National College of Ireland

A Quantitative Analysis of Cyber Crime in Ireland

MSc Research Project

MSc in Cyber Security

Paul Gibbons

Student ID: x22167846

School of Computing

National College of Ireland

Supervisor: Mustafa Ul Raza

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: Paul Gibbons

Student ID: X22167846

Programme: MSCCYBETOP **Year:** 2024

Module: .....

Supervisor: Mustafa Ul Raza

Submission Due Date: 16th September 2024

Project Title: A Quantitative Analysis of Cyber Crime in Ireland

Word Count: **.....11061.....** **Page Count**..... **24**.....

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project. ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:

Date: **15/09/24**

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	X
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	X
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	X

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

A Quantitative Analysis of Cyber Crime in Ireland

Paul Gibbons

Student ID: x22167846

Abstract

This study investigates how the incidence of cybercrime in Ireland is quantified and compares it to best practices internationally. By assessing data from the US, EU, and Ireland, the research demonstrates that Ireland's cybercrime detection and prosecution rates (50 per 100,000 and 0.54 per 100,000 respectively for 2022[1]) are inadequate compared to more comprehensive systems like those in the US (260 per 100,000 and 2.6 per 100,000 respectively for 2022[2]). The study also evaluates prosecutorial rates and examines case law to identify gaps in Ireland's approach to cybercrime. Key challenges include historical and ongoing cybercrime underreporting issues, jurisdictional issues, and fragmented data management among Irish authorities. The research concludes that significant investments in automated reporting systems, data integrity, and specialized training for law enforcement are necessary to improve Ireland's cybercrime response. Additionally, enhancing international legal cooperation within the EU is crucial for better cross-border investigations and prosecutions. The study's findings highlight the need for a multi-disciplinary, cohesive strategy to address the growing cyber threats effectively.

Keywords: Cybercrime, Ireland, prosecution of cybercrime, cybercrime taxonomy, European cybercrime statistics, American cybercrime statistics.

1 Introduction

The aim of my project is to attempt to assess in quantitative terms how many cybercrimes have been investigated and prosecuted in Ireland since the introduction of significant computer crime related legislation. I have taken as a starting point the Criminal Justice (Offences Relating to Information Systems) Act 2017, transposed from the EU directive EU Directive 2013/40/EU[3] and commonly referred to as the Cybercrime Act 2017. This is the first piece of legislation dealing with computer crime passed in Ireland since 2003, albeit some researchers think the gap wider, going back to the passing of Criminal Damage Act of 1991. The act focuses primarily on hacking, unauthorised access, and interference with information systems, but it lacks provisions to fully address the evolving nature of cybercrime. Emerging forms of cybercrime, such as ransomware, deepfakes, cryptocurrency-related crime, and complex forms of online fraud, are not sufficiently addressed by the law. The Cybercrime Act 2017 represents the beginning of implementation of a raft of legislation European legislation such as the General Directive on Data Protection (GDPR), the Network and Information Security Directives (NIS 1 and 2), and the confusingly named Cyber Resilience, Security and Solidarity Acts, respectively, the adoption of some of which is still ongoing at the time of writing. It also closely coincides with the reorganisation of the An Garda Síochána (AGS)

[1] https://www.garda.ie/en/about-us/our-departments/office-of-corporate-communications/press-releases/2023/october/an-garda-siochana-annual-report-2022.html
[2] https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf
[3] https://www.gov.ie/en/publication/0735b-criminal-justice-offences-relating-to-information-systems-act-2017/

cyber unit, known as the Garda National Cyber Crime Bureau (GNCCB), established in 1991 as the Cyber Crime Investigation Unit[4] with the passing of the Criminal Damage Act of 1991[5].

This report will assess the available Irish cybercrime datasets in comparison with US and EU Cybercrime datasets and will show that the US data set represents the most holistic and detailed data set for cybercrime globally at this point in time. This comparison of international datasets will attempt to reflect the varying investigative practices, prosecutorial rates, and related statistics, without recourse to commercial data. I will then endeavour to outline where there are gaps between the comparator data sets and outline any possible opportunities for improvements and possible future research, with reference to Ireland in particular.

2 Related Work

Legislation such as the transposition into law of the second iteration of the Network and Information Security EU directive (NIS2) and other upcoming regulations such as the Cyber Resiliency Act and the Digital Operations Resiliency Act (DORA) point to the ongoing need for continuous improvement as the cyber threat landscape changes.

There is a large amount of statistical information generated by the cyber security industry globally purporting to reflect cybercrime trends and the various analyses that attempt to provide paths to resolution, usually in the form of commercial, proprietary products[6]. As a cyber security professional for the last number of years, I have used this data in many discussions with clients. What has often occurred to me with regards to this type of commercial data is that it appears to be largely survey based, and I have speculated as to how empirical the data is that these surveys are based upon. Data based on logs from systems such as network security devices, Security Incident and Event Management (SIEM) systems, Extended Detect and Response (XDR) systems, privilege access management (PAM) systems etc. can deliver statistics to product vendors and customers about attempted exploits and attacks. However, this data is not always in the public domain, may not be available for peer review, the research methodologies used could be opaque, and final results skewed to commercial editorial[7]. Whether any of this data or related research leads to actual prosecutions and convictions is not apparent from this study.

Research Question:

How is the incidence of cybercrime in Ireland currently quantified, how does this compare to best practise internationally?

Objectives:

1. The research will assess this data in comparison with US and EU Cybercrime data and will show that the US data set represents the most holistic and detailed data set for cyber globally at this point in time.
2. The research will assess prosecutorial rates, and related statistics, where available, without recourse to commercial data.
3. This paper will assess case law relating to cybercrimes in Ireland and how they are policed and reported on, with a view to identifying problems which currently exist,

[4] https://www.garda.ie/en/about-us/organised-serious-crime/garda-national-cyber-crime-bureau-gnccb-/
[5] https://www.lawsociety.ie/gaette/in-depth/away-in-a-hack
[6] https://www.fortinet.com/resources/cyberglossary/cybersecurity-statistics
[7] https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023

flagging some developing issues and endeavouring to outline suggestions for reform or improvement.

4. This study will assess any data within the context of the transnational nature of cybercrime and related jurisdictional issues, under-reporting of cybercrime, and the technical and skills-based issues in investigation, evidence management, and subsequent prosecution.

2.1 Policing Context

Hamilton proposes that Ireland has an historically laggard attitude to criminology, if not outright resistance to criminological research, (Hamilton, 2023) and this has meant that Ireland has been slow to adopt a consistent modern approach to criminology in general, and by extension, cybercrime. As a result, the discipline as a whole was underfunded from a statutory perspective and culturally ignored until the inevitable happened and important public infrastructure was breached, namely the Health Service Executive infrastructure in May 2021[8]. At the time of the breach, the National Cyber Security Centre (NCSC) had been in place for the preceding 10 years (initially as the Irish State's National/Governmental Computer Security Incident Response Team (CSIRT-IE). Similar to the Irish Defence Forces and the GNCCB[9], the NCSC was viewed as underfunded and understaffed and had not had someone employed in its main leadership role at the time of the HSE breach[10], the largest cyberattack ever on Irish public infrastructure at the time of writing.

This level of government apathy also had a further complicating issue within AGS. The GNCCB has been established since 2017 (established as the Cyber Crime Investigation Unit in 1991) but the annual AGS report for 2018 highlighted a severe backlog of cases going back 6 years (An Garda Siochana, 2018). The same report does outline that efforts were made to improve this situation during 2018, and this reduced it down to a 5-year backlog. From a reporting perspective there is no further allusion to this issue in the subsequent years, highlighting a consistency issue with regards to reporting. If a concerted, if incomplete, effort in 2018 was made, there is a valid expectation this situation would be monitored on a year-on-year basis from that point. However, there is no further mention of the bureau backlog in any other annual reports from that point on, with no published report for 2023 at the time at the time of writing[11]. Further, although AGS Public Attitude annual surveys [12] (commissioned by AGS) reflect high levels of confidence in the institution (An Garda Síochána, 2023) , when it comes to cybercrime, there are persistent challenges with underreporting, data quality, inter jurisdictional engagement, and skills base that are discussed in the sections to follow. A complicating factor for GNCCB is that they are principally an internal forensics unit for AGS and not the lead investigators in a case except when called on by the NCSC where legal jurisdiction is with AGS as the statutory law enforcement agency for the Republic of Ireland, powers the NCSC do not have.

---

[8] https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf
[9] https://www.thejournal.ie/how-irelands-cyber-crime-response-works-hse-ransonware-5440629-May2021/
[10] https://www.irishtimes.com/news/politics/investment-in-national-cybersecurity-centre-less-than-14m-over-10-years-1.4568764
[11] https://www.garda.ie/en/about-us/publications/annual%20reports/an-garda-siochana-annual-reports/
[12] https://www.garda.ie/en/about-us/publications/research-publications/

2.2 Definition of Cybercrime

2.2.1 Evolving Nature of Cybercrime

The term "cybercrime" itself may become increasingly redundant as technology becomes an integral part of almost all criminal activities. Furnell and Dowling (2019) suggest that the prefix "cyber-" might soon be unnecessary, as most serious and organised crimes now involve some form of technology, such as encryption or the internet. The National Crime Agency (2020) notes that traditional crimes, including counterfeiting physical currency, now frequently involve online components like recruitment, victimisation, and profiteering.

The evolving nature of cybercrime necessitates continuous updates to legal frameworks and law enforcement strategies. De Paoli et al., (2021) highlight the importance of mapping various types of cybercrime onto existing laws, including the Convention on Cybercrime (Council of Europe, 2001). This effort is crucial for ensuring that legal definitions keep pace with technological advancements and the changing landscape of criminal activity.

Cyber-dependent crimes are offences that can only be committed by using a computer, computer networks or other form of ICT[13]. These acts include the spread of viruses and other malicious software, hacking and distributed denial of service (DDoS) attacks – i.e., the flooding of Internet servers to take down network infrastructure or websites. Cyber-dependent crimes are primarily acts directed against computers or network resources, although there may be secondary outcomes from the attacks, such as fraud.

