National Audit Office. https://www.nao.org.uk/wp-content/uploads/2012/05/Improving_the_criminal_justice_system.pdf

National Crime Agency Website (2020). Cyber crime https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime

Nato website (2020). Cyber Coalition helps prepare NATO for today's threats, Published 27 Nov. 2018, Accessible at https://www.nato.int/cps/en/natohq/news_160898.htm

NCSS (2019) *National Cyber Security Strategy Consultation Document, Department of Communication, Energy & Natural Resources*, Retrieved from https://www.dccae.gov.ie/en-ie/communications/consultations/Documents/87/consultations/National%20Cyber%20Security%20Strategy%20Consultation%20Document.pdf

O'Brien, C. 2019. *Employees are major risk to employers' cyber security, study finds*. Irish Times. Accessible at https://www.irishtimes.com/business/technology/employees-are-major-risk-to-employers-cyber-security-study-finds-1.3797153.

O'Connor, N (2018). *The Government would not say that out loud but that was the Russians using our system because it is linked up with the British and it is very similar*. Irish Mirror. Accessible at: https://www.irishmirror.ie/news/irish-news/russian-hackers-already-accessed-hse-12242336.

O'Donovan, D. (2016). Ireland not ready for cyber crime threat, say 90pc of businesses. Independent.ie. Accessible at: https://www.independent.ie/business/technology/ireland-not-ready-for-cyber-crime-threat-say-90pc-of-businesses-35155451.html.

Office for National Statistics. (2020). *Dataset - Crime in England and Wales: Appendix tables.* HM Government. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables.

Picotti, L., & Salvadori, I. (2008) '*National Legislation Implementing the Convention on*

Cybercrime - Comparative analysis and good practices'. Strasbourg: Council of Europe.

PQ 26882/19 (2019) Parliamentary Question asked on the Wednesday, 26 June 2019, https://www.oireachtas.ie/en/debates/question/2019-06-6/32/?highlight%5B0%5D=26882

PQ, 24156/17 (2017) Parliamentary Question, Tuesday, 23 May 2017, https://www.oireachtas.ie/en/debates/question/2017-05-23/117/?highlight%5B0%5D=24156&highlight%5B1%5D=17

PQ 22645/18 (2018) Parliamentary Question, Wednesday, 23 May 2018, https://www.oireachtas.ie/en/debates/question/2018-05-23/38/?highlight%5B0%5D=22645&highlight%5B1%5D=18

Press Association. *Cyber crime attacks and losses surge in 2018*. Irish Examiner. Accessible at: https://www.irishexaminer.com/breakingnews/business/cyber-crime-attacks-and-losses-surge-in-2018-919451.html.

PwC. (2018). *Shining a light on fraud: Irish Economic Crime Survey 2018*. Accessible at: https://www.pwc.ie/reports/irish-economic-crime-survey-2018/download.html.

Raab, C., Jones, R. and Szekely, I. (2015). Surveillance and Resilience in Theory and Practice (August 17, 2015). Media and Communication, Vol 3, No 2 (Special Issue on Surveillance).

Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA.

Renaud, K. and Weir, G. (2016). *Cybersecurity and the Unbearability of Uncertainty*. IEEE.

Resolution on Combating the Criminal Misuse of Information Technologies. GA Res. 55/63, UN GA, 55th sess, 81st plen mtg, UN Doc A/RES/55/63 (2001).

Ross, A. (2018) 5 cyber security best practices for 2018: From culture to coping with BYOD, Information Age, Retrieved from https://www.information-age.com/5-cyber-security-best-practices-2018-123472164/ on 15 October 2019.

Sarre, R., Yiu-Chung, L. & Chang, L. (2018) Responding to cybercrime: current trends, *Police Practice and Research*, **19**(6), 515-518.

Schulman, Cristina (2011). *'About the Budapest Convention on Cybercrime'*, Presentation at Conference on the Budapest Convention on Cybercrime Organised by the Ministry of Information and Communication Technology of Mauritius and the Council of Europe Balaclava, Mauritius, 11 August 2014. Retrieved from https://rm.coe.int/16803028aa 15 October 2019 on 14 October 2019

Scottish Government. *Cyber Resilience*. Website: https://www.gov.scot/policies/cyber-resilience/.

