Copyright © 2020 International Journal of Cyber Criminology – ISSN: 0974–2891
July – December 2020. Vol. 14(2): 383–399. DOI: 10.5281/zenodo.4766528
Publisher & Editor-in-Chief – K. Jaishankar / Open Access (Authors / Readers No Pay Journal).

Fighting Cybercrime: A Review of the Irish Experience

Catherine Friend[1], **Lorraine Bowman Grieve**,[2] **& Jennifer Kavanagh**[3]
Waterford Institute of Technology, Ireland

Marek Palace[4]
Liverpool John Moores University, United Kingdom

Abstract

Criminal computer data legislation in Ireland dates to 1991, however its next iteration was not until 2017. Its implementation is still in its infancy and needs an effective, consistent constitutional framework to ensure accountability and action. Irish legislation is important for monitoring 30% of EU data but is limited in its belated modernisation. Therefore, it is important for personal, criminal, and national security defining cybercrime legislation to review current Irish legislation of technology related crimes. Statistics alone cannot interpret legislative efficacy, and therefore qualitative understanding the experiences of digital security practitioners whose professions are directed by relevant legislation could produce beneficial insights. This research analysed interviews with seventeen digital security experts about their professional experiences and opinions relating to cybercrime legislation. Primary emergent themes were identified as: Awareness and prioritisation, jurisdiction and reporting limits, technological advances and the legislative sprawl of dealing with cybercrime today. This research contributes to Irish legal understandings of cybercrime regulation and technology use today and suggests how to address legislative developments in the future, based on the experiences of an expert security panel.

Keywords: Cybercrime, Qualitative, Legislation.

Introduction

Legislators dictate law enforcement response to any activity, and therefore must understand how and why cybercrimes are classified by digital security experts to find meaningful solutions (Holt, Burruss & Bossler, 2015). This reflects the 'human' side of cybercrime, instead of relying predominantly on IT solutions to cybercrime (Hyman, 2013; Kshetri, 2013a; Kshietri, 2013b; Ryan & Harbison 2010). Additionally, it is

[1] Waterford Institute of Technology, Ireland. Email: catherinefriend09@gmail.com
[2] Waterford Institute of Technology, Ireland. Email: lbowmangrieve@wit.ie
[3] Waterford Institute of Technology, Ireland. Email: JKAVANAGH@wit.ie
[4] Liverpool John Moores University, United Kingdom. Email: M.Palasinski@ljmu.ac.uk

important to understand the societal and legal response to emerging cybercrime for the design of new prevention and protection methods. Cybercrime's significance is illustrated in the high costs recorded, for example in a study of 419 companies in 13 countries the average total cost of a cyber data breach was USD $3.62 million, and that the average cost per stolen data record was $141, with the likelihood of recovering lost or stolen data at 27.7% (Ponemon, 2017). In Ireland, between 2017 to 2019 the cost to online fraud was estimated at €3.1 million (Government of Ireland, 2019). Online technologies and Internet Communication Technologies [ICT] areas supplied 4.4% to the Irish economy GDP as early as 2013 (Department of Communications, Energy and Natural Resources, 2013), monitoring an estimated 30% of EU data (Government of Ireland, 2019). These reports emphasise the significance of Irish legislation, but are challenged by differing rates of cybercrime gathered from varied sources and data gathering methodologies (McIntyre, 2015). For example, law enforcement statistics categorised cybercrimes in 2008 as property damage or dishonesty crimes (McIntyre, 2015), and there is still no cybercrime category in the Central Statistics Office [CSO] to this day. For the sake of illustration, keeping in mind the limited categorisation of cybercrime the CSO recorded a 14% increase in fraud offences between 2019 and 2020 (Central Statistics Office, 2020). This is further limited by estimated reporting as low as 7.7%, attributed to low awareness of cybercrime by public and professionals (Öğütçü, Tistik & Chouseinoglou, 2016).

Cybercrime has been described as a range of behaviours involving crimes assisted by and targeted against computers, that harm an individual or society for private gain (Brenner, 2007; Dashora & Patel, 2011; Fahey, 2014; Ionescu, Mirea & Blajan, 2011; Regoli, Hewitt & Maras, 2013; Yar, 2006). Cybercrime legislation needs to recognise that online crime may not functionally be analogous or equivocal to offline legal scenarios, which can be illustrated by a wider victimisation pool and opportunities for anonymisation of offenders (Felstiner, 2011; Van Royen, Poels & Vandebosch, 2016; Wada, Longe & Danquah, 2012). Though conducted primarily through the internet, cybercrime has physical real-world consequences, including physical harm from online threats, infrastructure disruptions, trade obstruction and information validity concerns (Ashmore, 2009; Awan & Zempi, 2017; Holt, Bossler & Spellar, 2015; Khadam, 2012; Kshetri, 2013a; Kshetri, 2013b; Lastowka, 2010; Uma & Padmavathi, 2013; Wada et al., 2012; Vlachos, Minou, Assimakopouos & Toska, 2011). Globally, cybercrime legislation is still in its infancy and needs an effective and consistent constitution and framework (Collinwood & Broadbent, 2015; Hunton, 2011). Legislation is important for deterrence; without it, crime threatens societal and economic growth, having varied but costly consequences (Dashora & Patel, 2011; Holt & Turner, 2012; Hyman, 2013; Ionescu, 2012; ITU, 2012; Regoli et al., 2013). Furthermore, ongoing communication advances create more opportunities for cybercrime and cybervictimisation through higher internet of things [IoT] proliferation, and is often influenced by traditional crime methods (Armencheva & Smolenov, 2015; Holt & Turner, 2012; Hoscheidt & Felber Eichner, 2014; Ion, Langheinrich, Kumaraguru & Capkun, 2010; Mishna, Cook, Saini, Wu & McFadden 2010).

Both low reporting and problematic measurement of cybercrime necessitate a greater focus on the legislation required in this area, and the role of experts in the detection and prevention of cybercrime. Considering its early negative impact, O'Connor and Gladyshev (2006) estimated a cost from data breaches by 76% of respondents of over €5,000 due to [cyber] victimisation to Irish businesses and 22% of respondents reported of costs of over €100,000. Although this data is too dated and too early in the years of cybercrime as we know it today to indicate realistic rates, it gives an indication that cybercrime itself is not new. Both early and later data, such as Government of Ireland (2019)'s cost estimation of €3.1 million, highlight the need to review legislative processes on cybercrime in Ireland.