Cyber-enabled crimes are traditional crimes that are increased in their scale or reach by the use of computers, computer networks or other ICT[14]. Unlike cyber-dependent crimes, they can still be committed without the use of ICT. Examples can include fraud (including phishing and other online scams), theft and sexual offending against children.

To do credit of the Department of Justice in Ireland, their published definition[15] makes efforts to collate the above definitions :

"Cybercrime comprises:

- traditional offences (for example: fraud, forgery and identity theft)
- content related offences (for example: online distribution of child sexual abuse material, hate speech or incitement to commit acts of terrorism)
- offences unique to computers and information systems (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 or reputational damage)"

2.3 Cybercrime Data

2.3.1 PULSE System and Data Quality Issues

The Police Using Leading Systems Effectively (PULSE) system is the official system used by AGS for logging and managing crime data in Ireland since 1999. Since its inception, the system

[13] https://www.europol.europa.eu/socta/2017/cybercrime.html

[14] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/248621/horr75-chap2.pdf

[15] https://www.gov.ie/en/policy-information/80370-cybercrime/

has faced significant scrutiny and has often been a point of contention. The Central Statistics Office (CSO) raised public caveats regarding the quality of data from the PULSE system in 2017, which were only removed in February 2023. These caveats highlighted substantial issues in data accuracy and reliability, impacting the overall perception and utility of crime data and indeed the PULSE system itself[16] [17].

2.3.2 Reporting Quality and Consistency

Consistent and high-quality reporting is crucial for effective crime management and policy development. However, the AGS Reports from 2018 to 2022 reveal inconsistencies in data taxonomy and reporting standards. For instance, the GNCCB reported varying categories and case volumes over the years, indicating a lack of standardisation in data reporting. In 2019, for example, the GNCCB reported significant discrepancies in the classification and number of cases related to child exploitation, theft, and fraud compared to previous years. This inconsistency complicates the analysis of trends and the development of targeted interventions. The CSO also have their own discrepancy in that they publish general high level crime statistics, but do not correlate this to a specific offence, that is to say, an offence defined in the Cybercrime Act 2017 for example, is not registered in explicit terms as part of the annual crime statistics the CSO publishes, as detailed in Section 11 of the Configuration Manual.

2.3.3 Information Sharing and Ethical Considerations

Effective information sharing is critical for combating cybercrime, which often crosses national and organisational boundaries. Nouh et al. (2019) highlight the lack of information sharing within and across law enforcement agencies as a significant barrier. The study suggests that a hierarchical or flat architecture for information sharing could improve coordination and efficiency.

Sharing data across jurisdictions involves navigating complex legal and ethical landscapes. For instance, the GDPR imposes stringent requirements on how PII is handled and shared, necessitating robust data governance frameworks. The AGS Reports indicate that collaboration with international bodies such as Europol, Interpol, and the Cyber Defence Alliance has been instrumental in how AGS addresses transnational cybercrime. However, these efforts must be underpinned by strong ethical practices to protect individual privacy and data integrity.

2.3.4 Management Information and Data Utilisation

Law enforcement agencies (LEAs) leverage a patchwork of data to drive effective policing and crime prevention strategies. The AGS Reports illustrate various initiatives to enhance data management and utilisation. For instance, going back as far as 2018, the GNCCB's proactive engagement in operations like Ketch and Myriad demonstrates the importance of interdepartmental data sharing and collaboration. These operations have involved extensive analysis and forensic examination of digital evidence, leading to successful prosecutions and the disruption of organised crime networks.

However, effective data management also involves addressing the quality of reported information. De Paoli et al., (2021) point out that the lack of formal police taxonomy and technological support hinders the easy capture and analysis of cybercrime reports. This gap

[16] https://www.rte.ie/archives/2019/1114/1090829-gardai-not-on-pulse/
[17] https://www.irishtimes.com/news/crime-and-law/garda-s-pulse-database-symbolic-of-a-force-under-pressure-1.2646105

underscores the need for standardised data collection processes and the integration of advanced analytical tools to improve data accuracy and utility.

2.4 Jurisdictional Issues

Ireland's legal framework for cybercrime, particularly the Cybercrime Act 2017, is still relatively new and limited in scope, addressing crimes like hacking and unauthorized access but lacking provisions for emerging threats such as ransomware and cryptocurrency-related offenses. This has led to fewer precedents in prosecuting complex cybercrimes due to the country's relatively recent focus on cybercrime. In contrast, the United States has a far more mature and robust legal framework, with longstanding laws like the Computer Fraud and Abuse Act (CFAA) and the Electronic Communications Privacy Act (ECPA), which have evolved to cover a broad range of cyber activities, including hacking and DDoS attacks. U.S. federal agencies such as the FBI and Department of Homeland Security (DHS) collaborate extensively with state and local authorities to create a more comprehensive and coordinated cybercrime enforcement network, though its decentralized law enforcement structure often results in overlapping jurisdiction.

To complication matters further, cybercrime often transcends national borders, complicating the jurisdictional landscape. Jardine (2015) highlights that cyber-attacks can originate from any country with an internet connection, making it difficult to pinpoint the exact jurisdiction for prosecution. This global reach of cybercrime necessitates robust international cooperation and coordination among law enforcement agencies.

Curtis and Oxburgh (2022) discuss the jurisdictional issues surrounding the geographical locations of victims, suspects, and the technology used in cybercrimes. Complexity arises from uncertainty over which authority is responsible for investigating these crimes. Different entities such as local police, national agencies like the National Crime Agency (NCA) in the UK, and international organisations like Interpol and Europol are involved, but there is often a lack of clarity and coordination.

Legal frameworks have struggled to keep pace with the rapid evolution of cyber technology. Onomrerhinor (2023) argues that states continue to apply traditional territorially based rules to online activities, which are inadequate for addressing the borderless nature of the internet. This results in jurisdictional challenges, as existing laws do not fully capture the complexities of transnational cybercrime. Ireland's experience with cybercrime legislation highlights the difficulties of modernising legal frameworks to address cybercrime effectively. According to Friend et al. (2020), Irish legislation, which is crucial for monitoring a significant portion of EU data, has lagged in its modernisation efforts

The concept of jurisdiction encompasses several principles: territorial, nationality, protective, passive personality, and universality (Onomrerhinor, 2023). Each principle has its limitations when applied to cybercrime. For instance, the territorial principle is often rendered ineffective due to the lack of a physical crime scene in cyberspace, while the universality principle, although promising, is only widely accepted for a limited set of international crimes.

2.4.1 International Cooperation and Mutual Legal Assistance

The importance of international cooperation in combating cybercrime cannot be overstated. The AGS Reports from 2019 to 2022 detail various efforts by AGS to engage with international partners, including Europol, Interpol, and the Cyber Defence Alliance. These collaborations are vital for sharing information and intelligence on transnational cybercrime and developing joint strategies to combat these threats.

Mutual Legal Assistance Treaties (MLATs) are a critical tool for facilitating international cooperation. De Paoli et al., (2021) emphasise the need for such treaties to keep pace with technological changes and the evolving nature of cybercrime. The Budapest Convention on Cybercrime serves as a framework for international cooperation, but its implementation and the extent of its impact vary among countries.

2.4.2 Misconceptions and Public Understanding

A significant challenge in addressing cybercrime is the public's misconception about jurisdictional responsibilities. Cassandra Cross (2019) illustrates the disconnect between victims' expectations and the reality of who can investigate online fraud, where victims often find that their local police cannot assist due to jurisdictional constraints. Nouh et al. (2019) point out that most literature on how police deal with cybercrimes is based in the US, with little research focusing on other regions. This gap in the literature highlights the need for more comprehensive studies that consider the diverse legal and jurisdictional contexts across different countries.

2.5 Under Reporting

2.5.1 Individual Underreporting

Several studies have identified reasons why individuals fail to report cybercrime. According to (De Paoli et al., 2021), individuals may not report cybercrime because they do not recognise that they have been victimised (Jewkes and Yar, 2008), are embarrassed to admit their victimisation (Brown, 2015), or are apathetic due to the low impact of many cyber incidents (Wall, 2007). Additionally, a lack of awareness about reporting mechanisms (McMurdie, 2016) and a lack of confidence in police capabilities (Brown, 2015) contribute significantly to underreporting. The UKs Crime Survey for England and Wales estimates that only 1 in 14 incidents of computer misuse are actually reported to authorities[18].

2.5.2 Organisational Underreporting

Organisations also underreport cybercrime for various reasons. Lydon and Holloway (2022) highlight that small and medium-sized enterprises (SMEs) often lack the awareness or ability to detect cyber-attacks. Larger corporations, despite having extensive technology infrastructures, may choose to monitor selectively rather than comprehensively due to the potential negative impacts of breach disclosure on share prices, brand reputation, or financial penalties. Additionally, reporting decisions are often influenced by risk-averse corporate lawyers who may decide against reporting in the absence of definitive data. As De Paoli et al., (2021) further explain, businesses might avoid reporting to prevent reputational damage, believe they have better strategies to handle the problem internally (Brown, 2015), or have different objectives than law enforcement, such as minimising losses and avoiding negative publicity. That said, Lydon and Holloway (2022) go on to suggest there is some evidence that the effect of these perceived reputational impacts are potentially overstated, with only a short-term level of persistence as regards negative perceptions in particular.

[18]https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2024#computer-misuse

2.5.3 Challenges in Cybercrime Reporting

The complexity of cybercrime reporting is compounded by several factors. Bidgoli and Grossklags (2016) discuss how the lack of a clear definition of cybercrime (as discussed above) and its related victimisation, insufficient knowledge on how to report, and inadequate incentives and feedback mechanisms hinder effective reporting. Thakare et al. (2024) point out that in India, the burdensome process of filing complaints and fear of reprisals further discourage reporting. Additionally, the ease with which evidence can be tampered with in current systems adds to the challenges.