Seger, A. (2012). Cybercrime strategies Global Project on Cybercrime. https://rm.coe.int/16802fa34f

Shah, M., Jones, P., & Choudrie, J. (2019) Cybercrimes prevention: promising organisational practices, *Information Technology & People*, 32(5), 1125-1129, Emerald Publishing Limited.

Shinder, D. (2002). *Scene of the Cybercrime*, Syngress, U.S.A., p. 6.

Siddaway, A., Wood, A. & Hedges, L. (2019) How to Do a Systematic Review: A Best Practice Guide for Conducting and Reporting Narrative Reviews, Meta-Analyses, and Meta-Syntheses, Annual Review of Psychology 2019 70:1, 747-770.

Slevin, S. & O'Reilly, S. (2017) Dedicated cybercrime legislation in Ireland: Worth the wait? Retrieved from https://www.lexology.com/library/detail.aspx?g=683a61b0-4e1a-496c-9224-bd41dacaf6e7 on 8 September 2019

Smith, G. (2019). *Security Roundup August 2019* [online]. BHConsulting Blog. Accessible at https://bhconsulting.ie/security-roundup-august-2019/.

Speer, D. (2000). Redefining borders: The challenges of cybercrime. Crime, Law and Social Change. Volume 34 Issue 3.

Stanton D. T.D., (2019). *Keynote address: Cybersecurity Transatlantic Policy Forum*.

Statistica (2018). ‘Number of Social Network Users Worldwide from 2010 to 2021 (in Billions)’: https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users.

Symantec Corporation. (2019). *Internet Security Threat Report*. United States.

Taylor, C. (2019). Majority of businesses across the world unprepared for cyberattacks. Irish Times. Accessible at https://www.irishtimes.com/business/technology/majority-of-businesses-across-the-world-unprepared-for-cyberattacks-1.3756463.

Taylor, G. (2001) The Council of Europe Cybercrime Convention: a civil liberties perspectives. *PrivLawPRpr* **8**(4). Privacy Law and Policy Reporter 69.

Taylor, P. (1999). *Hackers: Crime in the Digital Sublime*. Psychology Press.

UK Government Publication (2011). Improving the Criminal Justice System – lessons from local change projects, produced jointly by Her Majesty’s Crown Prosecution Service Inspectorate, Her Majesty’s Inspectorate of Constabulary, Her Majesty’s Inspectorate of Probation, and the National Audit Office.

UK NCSC website (2020). Cyber Security Information Sharing Partnership. https://www.ncsc.gov.uk/section/keep-up-to-date/cisp

United Nations General Assembly. (2015). *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. New York: United Nations A/70/174.

UNODC (2013). ‘Comprehensive Study on Cybercrime’. Accessible at https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

UNODC website (2020a). Global Programme on Cybercrime. Accessible at https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html

UNODC website (2020). The Commission on Crime Prevention and Criminal Justice (CCPCJ) Accessible at https://www.unodc.org/unodc/en/commissions/CCPCJ/index.html

Walden, I. (2018). *The Sky is Falling!’ – Responses to the ‘Going Dark’ problem*. Computer Law & Security Review: The International Journal of Technology Law and Practice. Volume 34, Issue 4.

Wall, D. (2004) What are Cybercrimes? *Criminal Justice Matters*, **58**(1), 20-21

Wall, D. (2007). *Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace*. Police Practice and Research: An International Journal. Taylor & Francis.

Wilton Park report. (2018). *Military operations in cyberspace*. WP1635.

Yar, M. and Steinmetz, K. (2019). *Cybercrime and Society*. Sage.

Appendix A Data coding process matrix

Author	Year	Name of Publication	Type of study	Evaluation type and strength	Relevance to one of the three project sections	Additional information
Ablon L, Libicki M, and Golay A.	2014	Markets for Cybercrime Tools and Stolen Data : Hackers' Bazaar	Book/Report	Relevant for conducting a deeper analysis on black markets/the “hackers bazaar” in order to develop responses – although dates back to 2014	High	
Amárach Research	2019	Securing the Future: The Cyber Security Climate in Ireland	Industry report/ survey	Research related to the current cybersecurity climate in Ireland	High	Amárach report commissioned by Microsoft. This research in particular focuses on the security of medium and large organisations, and the behaviour and attitudes of employees of these organisations in regard to technology and cyber security.