Primary cyber-related criminal legislation in Ireland

There have been laws in Ireland used primarily to defend against cybercrime, these include: Criminal Damage Act 1991 [covering property damage and data access]. It had a limited understanding motive, permission and scope of [digital] property damage with ambiguous terms of operating a computer and a limited understanding of intent. Although it boasted the first mention of 'computer', the legislation was not specifically written with computer crime in mind. Next was the Criminal Justice (Theft and Fraud Offences) Act 2001 [covering data access, though mainly focused on extending warrant powers and rarely used for prosecution (Ryan et al., 2016)]. It maintained ambiguous definitions of 'computer' and 'operate' and ignored mixed modal crimes. However, it did first acknowledge corporate responsibility and perhaps the vague nature of the provisions allowed room for development in its implementation. Third was the Criminal Justice (Offences Relating to Information Systems) Act 2017, which introduced the term 'Information systems', an updated 'data' definition and acknowledged intent of harm which removed the remit of the 1991 Act. It extended the scope of attacks, the scope of data transmission, elements of social engineering and machine tools to do so as well furthering corporate liability in data attacks. Finally, the Harassment, Harmful Communications and Related Offences Bill 2017 [formerly the Non-Fatal Offences Against the Personal Act 1997 which defined 'communication', 'harassment', 'distributes', 'publishes', extended the scope of harassment to online actions. For example, cyberharassment, cyberbullying, cyberstalking, which addressed indirect harassment and corporate liability.

Each provision has improved upon the last and required legislation to reconsider what constitutes technology today, what was its original purpose and what potentially could technology be used for in the future. For example, cybercrime has been described as the "unauthorised or unethical use of technology" which is now not limited to a personal computer (Fafinski, 2009; Khadam, 2012). This was reflected in improvements from the 1991 Act to the 2017 Act in the 2017 Act which formally recognised computers as part of a system rather than a standalone unit.

Limits to legislation

Keane (2007) suggested that it was possible to be prosecuted for various computer-related crimes in Ireland [with the 1991 and 2001 Acts] however, the interpretation and application of the Acts at the time influenced their effectiveness. For example, over-broad legislation to allow a one-size fit for all instances in computer-related offences, inconsistent use, incorrect application to cases, low legal, or professional expertise and public education (Armenchava & Smolenov, 2015; Clough, 2011; Dashora & Patel, 2011; McIntyre, 2005; Ryan, Browne & McDermott, 2016; Ryan & Harbison, 2010). This could lead to: Ineffective policing, evolving perception of appropriate sanctions, higher pressure on resources, censorship, and a remaining prioritisation of physical harm over cyber offences

(ITU, 2012; Yar, 2006). Additionally, the fast pace of cyber technology developments, its [mis] requires consideration in the formulating of legal amendments.

Legislation has been criticised for being rushed, opting for "quick and easy" solutions, attempting to solve a problem after the fact with amendments to existing laws, instead of taking the time to assess security strategies in the face of economic loss (Colombo, 2009; Dashora & Patel, 2011; Ion et al., 2010; Kaiser & Brown, 2015; Palasinski & Svoboda, 2014). Legislation may also be focused more on helping business growth rather than crime regulation (Dashora & Patel, 2011), and different judicial systems with alternating legislative power, complexity, regulation and punishments (Armencheva & Smolennov, 2015; Brenner, 2007; Fahey, 2014; Horsman, 2016; Hoscheidt & Felber Eichner, 2014; Karabacak, Yildirim & Sevgi 2016; Khadam, 2012; Ruttenberg, von Mehren & Yen, 2013; Tonry, 2011). Add to this, the length of time to assess resource and legal framework strength regarding deterrence and penalty efficacy (Kaiser & Brown, 2015; Öberg, 2013).

Therefore, legislation needs to reflect changes in society over time (Regoli et al., 2013; Ruttenberg et al., 2013), to reflect the pervasive and ubiquitous nature of computer and internet use, with proportionate punishments and consequences (Kesan, Hayes & Bashir, 2016; Mishna, 2008; Padmanabhan, 2012). This may involve questioning the original purpose or function of a computer with clear principles of what is considered a breach of the law (Fafinski, 2009; Öberg, 2013). The sixteen year legislative gap between 1991 to 2017 missed an opportunity to keep abreast with technology developments, which the impetus to do so could have been hindered by underreporting cybercrime (Collingwood & Broadbent, 2015; Dashora & Patel, 2011; Hoscheidt & Felber Eichner, 2014; Ionescu, 2012; ITU, 2012). These updates require implementation into new legal frameworks (Collingwood & Broadbent, 2015) requiring engagement with experts who can offer first-hand information about such issues.

Exploring police officer cybercrime awareness as first responders to cybercrime could offer an understanding of legislative developments taking place. For example, Holt and Bossler (2012) found that investigative responsibility, professional support, and perception of cybercrime as a 'real' crime were integral themes to law enforcement attitudes toward cybercrime. The finding contributes to understanding that an alteration in the legal system is required to recognise computer crime, to set appropriate penalties, increase training resources and create a clear line of accountability. Similar findings were reported by Millman, Winder and Griffiths (2017) in their interviews with 8 police officers on their experiences in dealing with cyber harassment. This current research expands Millman et al. and Holt and Bossler's work while focusing on professions that are directly influenced by current legislation. Cyber-specific personnel would offer higher knowledge and experience to comment on procedures in place deal with cybercrime than the "everyday officer" than in Holt and Bossler (Whelan and Harkin, 2019).

The present study

The present study focuses on the perspective of digital security expert [DSEs] experiences regarding the implementation and impact of Irish cybercrime legislation in digital security. Seventeen Irish based DSEs were interviewed including law enforcement, legal personnel, and IT experts in Ireland.

The research questions are:

1. How is current cybercrime-related legislation perceived and utilised by digital security experts in Ireland?
2. What recommendations can be made to improve cybercrime-related legislation in Ireland?