The underreporting problem is not limited to individuals and organisations but also extends to statistical reporting mechanisms. According to Levi, (2017) statistical reporting often fails to account for cybercrime accurately. This issue is exacerbated by the fact that different industries have varying reporting requirements, leading to inconsistencies in data collection and analysis ((Sangari et al., 2022).

All that said, in Ireland there is section 19 of the Criminal Justice Act of 2011 that mandates reporting of any incident, irrespective of the nature of the incident, that is believed to be, or could be perceived to be, criminal in nature to AGS. The broad scope of this provision, and the fact that it is relatively underused, and its implications not well understood publicly, mitigates against its potential effectiveness[19].

2.6 Training, Education and Awareness

Research indicates substantial gaps in knowledge and training among police forces concerning cybercrime investigation. De Paoli et al., (2021)underscore the inadequacies in initial induction training, which often excludes comprehensive cybercrime education. This omission results in significant knowledge gaps that impede officers' ability to identify and respond to cybercrime incidents effectively. The study also points to cultural issues within police departments, where cybercrime is not always regarded as a "real" crime, further diminishing the priority given to cybercrime training and resources.

Leppänen and Kankaanranta, (2017) highlight similar concerns in Finland, where the organisational models for cybercrime investigation are unclear. The study emphasizes the need to better understand how cybercrime units are structured, the professional characteristics of the staff, and the integration of computer forensics with traditional crime investigation. This lack of clarity and organisation further complicates the training and preparedness of law enforcement personnel.

Several initiatives have been undertaken to address the training needs of law enforcement in cybercrime investigation. In Ireland, the AGS Reports from 2019 to 2022 outline various programs aimed at enhancing cyber safety and investigation capabilities within AGS. For instance, the INSPECTr project, funded by the EU Horizon 2020 project fund ("INSPECTr," 2019), aimed to develop a shared intelligence platform to aid in crime detection and management (AGS Report 2020). The INSPECTr evaluation and policy recommendations report set[20] highlights the fact that the training required to implement the toolset was viewed as easy to rollout out at scale. The challenge for the INSPECTr project from the start has been its delimited, project-based nature as its final report indicates it ended on the 8th of May 2023. While the final reports are warm in their praise of the tool in terms of management, functionality, and Artificial Intelligence (AI) ethic. The INSPECTr project also emphasizes the need for ethical considerations in data sharing, especially concerning Personally Identifiable Information (PII) and compliance with regulations like GDPR.

[19] https://www.mccannfitzgerald.com/knowledge/investigations/mandatory-reporting-of-relevant-offences-it-hasnt-gone-away

[20] https://inspectr-project.eu/resources.html#results

it was less clear how it will be supported and maintained on an ongoing basis as a production level law enforcement tool. As it turns out, although AGS were involved throughout the project, INSPECTr has not been adopted as production tool for the GNCCB as per communication with the GNCCB as detailed in Section 13 of the configuration manual.

Despite efforts like this, significant challenges remain. Curtis and Oxburgh (2022) note that human users are often the weakest link in computer security, and training is crucial in shaping officers' perceptions of their preparedness to handle cybercrime investigations. However, they go on to say that the time allocated for such training is frequently insufficient, and the training itself often lacks the depth required to address the complexities of cybercrime. Forouzan et al. (2018) and HMIC (2015) findings corroborate the findings of Curtis and Oxburgh and they report that existing training programs are inadequate in terms of both content and duration, leaving officers underprepared.

2.7 Cybercrime Frameworks

The NCSC operates under the Department of the Environment, Climate, and Communications. It oversees the country's cybersecurity policy, provides guidance for protecting critical infrastructure, and coordinates responses to significant cyber incidents. The NCSC assists both public and private sectors in detecting, preventing, and responding to cyber threats. Additionally, the NCSC serves as Ireland's Computer Security Incident Response Team (CSIRT), offering technical support and managing cyberattacks. However, the NCSC has been criticised for being under-resourced, particularly in light of Ireland's role as a major hub for tech companies, which has led to concerns about its ability to handle the growing cybersecurity demands. In response, the Irish government has started efforts to increase the NCSC's budget and staffing, but it still lags behind larger, better-funded entities like US-CERT.

In contrast, US-CERT (now part of CISA, the Cybersecurity and Infrastructure Security Agency) is a key player in cyber defence for the United States, responsible for incident response, threat analysis, and coordinating national-level defensive measures. US-CERT is more proactive than its Irish counterpart, with significantly more resources and technical capacity to coordinate responses to global cyber threats. Collaborating with federal agencies like the FBI and international alliances such as Five Eyes, US-CERT can manage large-scale incidents, providing comprehensive protection for both public and private sectors.

EU CSIRT (ENISA) plays a critical role in coordinating cybersecurity efforts across the European Union. The European Union Agency for Cybersecurity (ENISA) oversees EU CSIRT operations, providing guidelines, frameworks, and assistance to member states. The EU CSIRT Network, which facilitates cooperation between the national CSIRTs of member states, plays a crucial role in responding to cross-border incidents. Compared to Ireland's NCSC, the EU CSIRT is better positioned to handle transnational threats due to the collaborative nature of its operations, allowing member states to pool resources and share intelligence. While EU CSIRT works in a multinational framework, it faces the challenge of ensuring consistency in cyber defence across nations with varying levels of cybersecurity maturity.

2.8 In Summary

The current state of cybercrime reporting and investigation reveals a range of persistent challenges that require more robust solutions. Although there have been various efforts to improve reporting mechanisms, such as fostering public knowledge and engagement, as well as leveraging technological innovations, these initiatives have not fully addressed the complexities of the issue. Organisational incentives and legal requirements present another critical area where current approaches fall short. The perceived gap in mandatory reporting

reduces the overall effectiveness of incident reporting, leaving many cybercrimes unaddressed by LEAs. Furthermore, despite fears of financial repercussions, research indicates that the long-term impact of breach disclosures on share prices is minimal, which may lead organisations to underestimate the importance of reporting, further complicating efforts to achieve comprehensive reporting of cyber incidents.

Moreover, the literature underscores the necessity for better training and tools for cybercrime investigators. This would include equipment, training, and funding, to bridge the knowledge gaps among officers and improve their ability to manage cybercrime cases effectively. There is also a need for heightened information security and privacy awareness among the general public, which is crucial for fostering preventative behaviours against cybercrime. Socio-technical challenges also play a significant role in the effectiveness of cybercrime investigation. There is an ongoing need for increased awareness and procedural improvements to reduce the trauma experienced by cybercrime victims and ensure that police officers are better equipped to manage such cases with sensitivity and efficiency.

In conclusion, while there have been notable efforts to improve cybercrime reporting and investigation through public engagement, technological innovations, organisational incentives, and enhanced training, these measures have not fully resolved the existing challenges. The persistent gaps in public understanding, organisational compliance, and investigative capabilities highlight the paucity of foundational management information relating to cybercrime, and this inhibits LEAs, and the AGS's ability specifically, to develop more effective and comprehensive strategies. This research attempts to address this gap and in doing so aims to identify viable solutions so that cybercrime reporting and investigation are conducted in a more efficient, ethical, and supportive manner.

3 Research Methodology

3.1 Research Paradigm

This study adopts a positivist paradigm with an quantitative analysis of a variety of broadly related datasets. This research will comparatively assess the respective literature and datasets and develop a set of conclusions and recommendations for possible future research. The datasets in this research are all published, publicly available, datasets. In reference to the legal datasets that this research has compiled, this data is publicly available, but I have used tools that require registration and licensing in some cases, and in one case, I have leveraged a free trial. Data has been analysed through the development of R code scripts as defined in the configuration manual. Some data cleaning has been employed for a variety of reasons, which are discussed in the analysis. The data will be plotted into charts for ease of representation. The aim of the study is to assess the state of the criminal prosecution of cybercrime in Ireland, and contrast that with relevant comparators.

3.2 Data Collection & Analysis

Data were collected by collating publicly available data. This data is primarily published statutory cybercrime and cyber security industry data, either widely distributed on the internet or available upon request from relevant statutory agencies such as the Central Statistics Office in Ireland, the U.S. Federal Bureau of Investigation, or EUROPOC, and companies or institutions like Westlaw.ie or Justis Vlex.

All datasets used in this study include anonymous data relating to crime or cybercrime activities. In the case of the dataset compiled from legal case records, this research has not

used any personal identifiable information (PII) from any of the court records, merely a tabulation of prosecutions for cybercrime offences, be the cyber enabled or dependant.

The respective FBI complaints and costs information were compiled into two datasets and cleaned up to provide a consistent set of metrics across all years. This data took the following form. There were 21 different categories that the FBI used in their reports, and some of these were discontinued or created new during the scoped period of this study. These categories were excluded from this study as we could not analyse or trend the data points in these categories to the same degree as the more consistent categories over the period in question. Both FBI datasets were cleaned in this way, and then their remaining categories compared and where there wasn't a matched pair, this category was descoped from the respective dataset. The approach then taken to analyse the datasets using R code scripts that were created as part of this study. These scripts ordered the data by year, then in order of volume. Some statistical analysis was then performed, and the results plotted in a X-Y graph.

In terms of the dataset collated from the AGS annual reports, this dataset was cleaned up to provide a consistent set of metrics across all years. This data cleaning took the following form: there were upwards of 23 different categories that the GNCCB used in their reports, however only 5 were consistently reported upon across the scoped period of this study. Where categories were discontinued or newly created during the scoped period, they were excluded from this study as we could not analyse or trend the data points in these categories to the same degree as the more consistent categories over the period in question. The approach then taken to analyse the datasets using R code scripts that were created as part of this study. These scripts ordered the data by year, then in order of volume. Some statistical analysis was then performed, and the results plotted in a X-Y graph.

The CSO dataset relating to the Cybercrime Act of 2017 was requested by email from crime@cso.ie and received via a CSV based email attachment. It was a very simple table of data and required no additional cleaning or enhancement for the purposes of this research.

