Improving cybercrime reporting in Scotland: A systematic literature review

Juraj Sikra

PUBLISHED IN GLASGOW - UNITED KINGDOM

UNIVERSITY OF STRATHCLYDE

**'Improving cybercrime reporting in Scotland:
A systematic literature review'**

Graphics and front cover created with Microsoft PowerPoint

For any other questions please contact the author

PhDr. Juraj Sikra, M.A. (Hons), MSc., CIPD Assoc.

at

juraj.sikra@strath.ac.uk

PURE ID: 133 741 787
DOI: https://doi.org/10.17868/79836

This research has been funded by the University of Strathclyde Computer & Information Sciences and the Scottish Institute for Policing Research (SIPR).

ABSTRACT

I have explored how to improve cybercrime reporting in Scotland by conducting a systematic literature review. Due to the lack of data on Scotland, I have frequently extrapolated from both the UK and the West. The research questions were: 1. What is known about cybercrime in the UK to date? 2. What is known about cybercrime victims in the UK to date? 3. What is known about cybercrime reporting to date? The answers were retrieved by combining Boolean variables with keywords into Scopus, Web of Science and ProQuest. This resulted in the analysis of 100 peer-reviewed articles. This analysis revealed a common trend, a novel taxonomy, and an original conclusion. The common trend is that of responsibilisation, which is the shifting of responsibility for policing cybercrime from the government onto the citizens and private sector, which will inevitably responsibilise consumers. The novel taxonomy is for classifying cybercrime reporting systems according to three pillars, which I referred to as Human-To-Human (H2H), Human-To-Machine (H2M) and Machine-To-Machine (M2M). The original conclusion is that to improve cybercrime reporting in Scotland, the process needs to be treated also as a social one rather than a purely mathematical one.

ACKNOWLEDGEMENTS

I would like to thank my primary supervisor Dr D. R. Thomas for his consistent availability and support both practical and emotional, which by far exceeds the formal requirements. I would also like to thank Dr K. Renaud for introducing me to the systematic method, which made my reviewing much more enjoyable and developmentally meaningful. Finally, I thank Dr B. Collier for helping me understand the unique and exciting context of contemporary Scottish policing as well as the University of Strathclyde and SIPR (Scottish Institute for Policing Research) for their support and funding.

CONTENTS

1 INTRODUCTION

Having been employed in criminal mental health, the professional distinctions between what constituted the signs of a crime and what did not became blurred. A key phrase from the many variations of safety training was: "You don't have to be right when you report a concern, that will be for someone else to decide, you just have to report it."

After an emotional situation, this sometimes proved a challenging task: "Did I really see what I think I did?", "Am I being manipulated or am I just tired?" A big burden was always lifted from my shoulders when I reminded myself of that key phrase. I didn't have to be right, being honest was going to be enough.

Sometimes that meant being honest about feeling very confused after an experience. By acknowledging my confusion I was able to establish a baseline from which authentic clarification could occur. It is my conviction that without this approach, clarity on sensitive issues would have been difficult to establish. In an environment where there is crime and denial of confusion, more crime will soon follow.

By way of analogy, my experiences have paved way into the current research on economic cybercrime, which affects vulnerable populations in Scotland. The aim of this systematic literature review is to synthesise research on cybercrime in the UK and beyond with the aim of working towards "Improving cybercrime reporting in Scotland."

I have synthesised research on crime from the UK and beyond in order to make extrapolations to Scotland. Problems with insufficient cybercrime reporting are worldwide and yet there is a relative lack of data on this subject overall and in Scotland in particular. This research can be a source of positive change for improving cybercrime reporting in Scotland where this major problem has thus far received only limited research attention.

I look back at what my experiences in criminal mental health have taught me and remind myself that succeeding is not about *responsibilising* citizens with the same tools as the police to investigate what has happened to them. It is about empowering them to report any suspicious cyber activity without having the fear of being judged if they get it wrong.

I will predominantly focus on economic cybercrime that contains dishonesty such frauds and scams in their varied forms. I will also touch on other crimes that are carried out for an economic incentive such as selling illegal booter services.

The research questions I seek to answer are exploratory in nature:

RQ1: What is known about cybercrime research in the UK to date?

RQ2: What is known about cybercrime victims in the UK to date?

RQ3: What is known about cybercrime reporting to date?

> I will use the 7 Discussion to tie the answers to these questions with the information from the 2 Background with the aim of "Improving cybercrime reporting in Scotland."

I commence this paper by focusing on cybercrime in the United Kingdom (UK), which I will break down into three main sections: 4 What is known about cybercrime research in the UK to date? and 5 What is known about cybercrime victims in the UK to date?, which are based predominantly on studies from the UK. In the subsection 5.2 Victim experiences I will include other research from the Western world as there is a lack of equivalent data from the UK. The section 6 What is known about cybercrime reporting to date? will focus on worldwide research due to a lack of relevant studies from the UK.

2 BACKGROUND

Section 2.1 Police Scotland, describes the modern changes in Scottish policing within the context of UK policing and how both connect to improving cybercrime reporting in Scotland. Then, Section 2.2 Crime numeration, covers how the counting of crime evolved over time and what this implies for improving cybercrime reporting in Scotland.

2.1 Police Scotland

When discussing the democratisation of the UK police, Jones, Newburn, and Smith 1996 put forward the arguments that the latter cannot be effective without adequate supervision of the processes. This pro-active supervisory approach should always be prioritised over a reactive after the fact strategy, which should only come as a second option. They also viewed the effective collaboration between the police and localities as a key condition of democratic policing.