Method

This study was approved by the first authors Institutional ethics board. Interviewees were contacted following their completion of a short qualitative online survey regarding cybercrime legislation and awareness in Ireland. The survey was distributed online to professional digital security working groups in Ireland through the first author's Twitter and Linkedin accounts. A convenience snowball sampling approach was used to reach participants which self-selected to participate in the survey and who indicated their consent to be contacted for follow up interviews. From the 35 respondents to the online survey, 17 (male=12, female=5) volunteered to take part in a follow up semi-structured phone call interview based on the survey questions. All interviews were conducted between June 2017 to June 2019. Questions included: How does your work connect to technology-related crime? What in your opinion, are the main areas of concern in approaching technology-related crime today? How does legislation play a role in your line of work in connection to technology-related crime? How have you/your categorized approached technology-related crime to date? Do you/your categorized collaborate with any other organisations in approaching technology-related crimes? Where do you see the development of legislation against technology-related crime moving to in the future?

Each participant's data set was categorize during subsequent transcription [the first participant interviewed became P1 etc…]. Participants 1-3 represented law enforcement in Ireland, participants 4-11 & 13-17 represented IT specialists and participant 12 represented a legal specialist in Ireland. The interview data was qualitatively analysed using a thematic approach. Qualitative methods are particularly useful where samples sizes of participants are small and interviews are being conducted to gain an understanding of a particular perspective. Thematic Content Analysis (Braun and Clarke, 2006) is appropriate in this case as it allows for emergent themes of the participants to be identified and categorized to gain a deeper understanding of concerns and awareness of cybercrime legislation in the Irish context. In this study, each transcript was transcribed, reviewed for broad codes and subsequently categorized into specific themes that gave insight to experiences (Braun and Clarke, 2006; Castleberry & Nolen, 2018).

Results and Discussion

It is important to note that the most mentioned theme does not necessarily equate to its relative importance (Braun & Clarke, 2006) as this data relates to the individual experiences of each expert. As such, emergent themes are not mutually exclusive and illustrate the interconnectedness of cybercrime issues discussed previously in this paper: Public and practitioner awareness [37] and subtheme; offence prioritisation [10], issues and challenges concerning jurisdiction [27] and subtheme; problems in reporting (in particular lack thereof) [9], challenges of technological advances [17] and legislative sprawl of policing and legal deterrence [9]. Anonymised quotes are included to demonstrate themes in the discussion below.

Awareness & Prioritisation

All participants showed in-depth knowledge and awareness of cybercrime technology, for example crimes assisted by, targeted at or technology used during the commission of a crime. Both human and technology aspects of cybercrime were highlighted in the interview data: "…within our remit, we don't just look at technology, we look at people themselves, who are they…" [P13]. This included social engineering, deception and multi-modal scam methods. However, participants recognised that relevant expertise was rare and highlighted the importance of education across professions in the form of professional development. For example, from the everyday police officer, "first responders" [P3] to more cyber-centred professions in policy creation. Education can come from academic qualifications, standardised security certificates, public consultation, and above all, research and collaboration. Topics recommended for cross board training included, ethical hacking, good technology policy practice to combat social engineering deception. These use clever manipulative methods to take advantage of employee or procedural weaknesses through technology [P13]. Although technology can be used to exploit cyber weakness in fast developing ways, it is the human agents themselves that are the weak link [P9].

Cybercrime awareness is hampered by the lack of training in relevant professional security sectors in an area that is dynamic and fast moving involving under reporting, low funding resulting a negative view of law enforcement (Brenner, 2007; Lynch, 2014). Participants in this study attributed legal limits to the novelty of cybercrime for example, the lack of; precedent, legislation, collaboration across agencies who deal with cybercrime and legal jurisdiction differences. Additionally, the lack of specific training for cybercrime investigators requires significant time and resource investment: "…a combination of skills picked up on over probably 10-15 years or more" [P5]. Depending on the priorities of the industry and legal systems, education priorities will differ. "The big part of the problem is getting companies, people, organisations, governments, to recognise the extent of the problem", with a focus on case-by-case incidents despite 1000 breaches in countries every year [P14]. As a result, there is a reliance on private industry for public services for cybereducation and participants noted that education efforts remain low, even with victimisation potentially becoming a common occurrence. For example, general law enforcement personnel may be aware of most common terms such as Facebook, they require large amount of legal knowledge to deal with online cases [P1].

As such, who is responsible for providing education? One participant stated that the media outlets could reduce "paranoia and the hysteria" by advertising safety precautions. P11 ultimately saw the responsibility falling mainly with the Irish criminal courts for ensuring effective awareness of cybercrime. Participants noted an increased corporate interest in cybersecurity, but if responsibility lies instead in the corporate domain, overload with corporate compliance sprawl, multiple compliance frameworks to adhere further confusing legislation awareness could be a concern [P6]. P15 recommended a holistic cohesive approach to cybersecurity responsibility, while P7 conversely, noted that it is up to the individual to take responsibility for his or her own awareness and education of cybercrime legislation. Education is recommended to reduce the probability in engaging in victimisation behaviours and may potentially help law enforcement resource allocation for training in highlighted areas (Ho, Lin, Lu & Huang, 2011; Holt & Turner, 2012; Mishna et al., 2010; Saridakis, Benson, Ezingeard & Tennakoon, 2016; Yar, 2006). With a perceived lack of governmental legislative movement against cybercrime, change was predicted to come from either top-level or public "grassroots" movements. For now: "… it's not growing, it's not changing rapidly…" [P15].

Overall, awareness was the most salient legislative theme identified in this research but the priority of cybercrime in Ireland may remain low in comparison to other social and economic concerns for example, unemployment and homelessness. Therefore, P7 recommended not relying on a big event happening for change to happen just to "score cheap political points" and to therefore, be proactive in working on cybercrime legislation and its related issues. Cyber security education and management strategies should be treated as main priority. "[Technology is] … constantly evolving, there's no one size fits all and what works this year will not work in two years' time" [P5].