3.3 Ethical Considerations

Ethical approval was obtained from the National College of Ireland Ethics Committee. Any organisational representative that was contacted as part of this research were informed about the purpose of the study. Confidentiality and anonymity were ensured throughout the research process. All communications were logged in section 13 of the configuration manual.

3.4 Limitations of the Study

This study acknowledges certain limitations, including dataset sample size, detail, and availability in available data in Ireland from the CSO, GNCCB, and Irish case law databases.

I worked to develop a comparative dataset in the form of the US FBI data and its detailed taxonomy applied over many years in a consistent manner to use against the relative lack of data from the official reporting channels of the CSO and GNCCB. It was not possible to overcome the limitations of the Irish datasets that I was able to collate, indeed this constituted the source of the one of the main recommendations to come from this report.

4 Evaluation

4.1 U.S. Federal Bureau of Investigation (FBI) Data as International Comparator

It is useful at this point to consider a comprehensive set of cybercrime data in order to better bring its absence in the Irish context into sharper relief. To this end, U.S FBI Internet Crime Complaint Center (IC3) dataset is one of the most comprehensive sources of cybercrime data in the world. It includes reports from individuals and businesses, covering a wide range of cybercrime categories, from identity theft to business email compromise and, similar to the GNCCB data we will discuss below, has been collated from their annual reports. This dataset reflects the breadth and scale of cybercrime in the U.S., which is one of the largest targets for cybercriminals due to its economic size and reliance on digital infrastructure. The 850,000 reported incidents in 2022 illustrate the volume of cybercrime facing U.S. citizens and businesses, and the data helps in understanding the types of cyber threats most prevalent in the country, such as phishing and online fraud. Further reasons for selecting this dataset as a comparator are that for the time period that this study deals with, 2018 to 2023, from the research this is the best publicly available dataset that incorporates significant criminal offences (complaints in FBI nomenclature) detail using cybercrime terminology that is based on law enforcement activities. Secondly, the annual reports include tabulated figures for the estimated cost impacts in dollars of that set of complaint data for each respective year. These complementary datasets show that although phishing/vishing/smishing leads in terms of volume of incidents, in terms of economic impact, Business Email Compromise incidents are by far the greatest cost to the US economy, and yet their volume is comparatively steady over the range of years, as evidenced by their static standard deviation across the range compared to costs.

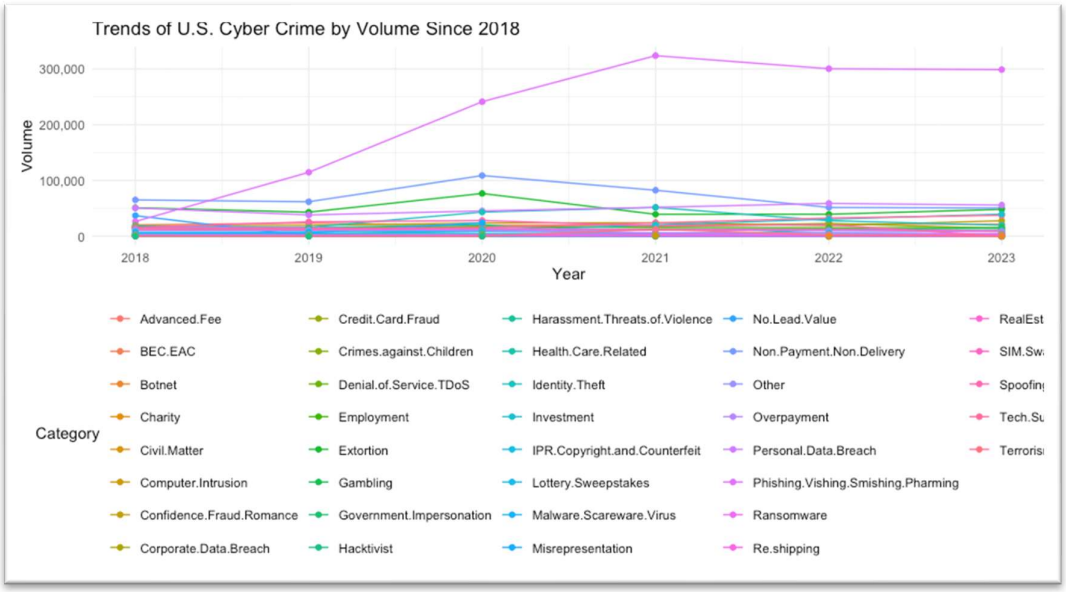

Figure 1 Trends of U.S. Cyber Crime by Complaint Volume Since 2018

We can see from Figure 1 that there a certain number of cybercrime categories that stand out above the others in terms of volume, with one in particular outstripping everything else in terms of growth over the data range in scope, this being the Phishing/Vishing/ Smishing/Pharming category of crime. We can then observe that this particular category plateaus from 2021 onwards. We can also note an increase cybercrime activity as evidenced in bumps in the graph in other categories that we see for 2020, but then drop

back down to pre-pandemic levels. The likely cause of this drop, and the plateau of the Phishing/Vishing/ Smishing/Pharming category of crime is due to the increased awareness of this activity at the time, and consequentially a greater subsequent focus on cyber risk mitigation.

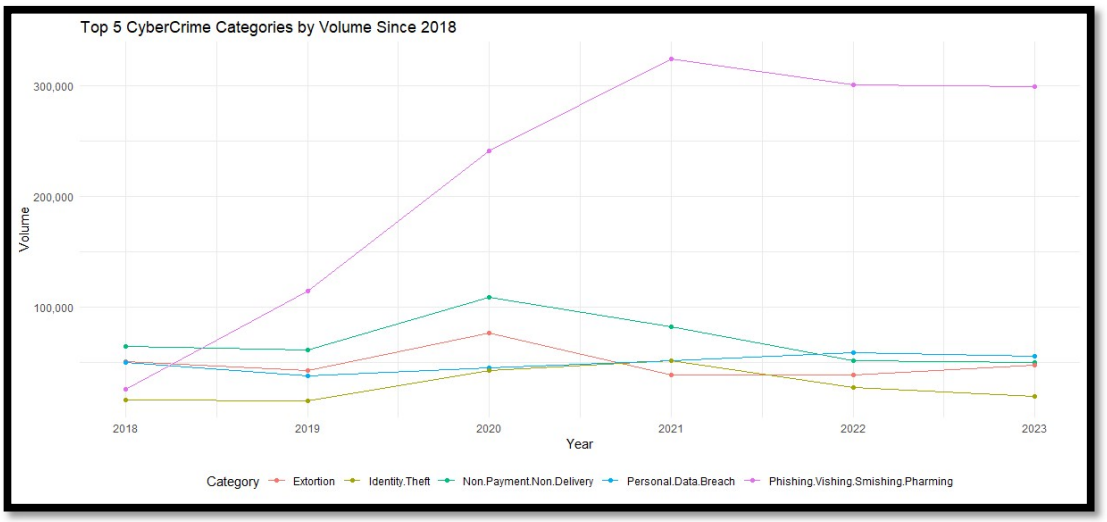

Figure 2 Trend of Top 5 U.S. Cyber Crime Categories by Complaint Volume Since 2018

This graph shows us that these efforts were more effective in decreasing the occurrence of reported incidents in terms of Non-Payment/Non-Delivery and Extortion, as we can see correlated in the costs in Figure 2 above. In the case of the Phishing/Vishing/ Smishing/Pharming category we approach something more akin to a détente or holding pattern, than outright decline in terms of volume.

Table 1 Statistical Analysis of Top 10 Annual U.S. Cybercrime Complaints Since 2018

Category	Mean	Standard Deviation	Minimum	Maximum
Phishing/Vishing/Smishing/Pharming	217628	120424	26379	323972
Non-Payment/Non-Delivery	70083	22235	50523	108869
Personal Data Breach	50122	7443	38218	58859
Extortion	49665	14083	39360	76741
Identity Theft	29140	15079	16053	51629
Tech Support	22911	10225	13633	37560
Confidence/Fraud/Romance	22143	3733	18493	27823
BECEAC	21132	1592	19369	23775
Investment	17857	14928	3693	39570
Credit Card Fraud	16776	3371	13718	22985

We see significant standard deviation numbers for Phishing/Vishing/Smishing/Pharming in Table 1 above and this reflected visually in the significant rate of change in volume. This level of volume, however, does not reward in monetary terms to the same degree that a much lower volume of complaints does in the case of Business Email Compromise (BEC/EAC) does, as evidenced in its extraordinary revenues detailed in Figure 3.

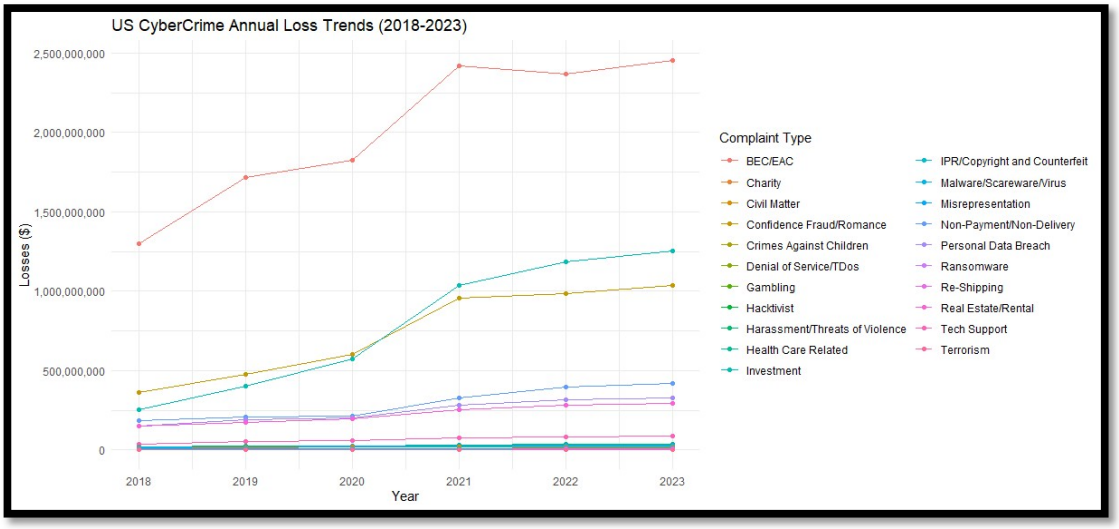

Figure 3 - Trend of U.S. Cyber Crime Categories by Cost in US Dollars Since 2018

4.2 Central Statistics Office (CSO) Cybercrime Data

CSO Data from 2018 to 2023 is taken directly from the AGS PULSE system as "the only source of recorded crime data available to the CSO to produce these statistics". As noted previously there are caveats the CSO have placed on the quality of data from the PULSE system prior to February 2023. This is a blanket caveat applied globally to all PULSE data, so we have to be cognisant of this as it relates to the analysis within this context. The data set I have used is from 2018 to 2023 as PULSE data in general prior to 2018 is further qualified by the CSO in terms of quality and accuracy[21] beyond the caveat of data quality prior to February 2023. This data also close aligns to the timing of the transposition into Irish law of the Cybercrime Act 2017. All that being said, the CSO have stated the following in relation to PULSE data from 2018 to 2023:

"The recorded crime series has been progressively improving over time with the cumulative impact of the improved data quality, assessment, and assurance measures being seen in a higher data quality level as noted in various CSO reviews in recent years."