An Garda Síochána	Jan-July2019	Monthly Reports to the Policing Authority	Government body report	General overview of policing activities for the policing authority	Low	Not solely focused on cybercrime – basic to little information on cybercrime trends, but informative for Section 2 in relation to providing public insight and updates on modern responses and initiatives being undertaken
Arthur, C.	2018	Cyber Wars: Hacks that shocked the business world	Book	Case studies of cyber incidents	High	
Bada, M. and Nurse, J.	2019	Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs).	Journal Article	Informative re engagement with private sector	Medium	
Bada, M. & Sasse, A.	2014	Cyber Security Awareness Campaigns: Why do they fail to change behaviour?	Journal Article	Relevant re awareness campaigns	Medium	
BHConsulting	Ongoing	Security Roundup	Consultancy blog	Informative/ regular updates	Medium	
Blinderman E. and Din M.	2017	Hidden by Sovereign Shadows: Improving the Domestic Framework for	Journal article	Timely legal analysis on key questions	High	

		Deterring State-Sponsored Cybercrime		related to state-cybercrime activity		
Bossong R. & Wagner B.	2018	A Typology of Cybersecurity and Public–Private Partnerships in the Context of the European Union.	Chapter	Relevant re public private partnerships	Medium	
Brenner, S.	2012	Cybercrime and the Law: Challenges, Issues, and Outcomes	Book	Informative in respect to cybercrime law and policy	Medium	
Button, M & Cross, C.	2017	Cyber Frauds, Scams and their Victims.	Book	Learnings from cyber-enabled crime	Medium	
Cahill, K.	2018	GCHQ offers help to embryonic Irish cyber security organisation	Online media	Informative	Medium	
Calderoni, F.	2010	The European legal framework on cybercrime: Striving for an effective implementation	Article	Analysis of European legal framework on cybercrime	High	
Chatterjee S, Kar AK, Dwivedi YK et al	2019	Prevention of cybercrimes in smart cities of India: from a citizen's perspective	Journal article	Relevant in respect to awareness raising	Medium	
Chawki, M.	2005	A Critical Look at the Regulation of Cybercrime: A Comparative Analysis with Suggestions for Legal Policy	Journal article	Analysis in respect to legislation & responses	Medium	
Clough, J.	2015	Principles of Cybercrime	Book	Analysis in respect to legislation	Medium	

Clough, J.	2011	Cybercrime	Article	Relevant to challenges of cybercrime and related international instruments	High	
Commission on the Future of Policing	2018	The Future of Policing in Ireland Report	Report	Relevant to policing response	Medium	
Coventry L. and Branley	2018	Cybersecurity in Healthcare: A Narrative Review of Trends, Threats and Ways Forward	Journal article	Timely	Medium	
Coventry, Briggs, Blythe & Tran	2014	Using behavioural insights to improve the public's use of cyber security best practice	Report	Informative in relation to changing behaviour	High	
Crowdstrike	2019	2019 Global Threat Report: Adversary Tradecraft and the Importance of Speed	Cybersecurity vendor	Rather sales-oriented; better information on state-related threats	Low	
Cyber Essential	2020	Cyber Essentials website	Website	Informative	Low	
Cyber Ireland	2019	Cyber Ireland Website	Website	Informative	Low	
Day G.	2019	Ireland's commitment to cybersecurity	Industry blog		Low-medium	