Prioritisation

Limits to legislation result in low commitment by law enforcement or courts to take internet and technology related cases seriously, with few legislative alterations exacerbating the issue (Ryan & Harbison, 2010). As such, a sub-theme of awareness emerged as the perception of seriousness of cybercrime. The prioritisation of other issues over technical, professional and public education has led to a legislative deficit and remains a conundrum within the perception of cybercrime not being a "real" [i.e., offline] crime [P3] where a "real" crime gains priority over cybercrime. In other words, the average person does not view an offence carried out online as being as harmful as a direct or offline crime to an individual. Therefore, this has resulted in this area of regulation not receiving the same amount of attention. The lack of cybercrime data and precedent for offences also limits understanding. Reflected the Irish Law Reform Commission report (2014), recommended for online harassment to be taken more seriously with regards to its prevention and penalties. P1 and P2 reflected that this affected any cybercrime legislation which is not acknowledged for the depth of potential harm compared to offline crime and not appreciated as different from offline crime. Participants felt that this would remain a limit to legislative effectiveness and a priority of harm will continue to be used as a benchmark for legal responses: "Cybercrime isn't always seen as a 'major' crime in most countries because it is heavily underreported" [P5]. This may imply that cybercrime victims may still fear not being taken seriously and resist reporting incidents (Goucher, 2010).

Jurisdiction & Reporting

Cybercrime involves a lack of temporal and geographical boundaries which legislation cannot ignore (Hancock, Curry, Goorha & Woodworth, 2008; Hancock & Guillory, 2015). Participants identified the need for international partnerships for education and cybercrime investigations which is in line with literature who also recommend a clear communication and legal structure to ensure effective prosecution and penalties (Holt et al., 2015; Yeomans, 2014).

Although Mutual Legal Assistance Treaties [MLATs], European Arrest Warrants (EAWs) and informal collaborations were reported in use by participants, limits remain where there must always be a "like-for-like" legislated offence scenario between the different legal jurisdictions [P2]. Similarly, there will also likely be multiple legislative frameworks at play for example, criminal and financial which reflect judicial systems with alternating legislative power, complexity, regulation and punishments (Armencheva & Smolennov, 2015; Brenner, 2007; Horsman, 2016; Karabacak et al., 2016; Khadam, 2012; Tonry, 2011). Participants noted the inconsistencies in use, implementation, and cooperation across jurisdictions and interestingly, P3 saw international legislation as less effective than domestic, due to the increased complexity of multiple legal frameworks. For example, the practical legislative limits of physical tracing, apprehension, extradition and sentencing between different locations of the offender and the victim. This is due to jurisdiction and chain of evidence issues in determining the point of origin of cybercriminal activities (Hoscheidt & Felber Eichner., 2014; Ionescu, 2012). To add to this, international corporate organisations and businesses remain "in the middle" of jurisdictions and different legislative frameworks further compounding jurisdiction legislative problems [P4].

Since cybercrime exists internationally and does not remain in a legislative "vacuum" where legislation and its effectiveness stop at international boundaries [P1], collaboration is required. However, collaboration may also be seen as the "extra step" and not necessarily required in legal approaches to cybercrime [P5]. Instead, informal collaboration was reported as the most likely form of communication between agencies reported by participants. Therefore, perhaps a "global internet act" [P3] to address a "global problem" [P14] and the collaboration between social media companies in the EU could work towards legislative improvements. International and industry cooperation improvements could come from experts in multi-disciplinary work, sharing government initiatives and frameworks to enhance legislative efforts (Bedrijfsrevisoren et al., 2015; Brenner, 2007; Changa, Ramachandrana, Yaob, Kuoc & Lid, 2016; FBI, 2015; Hoscheidt & Felber Eichner, 2014; GrantThornton, 2015; Hunton, 2011).

However, the current differences and inefficient international legislation/investigations has resulted in an "international quagmire", where an international streamlined approach was recommended with the current approach is seen as "… very clumsy and doesn't really yield a whole lot of results, unfortunately" [P7]. This has left international arrest agreements still requiring a lot of "red tape" and "bureaucracy". For example, a legal procedure may start in Ireland, go to Germany, onto the Ukraine, onto Singapore and then to Brazil [P7]. There has been an amendment to this situation subsequent to the interviews in the Criminal Law (Extraterritorial Jurisdiction) Act 2019 where a crime that is committed abroad is also illegal in Ireland then it can be tried in Ireland which may be used to mitigate this procedural issue. However, participants believed that Irish legislation at the time did not cover jurisdiction complexities and that ultimately prosecution, using the then current legislation was ineffective:

> "For example, every cybercrime is immediately international. You have the victim in one country, you have the suspect in another country, there's probably three or four servers across other countries. Immediately we have, unlike any other crime, 4/5 jurisdictions involved. They all have their own laws, penalties, and laws of extradition and everything else. If that became synced up more, at least in Europe, where we had certain standard Acts across all of Europe then the same crime in France, in Germany, even in Ireland" [P5].

Reporting

'Reporting' is integral to cybercrime defence limited by its cross-jurisdictional nature, unclear accountability and poor definitions (Brenner, 2007; Fahey, 2014; Hoscheidt et al., 2014; Kshetri, 2013; Ruttenberg et al., 2013). "I have spoken with the Gardai [Irish law enforcement agency] …The biggest problem they see is that people here just aren't reporting cybercrime" [P7]. Additionally, even finding a suitable offence can be difficult with no one specific section available for online offences let alone international offences [P1]. [*It should be noted that participants were interviewed just after The Criminal Justice (Offences Relating to Information Systems) Act 2017 which encompassed a jurisdiction element, was just ratified and implementation had yet to be observed*]. While corporations may do enough to suffice basic legal requirements in reporting [for example, in line with the General Data Protection Act 2016] [P7], persons may not want to admit victimization. Victims may risk corporate reputation, fear admitting carrying out risky or illegal behaviours and they may fear an imposed or forced limit to technology use because of reporting victimisation (Case & King, 2014). An "everyday person" may also be embarrassed about being victimised particularly if it involves a sensitive offence [P2].