With an ongoing qualifier to data quality prior to that
"However, some judgement should be exercised by users when using data produced in the earlier years of the Recorded Crime time series given the legacy quality issues which have been commented on in various reviews. For instance, detections data pre- and post-2018 are not comparable given the improved governance controls introduced in that year"

The minimal data set that is used here has been confirmed by the CSO as the sum total of GNCCB data derived from the PULSE system. As per section 13 of the configuration manual and the communications chain detailed there, in offering this data, the CSO representative, unprompted, qualified the paucity of volume of data as relating to the transnational nature of the crimes in question. This view is not inconsistent with the literature review above but

21 https://www.cso.ie/en/methods/crime/liftingofunderreservationcategorisationforrecordedcrimestatisticsfaq/

does not represent the full picture of cybercrime in Ireland as it relates only to the Cybercrime Act of 2017 and only to incidents reported of offences defined in this act. Additionally, the CSO representative confirmed that this dataset does not represent prosecutions and the CSO "do not publish any data on prosecutions" anyway. This statement is authenticated by the two crime datasets available on the CSO website and detailed in section 11 of the configuration manual and on the CSO website[22] [23].

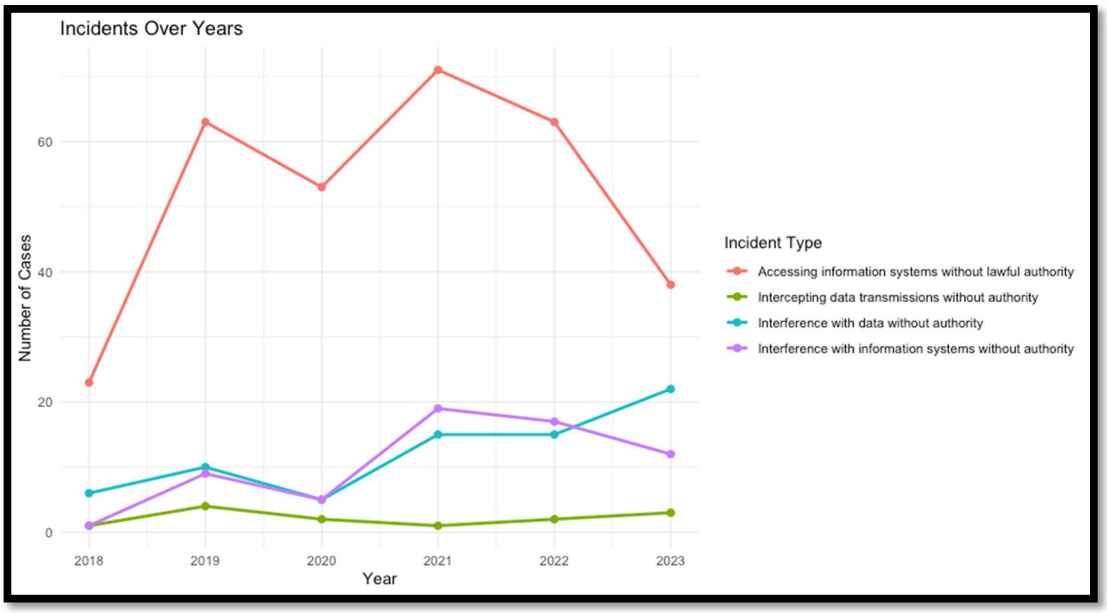

Figure 4. The Incidents recorded related to the Criminal Justice Act of 2017

What we can interpret from this data and associated is in part a confirmation of the research done in relation to the under reporting of crime in general and by extension, cybercrime. When we observe the simple fact of the limited volume of incidents recorded, makes it difficult to produce strong statistical determinations. This serves to underscore previous research findings reference in the literature review relating to under reporting of incidents, training and awareness of AGS in logging incidents that are reported and the inherent technological and data taxonomy limitations within the PULSE system to capture granular relational data. This relational aspect to the dataset is an important one, as we have noted in the literature review, the definition of cybercrime in Ireland has been framed by the Irish Department of Justice as related to, in part, "traditional offences (for example: fraud, forgery and identity theft". There is nothing inherently wrong with this approach, but a well-managed relational database could offer greater insight into the how traditional offences have been affected by modern cybercrime methods.

Similar to the trends observed in the FBI data above, the COVID pandemic appeared to positively influence the rate of occurrence in a downward trend, but we quickly see a recovery in the figures toward an initial post pandemic jump, particularly in occurrences of Accessing Information Systems without Lawful Authority, Interference with Data without lawful authority and Interference with Information Systems without authority. This is reflected in the

[22] https://data.cso.ie/table/CJQ06

[23] https://data.cso.ie/table/CJA07

standard deviations for these incident type across the range of years as shown in Table 3 below.

Table 2 Statistical Analysis of CSO Cybercrime Act of 2017 Offences

Incident Type	Mean	Median	Standard Deviation
Accessing information systems without lawful authority	51.83	58.00	18.12
Intercepting data transmissions without authority	2.17	2.00	1.17
Interference with data without authority	12.17	12.50	6.43
Interference with information systems without authority	10.50	10.50	6.92

4.3 Irish Case Law Review

Although the Director of Public Prosecutions (DPP) in Ireland is the statutory body that determines whether to prosecute or not, again, similar to other bodies, they report in great detail on their primary activities as we see in their annual reports[24], in to legal research in the form of contributions to conferences[25] but do not report publicly in a more granular way on the exact types of offences they work with. The Department of Justice, by the same token, do not separately report on cybercrime incidents or prosecutions, but rely on the CSO to analyse this data for them. The CSO in turn rely on the PULSE system as their sole source of crime statistics and have identified problematic incident resolution taxonomy results such as "Crimes being marked as "detected" when there is no corresponding sanction for the offender (e.g., a prosecution)."[26] This type of data is crucial in the cycle of incident management from inception to final resolution, irrespective of what that may be.
In an effort to collate some data concerning cybercrime prosecutions, this study took the 38 categories of complaint used by the FBI as per above and search for these terms in three different legal case law databases as the only legal searches available in the time afforded for this study. These databases are Westlaw.ie, Vlex.com and Bailii.org as detailed in section 10 of the configuration manual. It is important to caveat that a case law database is not criminal law one, and mostly contains legal decisions and judgements, and as such the results were not impressive. But in the absence of definitive prosecutorial data this was viewed as a viable avenue of research.

Suffice to say that result of this effort was that 22 search were assessed as too generic a term in case law and were excluded due to the prevalence of false positives. For the remaining 16 terms, there were 194 results returned 1 result, duplicated in all 3 databases, for the extradition of man to Poland for the deployment of a malware, botnet and Distributed Denial of Services attack.

4.4 AGS Annual Reports - GNCCB Data

GNCCB is the key national body handling cybercrime in Ireland, making it the best representative of the country's efforts in tackling cyber threats. The dataset includes the only information available directly from the AGS on cases handled, such as ransomware attacks,

[24] https://www.dppireland.ie/app/uploads/2024/05/AR-2022-eng-copy.pdf
[25] https://www.dppireland.ie/publications/conference-papers/page/2/
[26] https://www.cso.ie/en/methods/crime/liftingofunderreservationcategorisationforrecordedcrimestatisticsfaq/

data breaches, and cyber forensics investigations. The dataset also reflects Ireland's growing challenges with cybercrime as it showcases the limited volume of data available, similar to the CSO dataset.

There is a curious disconnect between the CSO Data presented above and the annual reporting data that the AGS GNCCB present in their public annual reports (see Figure 3.) both in terms of the volume and labelling of crime categories, and the volume of investigations that are in train.

That said, even with the admittedly small dataset presented here, we can see broad parallels to other datasets in terms of dips in volumes of case work performed during COVID. It is important to note that AGS as a whole were deemed "essential personnel" during the pandemic and as such, in as much as was possible, were permitted, if not obliged to continue working as normal, subject to certain public health constraints like vaccinations and masking. Rather the dip may represent a lack of facility on behalf of criminals to commit crime as freely as previously, but potentially more insidiously, that the restrictions on the movement of the general public may restricted reporting. Limitations on court cases and how the courts system was run, and the ability to gather forensic items such as hard drives etc., likely affected these figures as well. We see a return to normal new case figures at around the rate of five hundred per annum, but it worth noting that this set of data started with backlog of circa 480 cases going into 2018 as per the AGS report of 2019. Case age was not consistently reported across the AGS reports from this point on, but the very high closure rate in 2022 may indicate the resolution of some of these backlog cases.