Department of Communications, Climate Action & Environment	2019	National Cyber Security Strategy Draft Public Consultation.	Government publication	Pre-National Cyber Security Strategy 2019	Low	
Department of Communications, Energy & Natural Resources	2015 - 2017	National Cyber Security Strategy: Securing our Digital Future	Government strategy	Relevant to the Irish threat landscape	Medium	
Department of Justice and Equality	2019	Cybercrime	Website	Informative	Low	
De Myynck, J., Graux, H., and Robinson, N.	2013	The Directive on attacks against information systems, A Good Practice Collection for CERTs on the Directive on attacks against information systems	Report	Provides insights into good practice responses	High	
Director of National Intelligence, United States	2019	Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community	U.S. intelligence community threat assessment	Less focused on cybercrime; but significant trends highlighted	Medium	
Doolan, B.	2011	An introduction to Irish Criminal Law	Book	Informative	Low	
Drewer, D. & Ellermann, J.	2012	Europol's data protection framework as an asset in the fight	Article	Relevant to data protection and safeguardin	Medium	

		against cybercrime		g rights		
ENISA	2012 a	Give and Take, Good Practice Guide for Addressing Network and Information Security Aspects of Cybercrime Legal, Regulatory and Operational Factors Affecting CERT Co-operation with Other Stakeholders	Report	Provides insights into good practice responses	High	
ENISA	2012 b	The Fight against Cybercrime, Cooperation between CERTs and Law Enforcement Agencies in the fight against cybercrime**,** A first collection of practices	Report	Provides insights into good practice responses	High	
ENISA	2014	National-level Risk Assessments, An Analysis Report	Report	Provides insights into good practice responses	High	
ENISA	2016	NCSS Good Practice Guide, Designing and Implementing National Cyber Security Strategies	Report	Provides insights into good practice responses	High	
Epps, C.	2017	Best practices to deal with top cybercrime activities	Journal article	Provides insights into good practice	High	

				responses		
European Commission	2016	Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry	Strategy document	High relevance as EU policy document		
European Commission	2017 b	Annex 1, Annex to the Communication from the Commission to the European Parliament and the Council, Making the most of NIS-towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union	Strategy document	High relevance as EU policy document		
European Commission	2017 a	Joint Communication to the European Parliament and the Council – Resilience, Deterrence and Defence: Building strong cybersecurity for the EU	Strategy document	High relevance as EU policy document		Little depth on the nature of cyber threats, but relevant foundational information provided
European Commission	2019 a	Digital Economy and Society	Digital Economy		Low	

		Index (DESI). 2019 Country Report: Ireland.	ranking/EU Member States			
European Commission	2019	E-evidence - cross-border access to electronic evidence, Improving cross-border access to electronic evidence	Strategy document	High relevance as EU policy document		
European Commission	2019b	Questions and Answers: Mandate for the Second Additional Protocol to the Budapest Convention', European Commission Press Release Database, Brussels	Website	High relevance as EU policy document		
Europol European Cybercrime Centre (EC3)	2018	Internet Organised Crime Threat Assessment (IOCTA)	Expert strategic report/EU LE community	High relevance for strategic, policy and operational decision-making	High	Europol's EC3 publishes IOCTA annually as its flagship strategic report on key findings/emerging threats and developments in cybercrime from a law

						enforcement perspective
EUROPOL	2019	EUROPOL Website	Website	Insights into law enforcement responses	High	
EUROPOL & EUROJUST	2019	Common challenges in combating cybercrime, As identified by Eurojust and Europol	Report	Insights into common challenges combating cybercrime	High	
Gallagher, C.	2019	Gardaí receive intelligence on thousands of hackers	Online media/mainstream	Informative	Low-medium	
Gordon & Ford	2006	On the definition and classification of cybercrime	Journal Article	Relevant to measurement & definitions	Medium	
Government of Ireland	1991	Criminal Damage Act	Legislation	Relevant in relation to legislation	High	
Government of Ireland	1997	Bail Act	Legislation	Relevant in relation to legislation	Low	
Government of Ireland	2001	Criminal Justice (Theft and Fraud Offences) Act	Legislation	Relevant in relation to legislation	High	
Government of Ireland	2011	Criminal Justice Act	Legislation	Relevant in relation to legislation	Medium	
Government of Ireland	2017	Criminal Justice (Offences relating to Information Systems) Act	Legislation	Relevant in relation to legislation	High	