An implication of increased legislation may result in increased reported incidences, leading to increased court cases which would require further investment in personnel and resources to deal with offences [P11]. There was doubt as to whether the Irish legal system could handle this influx of cases indicating a need for a national framework to not stay behind cybercrime (Arthur Cox, 2013). Yet even when reporting can help detect a crime or the offender, the underreporting paradox remains according to participants: When a digital security or law enforcement agency is asked to produce statistics to show the severity and prominence of cybercrime, the statistics may not be available or only show that there are low levels currently reported – or detected: "The statistics don't measure up" [P2]. The hidden nature of online crime or the "dark side of the web" has inhibited research resulting in difficulties in detecting and tracing perpetrators and reluctance to report breaches by businesses [P5] (Brenner, 2007; Dashora & Patel, 2011; Holt et al., 2015; Hoscheidt & Felber Eichner, 2014; Hutchings, 2014; GrantThornton, 2015; Leong, 2014; Uma & Padmavathi, 2013). As such, the low cybercrime detection rates and identification of cybercriminals also reflect research difficulties with more effort needed on the issue (Brenner, 2007; Dashora & Patel, 2011; Leong, 2014; Levin & Ilkina, 2013). In trying to understand the true cost of cybercrime, P7 recommends that most security research is unbiased in reporting facts, even those trying to sell a security product. Either way, governments must start taking notice that cybercrime affects the public economy and thus need to find ways to measure cost: "It's a bit like trying to put an estimate on the illegal drug's trade as well. The cartels don't exactly issue tax returns ever year." [P5].

Technology

Legislative reform is also exacerbated by swift technology development: "The problem is that as technology increases exponentially, you've got tech' out there for which there is no case law, there is no precedent" [P9]. The lengthily time required to assess legislative robustness is continually challenged by rate of technology development (Kaiser & Brown, 2015; Öberg, 2013). For example, higher online connectivity and reliance on online communication methods can create more opportunities for cybercrime and cybervictimisation (Armencheva & Smolenov, 2015; Dashora & Patel, 2011; Holt & Turner, 2012; Hoscheidt & Felber Eichner, 2014; Ion et al.; Lastowka, 2004; Mishna et al. 2010; Smith, 2008). As such, P7 predicted an increase of IoTs which implied higher cybercrime rates should occur (Uma & Padmavathi, 2013). Therefore, defining and regularly updating cyber legislation is important for personal, criminal and, national security with continuing research paramount to accomplish this goal (Longo, 2013). As such, recognising the ubiquity of technology is key:

> "Technology is pervasive through everything we do, every industry every day. The idea with technology from a mobile device, desktop, perspective all the way out to the end-points which include a variety of technology systems from surveillance systems and radars, and seismic sensors, and security cameras and motion sensors, all of that kind of stuff... It's a lot of technology" [P14].

Defensive technology has remained the primary response to cybercrime, rather than preventative measures leading to further prosecution difficulties (Dashora & Patel, 2011; GrantThornton, 2015; Hyman, 2013; Kshetri, 2013a; Kshetri, 2013b). Defensive strategies alone are time consuming, costly, and unsustainable since effective prosecution cannot happen without effective prevention (Grant Thornton, 2015; Hoscheidt & Felber Eichner, 2014; ITU, 2012). This creates a cycle of trying to defend against cybercrime with sophisticated software developments while the cybercriminal continues to remain a step ahead (Bryant, 2015; Dashora & Patel, 2011; Holt & Turner, 2012; Smith 2008). Therefore, allowing research to understand technology use now involves multifaceted legal issues is important. However, research is impeded by unclear potential liability of security researchers: "…it's very difficult to do [research] properly and safely, to do research or to do investigation into issues without going into or getting in front of law enforcement" [P15]. As P15 further highlights, herein lies the modern information age paradox where unsecure information is easily found online, yet potentially liable to offence if searched for or viewed, thus revealing the inefficiency of research and security work. Thus, a need for policy creation with engagement from technology professionals and researchers is required, to address limits in legislative approaches which are no longer hardware specific for example, what computer is used, but includes software vulnerabilities, human users.

Legislative sprawl

Although legislation of cyber-related offences is present in Ireland, "the legislation has got to find its way into organisations policies and procedures" [P10]. The complex network of legislation requires simplification where actions are "put into context" [P1, P2] instead of appearing across multiple un-related legislative provisions. For example, criminal offences relating to jurisdiction occurs in both the Criminal Justice (Offences Relating to Information Systems) Act 2017 and the Criminal Law (Extraterritorial Jurisdiction) Act 2019. Another example could include victim data breach disclosure, where vitims may not be legally obligated to report under the 2017 Act but may be required to do so under the General Data Protection Act 2016 Art. 33. However, cybercrime legislative training and resources are "… not even one step behind, it's a few steps behind" [P4] challenging legislation awareness. Even with potential instruments to prosecute cybercrime in Ireland (Keane, 2007), interpretation, of the sprawling and ambiguous nature of current provisions may inhibit efficacy. For example, definitions that remain too broad, varied, overlapping or require further debate on labelling and categorisation based on the nature of the crime and technology use (Brenner, 2007; Holt & Turner, 2012; Khadam, 2012; Lastowka, 2004; Murray & Kelleher, 2016; O'Moore, 2013). A conclusive Cybercrime Act would also give clarity to the "big disparity" of actions legislated for online and offline such as hate speech which is dealt with much more swiftly offline than online [P4]. Without giving legal clarity to reduce legislative sprawl, this could decrease legislative efficacy. P3 likens this to the increased complexity of international to domestic legislation which results in more challenges to overall legislative efficacy. However, increased legislation could result in overcriminalisation and proportionality should be considered: "[Legislation is…] so broadly termed that anything that goes outside the expectations of the person that created the system could be deemed to be breaking the legislation and therefore, breaking the law." [P15].

> "…the question you have to ask yourself is cybercrime different from other forms of crime, in terms of actual type of that is being done, is it fundamentally different in terms of data or is it different in the mechanism is being used to commit the act?....If the difference is in the mechanism that is being used, is the existing legislation robust enough to cover that?... Is legislation always firefighting and maybe a losing battle trying to catch up?... Or should legislation be cast in a very broad way that it should cover all sorts of future eventualities that we haven't even though about?" [P10]

Overall, time is required to develop new approaches to emerging cybercrime legislative regulation, where online crime should be treated as "completely different" [P4]. For example, P8 described the complex procedures of evidential gathering and additional burden of proof in digital crimes as different from online crimes. However, cybercrime legislation must avoid over-criminalisation, seek proportionate sanctions, and consider offender motive. For example, be able distinguish between malicious data access for personal gain or accidental data access. Unfortunately, P5 predicted no significant European legal changes regarding cybercrime with increased nationalisation instead of collaboration over the next 5 years. However, participant thoughts on whose responsibility it is to push legislative reform remained mixed:

> "… we all have a responsibility in that sense, and I know it's a generic response, but certainly it's an individual responsibility, but it's also government's responsibility to make sure there's proper procedure and guidelines are being followed…" [P13].