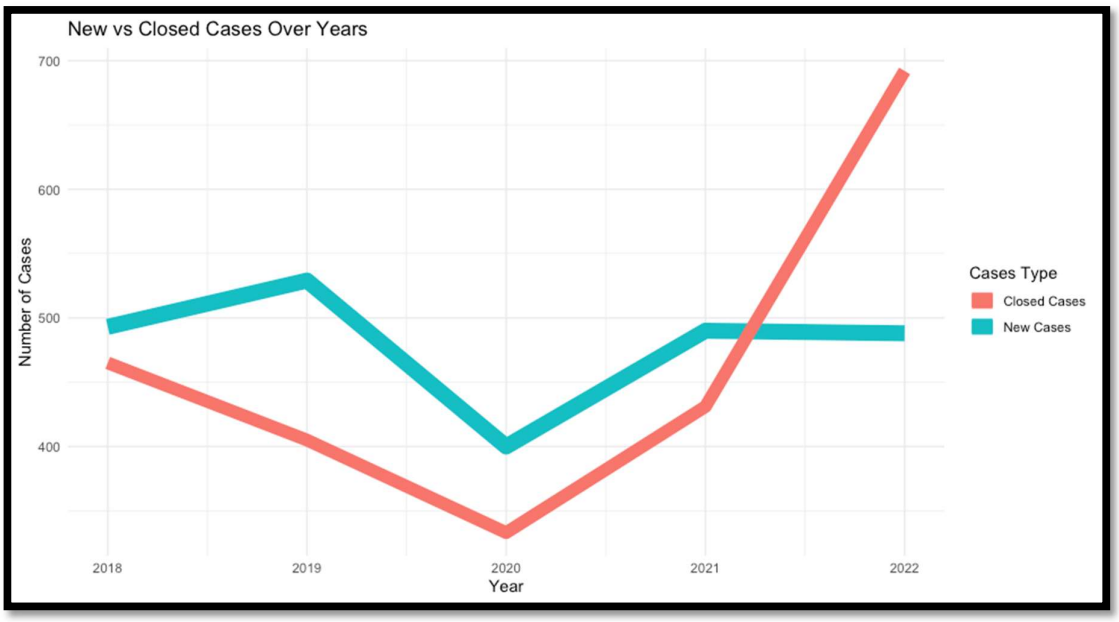

Figure 5. GNCCB Cases worked 2018 to 2022

There are some immediate further qualifiers to this dataset that need to be outlined.

- The data reflected here was collated for this study from the published AGS annual reports.
- The data set represents cases worked as by the GNCCB only, and not AGS as a whole.
- The data set consists primarily of computer forensic cases and some associated investigative cases, the exact nature of which is not specified by AGS or the GNCCB.
- There is no annual report data yet available for 2023 as reports have typically been issued from mid-year of the subsequent calendar year. In more recent years this

report issuance date has slipped to December, with the 2020 report only being published in January of 2022.

- There is mention made in the AGS reports of an internal Garda Research Unit (GRU) as part of internal Garda Analysis Services that collates the annual reports themselves, and also manages the annual public feedback survey called the Garda Attitudes survey; however, it has not been possible to definitively determine this.
- The CSO also clarified the data the GNCCB produced in the annual AGS reports is not generated by CSO but rather the GNCCB themselves or the Garda Research Unit (GRU), an internal research function within AGS. This is one of a few problematic statements I have received from representatives of the CSO, GNCCB, and GRU, as no one has been able to clarify were the GNCCB data has come from. The GRU say the CSO generate the data, the CSO say they get a small subset from the PULSE system relating to the cybercrime Act of 2017 only, and do not know what the categories in the AGS annual reports represent or where they come from.

4.5 European Union Agency for Cybersecurity Cyber Incident Reporting Online Research Data

The European Union Agency for Cybersecurity (ENISA) maintains CIRAS, the Cybersecurity Incident Reporting and Analysis System and collates, aggregates, and anonymises this data into annual summary reports.

In the EU, critical service providers have to notify cybersecurity incidents with a significant impact to the national authorities in their country. These requirements are contained in the following European legislation:

- NISD Article 14 and 16 Essential and Digital services
- EIDAS Article 10 e-ID systems
- EIDAS Article 19 Trust services
- EECC Article 40 Electronic communications (formerly Article 13a)

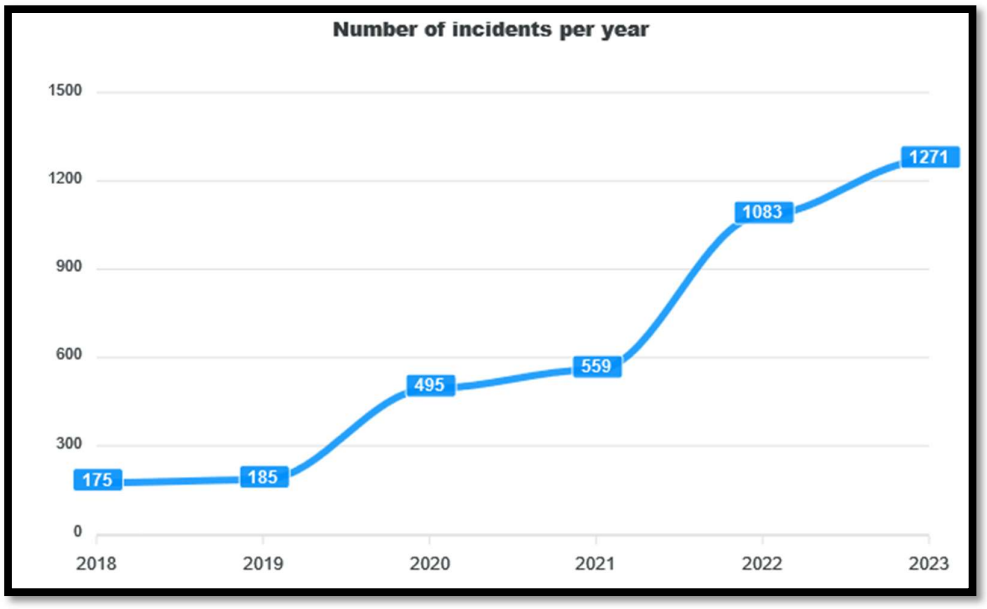

Figure 6 ENISA Collated Incidents by Volume per Year

These incidents are reported as result of mandatory reporting requirements for certain critical service providers as set out in the legislation above. They apply primarily to certain industry sectors as Energy, Transport, Banking, Finance, Health, Drinking Water Supply & Distribution, Digital infrastructure, Communications, Trust and identification services, Digital services and Government services.

We see a trend in Figure 6 that could visually correlate with some of the FBI data, but we have to be careful here to caveat the sources of this incident reporting, as it is not as holistic as the FBI dataset in terms of sources. The reason for this is the limited scope of entities subject to the EU legislation. For example, the legislation "NISD Article 14 and 16 Essential and Digital services", informally known as NIS1, only has 71 entities in its scope in Ireland currently, albeit they are significant structural importance to the country as a whole, i.e. Eirgrid, Bord Gais as critical energy suppliers. As referenced above, NIS2, the successor to NIS1, is currently pending transposition into Irish law with a due date of October 17th, 2024, barring the calling of early general election. NIS1, as recently assessed by the NCSC in Ireland, has almost 5000 entities potentially in scope, with a similar mandatory reporting requirement to be complied with.

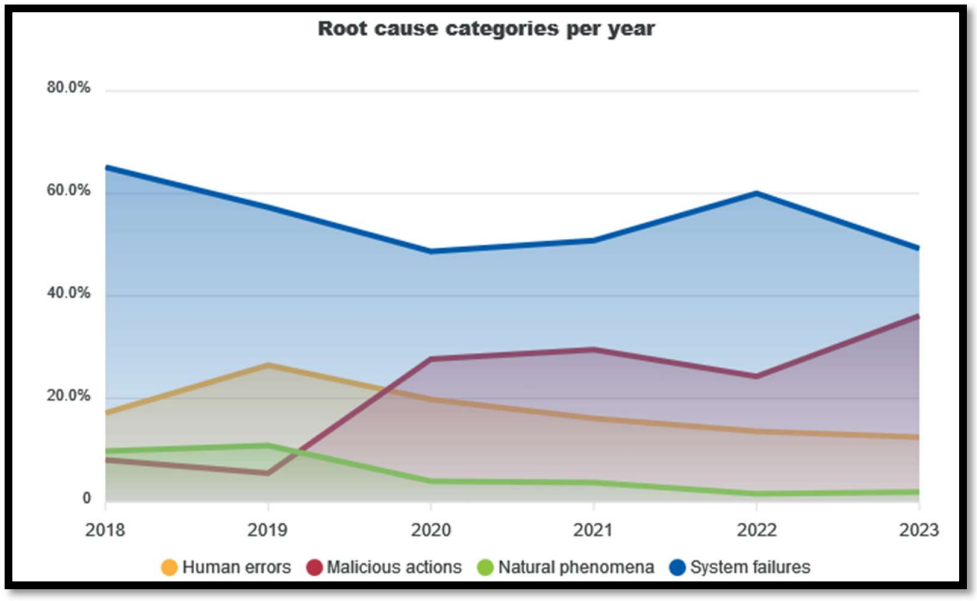

Figure 7 ENISA Collated Incidents Root Cause by Year

Once NIS2 is implemented, then the safe expectation is that these ENISA reports will attain much greater significance in their representation of the state of incident occurrence within the EU, and by extension Ireland. It still has to be caveated that this reporting requirement will still not represent prosecutorial rates and, as we can see from Figure 7, a lot more granular taxonomy will be generated as this as the nature of the entities required to report will intrinsically drive this, for example, costs data.

5 Conclusion and Future Work

How is the incidence of cybercrime in Ireland currently quantified, how does this compare to best practise internationally? In comparison with US and EU Cybercrime data, it has been demonstrated that Ireland fares poorly at best. The US data set is not perfect by their own but does show what Ireland can aspire to. NIS2 as note above, is step forward in terms of the scope of entities subject to mandatory reporting but will not cater for cybercrimes on a

personal level. Prosecutorial date in Ireland should be collected by AGS as per the CSO, but this information either does not exist in any significant sense, or is not reported on, possibly for political reasons but this study has not been able to determine a conclusive reason.