Grabosky, P.	2004	The Global Dimension of Cybercrime	Chapter	Insights into jurisdictional challenges	High	
Harkin, D., Whelan, C. and Chang, L.	2018	The challenges facing specialist police cyber-crime units: an empirical analysis.	Journal Article	Relevant to policing in this area	High	
Harkin, D. and Whelan, C.	2019	Civilianising specialist units: Reflections on the policing of cyber-crime.	Journal Article	Relevant to policing in this area	High	
Harnett, K. & Timon, V.	2018	Ireland: Cybersecurity 2019	Online Blog	Analysis of laws pertaining to cyber in Ireland	High	
Heinl, C.	2019	Russia and China – Their impact on Irish security from a cyber perspective	Independent commentary	Timely analysis on the Irish cyber threat landscape from a strategic perspective	High	
Heinl, C.	2019	An overview of the European Union's current strategies, policies and concepts on cyber	Independent commentary	Overview of EU strategies & policies on cyber	Medium	
Heinl, C.	2019	Enhancing national cyber deterrence and the Irish Defence	Journal article	Overview Irish cyber threat landscape	High	

		Forces' contribution				
Hildebrant, M.	2013	Balance or Trade-off? Online Security Technologies and Fundamental Rights, Philosophy & Technology	Journal article	Relevance in respect to balancing rights with security	High	
Hilliard M.	2018	Less fear and more transparency key to fighting cybercrime	News article/Irish Times	Informative	High	Hilliard M.
Holt, T. & Bossler, A.	2015	Cybercrime in Progress Theory and prevention of technology-enabled offenses	Book	Informative	High	
Honan, B.	2015	Cybercrime statistics for Ireland	Consultancy blog	Informative	Medium	
Horgan, S.	2019	Cybercrime and everyday life: exploring public sensibilities towards the digital dimensions of crime and disorder.	PhD Thesis	Informative	Medium	
Hull, M., Eze, T. & Speakman, L.	2018	Policing the Cyber Threat: Exploring the Threat from Cyber Crime and the Ability of Local Law	Journal article	Informative in relation to good practices	High	

		Enforcement to Respond				
Kabay, M	2001	Studies and Surveys of Computer Crime	Paper	Informative	Low	
Kaspersky Lab	2018	Reality vs Delusion: A Guide to the Modern Threat Landscape	Industry report (cybersecurity vendor)	Informative and timely in relation to emerging trends	High	Based on the company's global statistics/intelligence
Kaspersky Lab	2019	Kaspersky Security Bulletin: Threat predictions for 2019	Industry report	General observations; not overly informative	Low	
Keane, A.	2007	Computer Forensics and Irish Law	Journal article	Insightful in relation to legislation	Medium	
Keane, J.	2018	Dublin has ranked as one of Europe's top tech clusters – ahead of Paris and Copenhagen	Online media	Informative	Low-Medium	
Kigerl A.	2011	Routine Activity Theory and the Determinants of High Cybercrime Countries	Journal article	Theory	Medium	
Kennedy,	2018	Cybercrime growing faster in Ireland than anywhere else	Online media	Results of PWC report "Shining a light on fraud: Irish Economic Crime	Low	

				Survey 2018”		
Koops, Bert-Jaap and Goodwin, Morag,	2014	Cyberspace, the Cloud, and Cross-Border Criminal Investigation. The Limits and Possibilities of International Law	Paper	Informative in relation to jurisdiction and cross border issues	Medium	
Lessig, L.	1991	Code and Other Laws of Cyberspace	Book	Insightful in relation to legislation	Medium	
Leukfeldt, R.	2017	The Human Factor in Cybercrime and Cybersecurity	Book	Relevant for a non-technical perspective	High	
Levi, M. and Williams, M.	2013	Multi-agency partnerships in cybercrime reduction: Mapping the UK Information Assurance Network Cooperation Space.	Article	Informative	Medium	
McLaughlin, G.	2018	Cybercrime rise is threat to Ireland Inc – Flanagan	Online media	Timely/informative	Low-medium	
Maner, W.	1996	Unique Ethical Problems in Information Technology Science and Engineering	Journal article	Informative	Low	