Future Research

While this research was useful in providing some much-needed insight into digital security expert perceptions of cybercrime legislation and awareness in Ireland, there are recommendations that can be made to improve future research in this area. Firstly, this study interviewed 17 digital security experts who interact with cybercrime legislation. Despite the small number of participants in the study, the findings communicated are valuable based on their authority to give information on their experiences with cybercrime (Flick, 2014). This sample is representative of the participants in it and so interpretations should be made with caution. However, the participants themselves recognised the niche pool of knowledge in digital security at the time and future research could delve into specific professional case studies targeting specific harmful online behaviours for example. The pool of expert knowledge has grown in recent years to 6,500 personnel in Ireland giving ample opportunity for further research (Government of Ireland, 2019).

It is interesting that the interviews which captured responses across professions reflected similar concerns of awareness, jurisdiction, technology development and legislative sprawl. Sandywell (2010) recommend cross-discipline scientific research to reliably understand the dynamics of cybercrime by comparing cybercrime related research findings from multiple areas. Considering the lack of previous cross-discipline research, this research captured a unique analysis of experiences from digital security experts from different professional backgrounds who all highlight the need for legislative collaboration in the Irish legal system. Future research might build on this finding to provide more in depth understanding of the requirements of digital security experts (with different jobs, roles and backgrounds) in their work and contributions toward further developing awareness and legislation for cybercrime in Ireland.

Conclusion

"I think we're getting there; it will just take a little while." [P7]

Within this study Irish digital security experts perceived education, reporting mechanisms, recognition of complex jurisdictional limits, legislative sprawl and the race against technology development as concerns for cybercrime legislation efficacy. Although "…hastened legislation is never good legislation; reactionary legislation is not good legislation" [P1], policy should be swift in responding to harm caused by technology use. This could be aided by collaboration and research with experts, who have knowledge of how current legislation is used to work against cybercrime. Legislation needs to look toward how technology may be [mis]used rather than waiting for a significant incident to occur to regulate technology use as a remedy. Although, perhaps the situation is not all bad: "It is a natural human thing to focus on the bad and negative things, but there is also creativity and connectivity and it's not all doom and gloom" [P12]. In acknowledging that legislative change requires is a lengthily process and it is not likely to happen soon, legislation should engage with events and technology creation as it happens since "…right now, legislation is not as involved as I think it could be" [P9]. For example, cybersecurity today faces difficulties and controversies that go beyond technology capabilities including the right to privacy, considering surveillance for public safety (Gallova, Palasinski, Shortland, Humann & Bowman-Grieve, 2018).

Although no successful approach to cybercrime has been found yet: "I think we're all very naive, the world as we know it has changed in the last 10 years and is going to change radically again probably over the next 10-15 years as all of the technology embeds" [P8]. Looking at digital security experts and their knowledge in this field will be increasingly important as they are often on the frontlines in terms of seeing and potentially forecasting such developments.

References

Androulidakis, I. & Kandus, G. (2011). What University Students Do (or Don't) Know about Security in their Mobile Phones. *Telfor Journal*, 3(1), 8-12.

Armencheva, I. & Smolenov, S. (2015). From Real Cyber Conflict Through Wishful Cyber Security To (Un) Likely Cyber Peace. *Military Art and Science*, 3 (79), 259-266.

Arthur Cox, (2013, January, 1). Cybercrime in Ireland – Recent legislative developments article. Retrieved from https://mondaq.com/ireland/Criminal-Law/218860/Cybercrime-In-Ireland--Recent-Legislative-Developments

Ashmore, W. C. (2009). Impact of Alleged Russian Cyber Attacks. Baltic Security & Defence Review, 11, 4-40.

Awan, I., & Zempi, I. (2016). The affinity between online and offline anti-Muslim hate crime: Dynamics and impacts. *Aggression and Violent Behavior, 27*,1 –8.

Awan, I., & Zempi I. (2017). 'I will blow your face off'—virtual and physical world anti-Muslim hate crime. *The British Journal of Criminology, 57*(2), 362–380.

Bedrijfsrevisoren, D., Muynck, J. D. & Portesi, S. (2015, December). *Cybersecurity and information sharing: An Overview of Regulatory and Non-regulatory Approaches.* Retrieved from https://www.enisa.europa.eu/publications/cybersecurity-information-sharing/at_download/fullReport

Braun, V. and Clarke, V. (2006) Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77-101.

Brenner, S. W. (2007). "At Light Speed": Attribution And Response To Cybercrime/Terrorismavarfare. *The Journal of Criminal Law & Criminology,* 97(2), 379-475.

Bryant, W. D. (2015). Resiliency in Future Cyber Combat. *Strategic Studies Quarterly*, 9(4), 87-107.

Case, C. J. & King, D. L. (2014). System Security: A Trend Analysis of Student Electronic Resources Use Policy. *Perceptions and Risky Behavior. Asbbs Ejournal, 10*(1).

Castleberry, A. & Nolen, A. (2018). Thematic analysis of qualitative research data: Is it as easy as it sounds? *Currents in Pharmacy Teaching and Learning 10*, 807–815.

Central Statistics Office (2020). *Recorded Crime Q1 2020.* Retrieved from https://www.cso.ie/en/releasesandpublications/ep/p-rc/recordedcrimeq12020/

Changa, V., Ramachandrana, M., Yaob, M., Kuoc, Y. & Lid, C. (2016). A resiliency framework for an enterprise cloud. *International Journal of Information Management 36*(1), 155–166.

Clough, J. (2011). Data theft? Cybercrime and the increasing criminalization of access to data criminal. *Law Forum, 22*, 145–170.

Collingwood, L. & Broadbent, G. (2015). Offending and being offended online: Vile messages, jokes and the law. *Computer Law & Security Review,* 31(6), 763-772.