This study has shown that, by any effective measure, cybercrime data in Ireland is in a fractious state. The CSO reports on a particular set of cybercrime incident data but don't report any data at all related to criminal convictions. The GNCCB report on their own internal dataset that is ostensibly gleaned from PULSE, but the CSO by their own admission do not know what the GNCCB dataset is. The GRU maintain they don't perform research or reporting on cybercrimes at all for AGS as a whole or the GNCCB, and they believe the CSO do this. AGS only report on traditional crime via the CSO in their annual reports. The DPP doesn't report on conviction rates only prosecutorial decisions, and the Department of Justice uses the CSO to collate their statistics on AGS activities.

It would appear that none of the statutory entities that could be reasonably assumed to have responsibility for cybercrime data and related statistics, in fact do so. At least not in an holistic manner. The root of this is the PULSE system, which was criticised on implementation and never really shook off that image. This was compounded by the CSO's qualification of PULSE data quality over many years. As a foundation stone of law enforcement data collection at the point of an incident, it informs the quality of reporting and by extension management information[27]. The layering in of investigation management system in conjunction to PULSE, rather than replacing it, has not generated any more management information. It is difficult for any organisation to make good decisions without the requisite data to act upon. The implication here is not confined to AGS and its resourcing and responsibilities, but also directly affects the formulation of governmental policies, and potentially interactions with the National Cyber Security Centre and its incident response capabilities.

We have also discussed in this report the historical culture of antipathy from the Irish department of justice to academic research, and also referenced the technological resistance from AGS to the PULSE system on its introduction, and the subsequent, incremental, degradation of data quality in the PULSE system to the point of declaring significant portions of it of limited use by the CSO. The conclusions that can be drawn from this are that the Irish State has a set of convoluted problems to unpick to remediate this multi-faceted issue of cybercrime. One is cultural, both in the timely adoption of new ideas and technologies from academic research, and the successful rollout of these new approaches. This has not been the Irish States strong suit, irrespective of department, statutory body or agency. A second problem is the holistic management of the various stakeholders when an approach has been adopted. There are legislative challenges in terms of the scope, formulation and implementation of any new laws, there are further skills-based training and education challenges in the policing of any new laws or regulations adopted, and challenges in reporting and public awareness once in place. There is no overarching operational body that is appointed to do this – it may seem that the department of justice is best placed for this, but they do not appear to lead in this regard.

Jurisdictional issues remain a very complicated issue to resolve, but this does not mean that it should not be attempted. Espionage has always been a factor in geo-political relations, but it would appear it has become more public in its visibility in recent years. As always, there appears a certain cognitive dissonance between diplomatic relations and the activities in this area by Advanced Persistent Threats (APTs).

---

[27] https://www.garda.ie/en/about-us/publications/policy-documents/investigation-management-system-ims-.pdf

6 Recommendations

Automated Incident Reporting System.
The FBI has developed a web-based reporting mechanism and the automation of cyber incident triage in the form of the IC3 system. It has some issues of its own, as all systems do. There is an argument to be made that we implement a similar system here in Ireland, and indeed we will, partially, due to the provisions of the NIS2 directive for the legal entities in scope of that. For the general some awareness work has been done, but a system of incident logging may prove invaluable in facilitating better reporting rates. This awareness could be served by trying to raise awareness of the realistic limitations of cyber incident investigations as well.

Investment in Data Systems and integrations to drive organisational improvement

Investment in cybercrime data processing is vital for driving organisational improvement and enhancing the effectiveness of cybersecurity efforts for LEAs. By investing in the systematic collection, analysis, and interpretation of cybercrime data, organisations can make informed decisions that lead to more effective strategies and policies. The key here for Ireland to make progress in this area is to capture and report on data across and incidents lifecycle from technology to improve incident reporting, investigation of reported incidents and their conclusions. As we see from the confused nature of cybercrime data producers and consumers above, this would require an holistic multi-disciplinary, multi-stakeholder approach to scoping and investment. No mean feat in light of the current siloed nature of cybercrime data management currently.

Investment in people and training.

Investment in people and training is crucial for bolstering the capabilities of cyber and law enforcement agencies. As the digital landscape becomes increasingly complex, so do the threats that challenge our security. To effectively combat cybercrime, it is essential to equip law enforcement professionals with the skills and knowledge necessary to navigate the ever-evolving technological environment. This requires not only continuous education in the latest cyber tools and techniques but also fostering a deep understanding of digital forensics, threat analysis, and cybersecurity principles. Moreover, investment in people goes beyond technical training; it involves building a workforce that is adaptable, collaborative, and capable of addressing the multifaceted challenges of modern cyber threats. By prioritizing comprehensive training programs and ongoing professional development, we ensure that our cyber and law enforcement personnel are prepared to protect and serve in an increasingly digital world.

Improvement of International Legal Cooperation Facilities

Enhancing international legal cooperation facilities within the EU and beyond, is essential for improving cybercrime incident response outcomes. In an increasingly interconnected world, cyber threats often transcend national borders, making it imperative for EU member states to collaborate effectively in the face of such challenges. Strengthening legal cooperation enables the swift exchange of information, evidence, and best practices, which are critical for timely and coordinated responses to cyber incidents. By improving these facilities, members states like Ireland can ensure that legal frameworks are harmonised, enabling more responsive cross-border investigations and prosecutions. This, in turn, fosters a unified approach to tackling cybercrime, reducing the gaps that criminals might exploit. Moreover, better international legal cooperation facilities support the development of joint strategies and initiatives, allowing for a more robust defence against cyber threats. Ultimately, investing in the improvement of these facilities not only enhances Ireland and the EU's collective cybersecurity resilience but also sets a global standard for cooperation in the digital age.

Single Point of Coordination of Cyber Defence and Cyber Crime Prosecution.
There should be a decision made in Ireland about which senior minister is going to be responsible as a whole for cybercrime and therefore the coordination of the agencies under one umbrella of control. This is similar to the requirements for ISO27001 certification and the NIS2 directive where Chief Executive Officers and senior leadership teams are required to be aware of and approve cyber initiatives and there is no reason the same should not be done on a national level. To this end, my recommendation would be to appoint the minister for justice in this role, as they are in charge of a significant proportion of the relevant state agencies already. However, the NCSC in Ireland operates under the Department of the Environment, Climate, and Communications and this would need to be changed to reflect the new proposed chain of command.

References

abuse.ch | Fighting malware and botnets [WWW Document], n.d. URL https://abuse.ch/#statistics (accessed 6.17.24).

Adoption of the NIS2 law by the Parliament [WWW Document], 2024. . Cent. Cyber Secur. Belg. URL https://ccb.belgium.be/en/news/adoption-nis2-law-parliament (accessed 5.9.24).

An Garda Síochána, 2023. garda-public-attitudes-survey-2022.pdf.

An Garda Siochana, 2018. garda-annual-report-2018.pdf.

Anmeldelser og sigtelser | Statistik og udgivelser | Politi [WWW Document], n.d. URL https://politi.dk/statistik/anmeldelser-og-sigtelser (accessed 5.22.24).

Away in a hack [WWW Document], n.d. URL https://www.lawsociety.ie/gazette/in-depth/away-in-a-hack (accessed 12.10.23).

Book (eISB), electronic I.S., n.d. electronic Irish Statute Book (eISB) [WWW Document]. Electron. Ir. Statute Book EISB. URL https://www.irishstatutebook.ie/eli/1997/act/20/enacted/en/html (accessed 3.13.23).

Brown, C.S.D., 2015. Investigating And Prosecuting Cyber Crime: Forensic Dependencies And Barriers To Justice. https://doi.org/10.5281/ZENODO.22387

Centre for Cyber Security [WWW Document], n.d. . Cent. Cybersecurity. URL https://www.cfcs.dk/en/ (accessed 3.31.24).

CFCS-the-cyber-threat-against-denmark-2022.pdf, n.d.

commissioner-s-monthly-report-to-the-policing-authority-february-2024.pdf, n.d.

Contact [WWW Document], 2024. . NCSC-FI. URL https://www.kyberturvallisuuskeskus.fi/en/contact-us/contact (accessed 3.31.24).

Crime statistics [WWW Document], n.d. URL https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Crime_statistics (accessed 5.6.24).

Crime [WWW Document], n.d. URL https://www.dst.dk/en/informationsservice/oss/kriminal (accessed 5.22.24).

Criminality in Belgium - The Organized Crime Index [WWW Document], n.d. URL https://ocindex.net/ (accessed 5.8.24).

Cross, C., 2020. 'Oh we can't actually do anything about that': The problematic nature of jurisdiction for online fraud victims. Criminol. Crim. Justice 20, 358–375. https://doi.org/10.1177/1748895819835910

Cyber Crime: An inspection of how the criminal justice system deals with cyber crime in Northern Ireland, n.d.

Cyber Crime [WWW Document], n.d. . Fed. Bur. Investig. URL https://www.fbi.gov/investigate/cyber (accessed 6.17.24).

Cybercrime | Europol [WWW Document], n.d. URL https://www.europol.europa.eu/crime-areas/cybercrime (accessed 6.17.24).

Cybercrime - Crisiscenter [WWW Document], n.d. URL https://crisiscenter.be/en/risks-belgium/security-risks/cybercrime (accessed 5.9.24).

Cybersecurity Label [WWW Document], n.d. . Cybersecurity Label. URL https://tietoturvamerkki.fi/en/cybersecurity-label (accessed 3.31.24).

cycles, T. text provides general information S. assumes no liability for the information given being complete or correct D. to varying update, Text, S.C.D.M. up-to-D.D.T.R. in the, n.d. Topic: Crime in Finland [WWW Document]. Statista. URL https://www.statista.com/topics/7935/crime-in-finland/ (accessed 4.22.24).