Manning, C.	2016	Old Laws, New Crimes: Challenges of Prosecuting Cybercrime in Ireland	Journal article	Relevance in relation to legislation and prosecuting challenges	High	
Maurer T.	2018	Cyber Mercenaries: The State, Hackers, and Power	Book	Relevant for a deeper analysis on state use of hackers/proxies	Medium	
McEnroe, J.	2019	Harris promises faster investigation of crimes and more frontline gardaí	News Article	Relevant to policing in this area	Medium	
McGuire, M. & Dowling, S.	2013	Cyber crime: A review of the evidence	Government Report	Provides insight into the situation in the UK	Medium	
McIntyrne, TJ	2015	Cybercrime: Towards a Research Agenda	Chapter	Significant Insights	High	
Microsoft	2016	The Budapest Convention on Cybercrime – 15th Anniversary, Microsoft Secure Blog Staff	Online blog	Informative	Medium	
Murray, K.	1995	Computer Misuse Law in Ireland	Journal article	Provides historical context	Medium	
O'Brien, C.	2019	Employees are major risk to employers' cyber	Online media/mainstream/Irish Times	Informative	Medium	O'Brien, C.

		security, study finds				
O’Connor, N.	2018	The Government would not say that out loud but that was the Russians using our system because it is linked up with the British and it is very similar	Online Press	General	Low	
O’Donovan, D.	2016	Ireland not ready for cyber crime threat, say 90pc of businesses	Online media	Informative/ non-analytical	Low	
Picotti, L., & Salvadori, I.	2008	National Legislation Implementing the Convention on Cybercrime - Comparative analysis and good practices	Report	Very insightful into legislation	High	
Press Association	2019	Cyber crime attacks and losses surge in 2018	Online media	References to new industry report	Medium	
PwC	2018	Shining a light on fraud: Irish Economic Crime Survey 2018	Industry report	Irish threat landscape	Medium	Not solely focused on cybercrime – economic crime survey of Irish businesses
Ross, A.	2018	5 cyber security best practices for 2018: From culture to coping	Online blog	Informative	Medium	

		with BYOD, Information Age				
Sarre, R., Yiu-Chung, L. & Chang, L.	2018	Responding to cybercrime: current trends	Article	Informative	Medium	
Schulman, C.	2011	About the Budapest Convention on Cybercrime	Presentation	Insightful in relation to the Convention	Medium	
Shah, M., Jones, P., & Choudrie, J.	2019	Cybercrimes prevention: promising organisational practices.	Journal article	Informative	Medium	
Shinder, D.	2002	Scene of the Cybercrime	Book	Informative	Medium	
Slevin, S. & O'Reilly, S.	2017	Dedicated cybercrime legislation in Ireland: Worth the wait?	Online blog	Informative in relation to cybercrime in Ireland	Medium	
Speer D.	2000	Redefining borders: The challenges of cybercrime	Journal article	Cybercrime analysis, dating back to 2000	Low	
Symantec Corporation	2019		Security industry report	Current global trends from an industry perspective	High	
Taylor, C.	2019	Majority of businesses across the world unprepared for cyberattacks	Mainstream media/Irish Times	Sheds little light	Low	

Taylor, G.	2001	The Council of Europe Cybercrime Convention: a civil liberties perspectives	Article	Insightful into balancing privacy and security	Medium	
United Nations General Assembly	2015	Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security A/70/174.	Report of UN Group of Governmental Experts	Consensus report of 2015 group of governmental experts on ICTs in the context of international security	Medium/ Section 3	Evolving international law related to state behaviour/international security
Walden I.	2018	'The Sky is Falling!' – Responses to the 'Going Dark' problem	Journal article	Analysis on encryption/anonymity	Medium	
Wall, D.	2004	Wall, D. (2004) What are Cybercrimes?	Journal article	Informative	High	
Wilton Park	2018	Military operations in cyberspace	Workshop report	Military focused	Low	

Appendix B List of Interviewees

Interviews were conducted with representatives from the following organisations. Their time, insights and opinions are greatly appreciated.

Professor David Wall, University of Leeds

Representatives from An Garda Síochána

Representative from an Irish Academic Institute

Representatives from Banking & Payments Federation Ireland (BPFI)

Representative from the Central Statistics Office (CSO)

Representative from a Corporate Consultancy Firm

Representative from EUROPOL

Representative from the UK’s National Crime Agency (NCA)

Representatives from two financial institutions.