Colombo, R. J. (2009). Trust and the Reform of Securities Regulation. *Villanova Law Review, 09-22.*

Dashora, K. & Patel, P. P. (2011). Cyber crime in the society: Problems and preventions. *Journal of Alternative Perspectives in the Social Sciences, 3(1), 240-259.*

Department of Communications, Energy and Natural Resources (July, 2013). Doing more with National Digital Strategy for Ireland Phase 1 – Digital Engagement. Ireland.

Federal Bureau of Investigation (2015, April, 3). *Cyber Action Team*. Retrieved from https://www.fbi.gov/news/stories/the-cyber-action-team

Fafinski, S. (2009). The UK Legislative Position on Cybercrime: A 20-Year Retrospective. Journal of Internet Law, 13(4), 3-13.

Fahey, E. (2014). The EU's Cybercrime and Cybersecurity Rule-Making: Mapping the Internal and External Dimensions of EU Security. *European Journal of Risk Regulation, 1*, 46-60.

Felstiner, A. (2011). Grappling with Online Work: Lessons from Cyberlaw. S*aint Louis University Law Journal*, 56(1), 209-229.

Flick, U. (2014). An introduction to qualitative research. Los Angeles: Sage.

Gallova, V., Palasinski, M., Shortland, N., Humann, M., & Bowman Grieve, L. (2018). Anxiety about digital security and terrorism, and support for counter-terror measures. *Safer Communities*, *17*(3), 156-166.

Goucher, W. (2010). Being a cybercrime victim. *Computer Fraud & Security, October 2010*(10), 26-18.

Government of Ireland (2019). *National Cyber Security Strategy 2019-2024*. Retrieved from https://www.dccae.gov.ie/documents/National_Cyber_Security_Strategy.pdf#page=4&zoom=100,93,96.

Grant Thornton (2015). *How to be cyber-secure?* Retrieved from https://www.grantthornton.global/globalassets/1.-memberfirms/global/insights/article-pdfs/2015/advisory/cybersecurity- viewpoint-final-online.pdf.

Hancock J. T., Curry, L. E., Goorha, S., & Woodworth, M. (2008). On lying and being lied to: A linguistic analysis of deception in computer-mediated communication. *Discourse Processes, 45*(1), 1-23.

Hancock, J. T. & Guillory, J., (2015). Deception with technology. In Sundar SS ed. *The Handbook of the Psychology of Communication Technology* (pp. 270-289). Chichester, West Sussex, UK Malden, MA: John Wiley & Sons, Inc.

Ho, L., Lin, Y., Lu, M. & Huang, C. (2011). Influences of Social Control on Juvenile Cybercrime Behaviors in Taiwan. *Procedia Engineering, 29*, 2545 – 2550.

Holt, T. & Bossler, A. (2012). Police perceptions of computer crimes in two southeastern cities: An examination from the viewpoint of patrol officers. *Journal of Criminal Justice, 37*, 396-412.

Holt, T. J. & Turner, M. G. (2012). Examining Risks and Protective Factors of On-Line Identity Theft. *Deviant Behavior, 33*, 308 –323.

Holt, T., Bossler, A. & Spellar, K. (2015). *Cybercrime and Digital Forensics: An Introduction*. Abingdon, Oxon UK New York, NY: Routledge.

Holt, T., Burruss, G. & Bossler, A. (2015). Policing cybercrime and cyberterror. Durham, North Carolina: Carolina Academic Press.

Horsman, G. (2016). Digital forensics: Understanding the development of criminal law in England and Wales on images depicting child sexual abuse. *Computer Law & Security Review*, 32(3), 419-432.

Hoscheidt, M. M., & Felber Eichner E. (2014). Legal and Political Measures to Address Cybercrime. *World Summit on the Information Society Forum,* 445-477.

Hunton, P. (2011). The stages of cybercrime investigations: Bridging the gap between technology examination and law enforcement investigation. *Computer Law and Security Review*, *27*(1), 61-67.

Hutchings, A. (2014). Crime from the keyboard: organised cybercrime, co-offending, initiation and knowledge transmission. *Crime Law Soc Change, 62*, 1–20.

Hyman, P. (2013). Cybercrime: It's Serious, But Exactly How Serious? *Communications of the ACM,* 56(3), 18-20.

Ion, I., Langheinrich, M., Kumaraguru, P. & Capkun, S. (2010, July, 14-16). Influence of User Perception, Security Needs, and Social Factors on Device Pairing Method

Choices. *SOUPS: Proceedings of the Sixth Symposium on Usable Privacy and Security, Redmond, WA, USA.*

Ionescu, L. (2012). Corruption, Unemployment, and the Global Financial Crisis. *Economics, Management, and Financial Markets, 7*(3), 127–132.

Ionescu, L., Mirea, V. & Blajan, A. (2011). Fraud, Corruption and Cyber Crime in a Global Digital Network. *Economics, Management, and Financial Markets, 6*(2), 373–380.

ITU (2012, September). *Understanding Cybercrime: Phenomena, Challenges and Legal Response*. Retrieved From http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf.

Kaiser, J. & Brown, S. (2015). When the story is too good to be true: a lawyer's role in resisting the lure of narrative. *Western New England Law Review, 37*, 233-265.

Karabacak, B. Yildirim, S. O. & Sevgi Baykal, N. (2016). Regulatory approaches for cyber security of critical infrastructures: The case of Turkey. *Computer Law & Security Review, 32(3), 526-539.*

Keane, A. J. (2007). Computer Forensics and Irish Law. *The ITB Journal, 8*(2), 17-21.

Kesan, J. P., Hayes, C. M., & Bashir, M. N. (2016). A comprehensive empirical study of data privacy, trust and consumer anonymity. *Indiana Law Journal*, 91(2), 267-352.

Khadam, N. (2012). Insight to Cybercrime. *Hanyang Law Review*, 29(1), 55-80.

Kshetri, N. (2013a). Cybercrime and cyber-security issues associated with China: Some economic and institutional considerations. *Electron Commer Res*, 13, 41–69.

Kshetri, N. (2013b). Cyber-victimization and Cybersecurity in China. *Communications of the ACM, 56(4),* 35-37.

Lastowka, F. (2010). *Virtual justice: the new laws of online worlds*. New Haven, Conn: Yale University Press.