Dasgupta, R., 2018. The demise of the nation state. The Guardian.

De Paoli, S., Johnstone, J., Coull, N., Ferguson, I., Sinclair, G., Tomkins, P., Brown, M., Martin, R., 2021. A Qualitative Exploratory Study of the Knowledge, Forensic, and Legal Challenges from the Perspective of Police Cybercrime Specialists. Polic. J. Policy Pract. 15, 1429–1445. https://doi.org/10.1093/police/paaa027
Denmark: number of reported crimes by type 2022 [WWW Document], n.d. . Statista. URL https://www.statista.com/statistics/1178744/number-of-reported-crimes-in-denmark-by-type/ (accessed 4.22.24).
Directive 2013/40 - Attacks against information systems - EU monitor [WWW Document], n.d. URL https://www.eumonitor.eu/9353000/1/j4nvk6yhcbpeywk_j9vvik7m1c3gyxp/vjcf5614azjn (accessed 6.9.24).
ENISA Threat Landscape 2023 [WWW Document], n.d. . ENISA. URL https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 (accessed 5.7.24).
eolas, 2021. Garda National Cyber Crime Bureau: "Most crime has a digital footprint." Eolas Mag. URL https://www.eolasmagazine.ie/garda-national-cyber-crime-bureau-most-crime-has-a-digital-footprint/ (accessed 6.19.24).
EU Policy Cycle - EMPACT [WWW Document], n.d. . Europol. URL https://www.europol.europa.eu/crime-areas-and-statistics/empact (accessed 5.6.24).
European Union Agency for Law Enforcement Cooperation., 2023. IOCTA, internet organised crime threat assessment 2023. Publications Office, LU.
Garda National Cyber Crime Bureau (GNCCB) [WWW Document], n.d. . Garda. URL https://www.garda.ie/en/about-us/organised-serious-crime/garda-national-cyber-crime-bureau-gnccb-/ (accessed 6.19.24).
Garda Síochána Analysis Service (GSAS) [WWW Document], n.d. . Garda. URL https://www.garda.ie/en/about-us/our-departments/garda-siochana-analysis-service/ (accessed 6.20.24).
GDPR Enforcement Tracker - list of GDPR fines [WWW Document], n.d. URL https://www.enforcementtracker.com (accessed 5.14.24).
GetPubFile.pdf, n.d.
GetPubFile.pdf, n.d.
GetPubFile.pdf, n.d.
GetPubFile.pdf, n.d.
GSOC's functions [WWW Document], n.d. . Garda Ombudsman. URL https://www.gardaombudsman.ie/about-gsoc/gsocs-functions/ (accessed 6.29.24).
Hamilton, C., 2023. Crime, justice and criminology in the Republic of Ireland. Eur. J. Criminol. 20, 1597–1620. https://doi.org/10.1177/14773708211070215
Hitting Pause: The unfinished story of the UN Cybercrime negotiations, n.d. . Glob. Initiat. URL https://globalinitiative.net/analysis/un-cybercrime-negotiations-pause/ (accessed 5.12.24).
Human Risk Review 2023 | SoSafe [WWW Document], n.d. URL https://sosafe-awareness.com/resources/reports/human-risk-review/ (accessed 5.22.24).
Information on data - Eurostat [WWW Document], n.d. URL https://ec.europa.eu/eurostat/web/crime/information-data (accessed 4.22.24).
Information security in 2020 – Annual report of the National Cyber Security Centre Finland, n.d.
INSPECTr Project [WWW Document], n.d. URL https://inspectr-project.eu/resources.html#results (accessed 6.20.24).
INSPECTr [WWW Document], 2019. . Univ. Gron. URL https://www.rug.nl/rechten/onderzoek/expertisecentra/step-research-group/project-descriptions/ongoing/inspectr (accessed 6.30.24).
KRP Kyberkeskus (@Kyberkeskus) / X [WWW Document], 2023. . X Former. Twitter. URL https://twitter.com/Kyberkeskus (accessed 3.31.24).
Kundnani, H., 2023. 'The Eurocentric fallacy': the myths that underpin European identity. The Guardian.
Kyberturvallisuuskeskus [WWW Document], n.d. . Traficom. URL https://www.traficom.fi/fi/kyberturvallisuuskeskus (accessed 5.22.24).
Leenen, D.L., 2018. ICCWS 2018 13th International Conference on Cyber Warfare and Security. Academic Conferences and publishing limited.
Legal cases processed in first instance courts by legal status of the court process until 2022 (crim_crt_case) [WWW Document], n.d. URL https://ec.europa.eu/eurostat/cache/metadata/en/crim_crt_case_esms.htm (accessed 5.6.24).
Leppänen, A., Kankaanranta, T., 2017. Cybercrime investigation in Finland. J. Scand. Stud. Criminol. Crime Prev. 18, 157–175. https://doi.org/10.1080/14043858.2017.1385231

Levi, M., 2017. Assessing the trends, scale and nature of economic cybercrimes: overview and Issues: In Cybercrimes, Cybercriminals and Their Policing, in Crime, Law and Social Change. Crime Law Soc. Change 67, 3–20. https://doi.org/10.1007/s10611-016-9645-3
Lifting of Under Reservation Categorisation for Recorded Crime Statistics FAQ - CSO - Central Statistics Office [WWW Document], 2023. URL https://www.cso.ie/en/methods/crime/liftingofunderreservationcategorisationforrecordedcrimestatistics faq/ (accessed 6.3.24).
Lydon, L., Holloway, R., 2022. Why does reporting to authorities matter?
Maundrill, B., 2024. LockBit Leader aka LockBitSupp Identity Revealed [WWW Document]. Infosecurity Mag. URL https://www.infosecurity-magazine.com/news/lockbit-leader-identity-revealed/ (accessed 5.9.24).
McMurdie, C., 2016. The cybercrime landscape and our policing response. J. Cyber Policy 1, 85–93. https://doi.org/10.1080/23738871.2016.1168607
National Special Crime Unit | | Danish police [WWW Document], n.d. URL https://politi.dk/en/about-the-police/national-special-crime-unit (accessed 3.31.24).
National_Cyber_Security_Strategy.pdf, n.d.
Offences recorded by the International Classification of Crime for Statistical Purposes (ICCS) by Year, Municipality, ICCS offence category, Case classification and Information [WWW Document], n.d. . PxWeb. URL https://pxdata.stat.fi:443/PxWebPxWeb/pxweb/en/StatFin/StatFin__rpk/statfin_rpk_pxt_13kq.px/ (accessed 4.22.24).
Publications [WWW Document], n.d. . Garda. URL https://www.garda.ie/en/about-us/publications/ (accessed 6.29.24).
Publications-ResearchPublications [WWW Document], n.d. . Garda. URL https://www.garda.ie/en/about-us/publications/research-publications/ (accessed 6.20.24).
Public_IndsatsResultater [WWW Document], n.d. URL https://statistik.politi.dk/QvAJAXZfc/opendoc.htm?document=QlikApplication%2F2999_Public%2FPublic_IndsatsResultater.qvw&anonymous=true (accessed 5.22.24).
Publikation: Kriminalitet 2018 [WWW Document], n.d. URL https://www.dst.dk/da/Statistik/nyheder-analyser-publ/Publikationer/VisPub?cid=29814 (accessed 5.22.24).
Reported criminal offences [WWW Document], n.d. URL https://www.dst.dk/en/Statistik/emner/sociale-forhold/kriminalitet/anmeldte-forbrydelser (accessed 4.22.24).
Reviews and Evaluations - Garda [WWW Document], n.d. URL https://www.garda.ie/en/about-us/publications/reviews-and-evaluations/ (accessed 6.20.24).
Sangari, S., Dallal, E., Whitman, M., 2022. Modeling Under-Reporting in Cyber Incidents. Risks 10, 200. https://doi.org/10.3390/risks10110200
Social media [WWW Document], n.d. . Police. URL https://poliisi.fi/en/social-media (accessed 3.31.24).
Statistics on offences and coercive measures - Statistics Finland [WWW Document], 2024. URL https://www.stat.fi/en/statistics/rpk (accessed 4.22.24).
Statistikbanken [WWW Document], n.d. URL https://www.statbank.dk/20059 (accessed 4.22.24).
Strategic training needs assessments | CEPOL [WWW Document], n.d. URL https://www.cepol.europa.eu/training-and-education/training-needs-analysis/strategic-training-needs-assessments (accessed 6.20.24).
The Cyber Emergency Response Team (CERT) [WWW Document], 2023. . Cent. Cyber Secur. Belg. URL https://ccb.belgium.be/en/cert (accessed 5.9.24).
The Organized Crime Index Podcast | GI-TOC, n.d. . Glob. Initiat. URL https://globalinitiative.net/analysis/ocindex-podcast/ (accessed 5.8.24).
Thomson, I., n.d. 10 years since the first corp ransomware and no end in sight [WWW Document]. URL https://www.theregister.com/2024/05/08/mikko_ransomware_decade/ (accessed 5.9.24).
Tietoturvan vuosi 2018 [WWW Document], 2019. . Kyberturvallisuuskeskus. URL https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/tietoturvan-vuosi-2018 (accessed 5.22.24).
Tietoturvan vuosi 2020 – Kyberturvallisuuskeskuksen vuosikatsaus, n.d.
Tietoturvan-vuosi-2020_210212_FIN.pdf, n.d.
Tietoturvan-vuosi-2021.pdf, n.d.
Traficom_tietoturvanvuosi_2019_WEB_sivuittain.pdf, n.d.
Vuosikatsaus_2018_tulostettava_sivuttain.pdf, n.d.
Wall, D.S., 2007. Cybercrime: the transformation of crime in the information age, Crime and society series. Polity, Cambridge.
Willits, D., Nowacki, J., 2016. The use of specialized cybercrime policing units: an organizational analysis. Crim. Justice Stud. 29, 105–124. https://doi.org/10.1080/1478601X.2016.1170282