Law Reform Commission (2014). Issues Paper on Cyber-crime affecting personal safety, privacy and reputation including cyber-bullying (LRC IP 6-2014). Dublin: Law Reform Commission.

Leong, K. B. (2014). Cyber-attacks more evasive, critical infrastructures at risk. *Network World Asia, 10*(3), 18.

Levin, A. & Ilkina, D. (2013, March). *International Comparison of Cyber Crime*. Retrieved from https://pdfs.semanticscholar.org/6fb2/7629aa7dc0dd4a1abc81a2e7729920997f53.pdf?_ga=2.75773781.1375583382.1595586015-1504963325.1595586015.

Lynch, J. (2014). The evolving role of self-report surveys of criminal victimization in a system of statistics on crime and the administration of justice. *Statistical Journal of the IAOS,* 30, 165–169.

Mantelero, A. (2016). Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection. *Computer Law & Security Review, 32*(2), 238-255.

McIntyre, T. J. (2005). Computer Crime in Ireland: A Critical Assessment of the Substantive Law. Irish Criminal Law Journal, 15(1), 13-22.

McIntyre, T. J. (2015). Cybercrime: Towards a research agenda. In D. Healy, C. Hamilton, Y. Daily & M. Butler (Eds.), Routledge Handbook of Irish Criminology. London: Routledge.

Millman, C., Winder, B. & Griffiths, M. (2017). UK-Based Police Officers' Perceptions of, and Role in Investigating, Cyber-Harassment as a Crime. *International Journal of Technoethics, 8(1), 89-103).*

Mishna, F., Cook, C., Saini, M., Wu, M. & MacFadden, R. (2010). Interventions to Prevent and Reduce Cyber Abuse of Youth. *Research on Social Work Practice*, 1-10.

Murray, K. & Kelleher, D. (2016). *Cybercrime*. Retrieved from http://ictlaw.com/computer-crime/cyber-crime/

O'Connor, O. & Gladyshev, P. (2006). *ISSA / UCD Irish Cybercrime Survey 2006.* Retrieved from https://www.ucd.ie/cci/news_and_events/publications/issa_ucd_irish_cybercrime_survey_2006.pdf.

O'Moore, M. (2013, November). *The Four Pillars Of Action: The Role of Guidance Counsellors in developing and implementing the Whole School Community Approach in Tackling Bullying, both Traditional and Cyber*. National Centre for Guidance in Education (NCGE). Retrieved from https://www.ncge.ie/school-guidance-handbook/four-pillars-action-role-guidance-counsellors- developing-and-implementing

Öberg, J. (2013). Is It "Essential" To Imprison Insider Dealers To Enforce Insider Dealing Laws? *Journal of Corporate Law Studies, 14(1), 111-138.*

Ögütçü G., Testik, O. M. & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security, 56,* 83–89.

Padmanabhan, S. (2012). Hacking for Lulz: Employing Expert Hackers to Combat Cyber Terrorism. *VANDERBILT Journal of Entertainment and Technology Law,* 15(1), 191.

Palasinski, M. & Svoboda. S. (2014). Reducing the Risk of Insurance Fraud by Appearances of Online Surveillance. *Psychology, Crime & Law. 20*(9), 821-832.

Ponemon (June, 2017). 2017 Cost of Data Breach Study: United States. Ponemon Institute Research Report.

Regoli, R. M., Hewitt, J. D. & Maras, M. (2013). Exploring Criminal Justice: The Essentials (2nd ed.). Burlington, Mass: Jones & Bartlett Learning.

Ruttenberg, J., von Mehren, P. & Yen, J. (2013). *Intellectual Property and cyberlaw.* Harvard, Cambridge. Retrieved from https://hls.harvard.edu/content/uploads/2008/06/IP-Cyberlaw-Guide-Final-2.pdf.

Ryan, P. & Harbison, A. (2010). The Law on Computer Fraud in Ireland - Development of the Law on Dishonesty. *Society for Computers and Law.* Retrieved from http://www.techlaw.org/wp-content/uploads/2010/07/Arthur-Cox-The-Law-on-Computer-Fraud-in-Ireland-June-2010.pdf.

Ryan, P., Browne, T. & McDermott, S. (2016). Cybercrime Legislative Developments in Ireland Group Briefing, Cybersecurity. *Arthur Cox*. Retrieved from https://www.mondaq.com/ireland/privacy-protection/474020/cybercrime-legislative-developments-in-ireland

Saridakis, G., Benson, B., Ezingeard, J., & Tennakoon, H. (2016). Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users. *Technological Forecasting & Social Change*, *102*, 320–330.

Smith, R. (2008). Book Review of Cybercrime and Society. *International Journal of Cyber Criminology, 2*(2), 397-399.

Sandywell, B. (2010). On the globalisation of crime: The Internet and new criminality. In Y. Jewkes & M. Yar (Eds.), Handbook of Internet crime (302-319). Cullompton: Willan Pub.

Tonry, M. (2011). *The Oxford handbook of crime and criminal justice*. Oxford New York: Oxford University Press.

Uma, M. & Padmavathi, G. (2013). A Survey on Various Cyber Attacks and their Classification. *International Journal of Network Security, 15(*5), 390-396.

Van Royen, K., Poels, K., Vandebosch, H., & Adam, P. (2017). "thinking before posting?" reducing cyber harassment on social networking sites through a reflective message. *Computers in Human Behavior, 66,* 345–352.

Vlachos, V., Minou, M., Assimakopouos, V. & Toska, A. (2011). The landscape of cybercrime in Greece. *Information Management & Computer Security, 19*(2), 113-123.

Wada, F., Longe, O. & Danquah, P. (2012). Action Speaks Louder Than Words - Understanding Cyber Criminal Behavior Using Criminological Theories. *Journal of Internet Banking And Commerce, 17(1), 2-12.*

Whelan, C. and Harkin, D. (2019). 'Civilianising specialist units: Reflections on the policing of cybercrime'. Criminology & Criminal Justice.

Yar, M. (2006), *Cybercrime and Society: Crime and Punishment in the Information Age*. London, Thousand Oaks, CA: Sage Publications.

Yeomans, H. (2014). Teaching and Learning in Crime and Criminal Justice History Overview. *Law, Crime and History, 4*(1), 1-14.