Taking into account the Scottish context in particular, in a research paper on the subject of rural policing, Wooff 2015 described the interactions between the police and their local community on cases of anti-social behaviour. With the use of vignettes, Wooff 2015 showed how police differently use discretion to respond to escalating violence. In the first vignette, the police officer used compassionate mentoring towards a group of youths that were engaged in verbal aggression, which deescalated the situation. In the second vignette, the police officer arrested the individual who was behaving antisocially due to the continued repetition of the problem behaviour. I argue that in both cases the police officers tried to behave in ways that increased cohesion in the community be it with the use of compassion or offender exclusion respectively. Police officers who are able to embody these qualities will be particularly well placed to build trust with their citizens to increase cybercrime reporting because people will feel confident to approach them after a crime.

In a follow-up research, Wooff 2016 has contextualised rural policing within the evolution of Scottish policing, which has undergone a major reform in 2013. During 2013, 8 regional forces were centralised under one Police Scotland. This has created new challenges for rural policing which Wooff 2016 analysed using the prism of "soft" vs. "hard" policing. Soft policing is based on the idea of police collaborating with the community to resolve shared issues. Hard policing is akin to the police enforcing the law and combating crime. Whilst Wooff 2016 warns against collapsing "rural policing" and "soft policing", the author sees the terms as complimentary. In his view, soft policing exploits localised expertise, which is required for rural policing. This is an important piece of research because it goes some length to show that centralised hard policing practices carry the risk of losing precious insight into the social dynamics of communities. Importantly, these insights will contain information about who is most vulnerable to cybercrime. This is why I argue that soft approaches to policing are better placed at improving cybercrime reporting in Scotland than hard approaches.

In remaining with the subject of the 2013's centralisation reforms in Police Scotland, Henry, Malik, and Aydin-Aitchison 2019 argued that the centralisation is best conceptualised as a process rather than event. The authors state that local policing is historically tied to the municipal structure of services and therefore honours a democratic system, which need not be completely abolished moving forward. This is because according Henry, Malik, and Aydin-Aitchison 2019 policing should remain at its heart democratic even if effective centralist reforms are put into place.

In order to preserve a balanced debate about the unification of modern policing in Scotland, I include a captivating viewpoint on this subject by Murray and Harkin 2017. Unlike, Wooff

2016, Murray and Harkin 2017 view the centralisation of Police Scotland under the nationalist government as a constructive manoeuvre. They argue that policing prior to this reform was devoid of effective scrutiny, which created problems for maintaining high standards of practice. I agree with the claim that localisation is not without its challenges, namely the discretion component frequently referenced by Wooff 2015 and Wooff 2016 is a double-edged sword when embraced uncritically. In other words, discretion is by definition about having power over an environment rather than about exercising that power ethically, which is an important distinction. Hence, police officers with privileged knowledge into their local communities are also in a far better position to abuse that knowledge than someone following centralised procedures of agreed best practice.

In parallel with the subject of centralisation of Police Scotland is the recent shifting away from the UK's centralised cybercrime reporting mechanism – Action Fraud. The latter is described as the fraud reporting system put into place by the Home Office and manned by City of London Police (Kenny MacDonald 2019). In response to a Freedom of Information request to Dyson, I. 2019, Kenny MacDonald 2019 supplied the evidence-based analysis which resulted in Scotland severing its relationship with Action Fraud. This is connected to centralisation. Firstly, Action Fraud was the central reporting system for England, Wales, Northern Ireland and Scotland until Scotland discontinued its membership. Secondly, by discontinuing its membership with Action Fraud, Scotland effectively centralised its cybercrime reporting systems under its devolved government.

In terms of the factors in favour and against remaining with Action Fraud, Police Scotland considered several of issues. Firstly, if the force were to remain with Action Fraud, Police Scotland would have to contribute £459 324 per year to the upkeep of the service. The advantages of this would include benefiting from a UK wide anti-fraud service and avoiding cases where the national police would conduct its own investigations. The disadvantages of this would include paying too much for a service that has been assessed as poor. Secondly, if the force were to refuse paying Action Fraud, then it would have to pave a new strategic direction for Police Scotland, which would include redirecting fraud complaints using the 101 non-emergency police helpline. The advantages of this would be victims receiving a tailored service including a vulnerability assessment and there would be no attached fees to Action Fraud. The disadvantages of this would include the risk of duplicate investigations in a situation where the central oversight of Action Fraud was removed. After weighing up the pros and cons, Police Scotland decided to move away from Action Fraud and follow their own approach (Kenny MacDonald 2019).

The question for practice is as follows: "What approach will work best to deliver on Police Scotland's ambition to prioritise the most vulnerable victims of cybercrime (Police Scotland and Scottish Police Authority 2020)?" The Cyber Strategy 2020 emphasises the need to pay closer attention to those who suffer with a disability or other form of adversity which puts them at greater risk of victimisation.

The prioritisation of vulnerability is not entirely new and is referenced in other literature where it is used to prioritise among high volume offences (Skidmore, Goldstraw-White, and Gill 2020). In fact, Skidmore, Goldstraw-White, and Gill 2020 found that 74% of police forces use the vulnerability of the victim to determine whether to proceed with an investigation. On the flip side, police officers were less likely to empathise with people who had played an active role in their victimisation. Increasingly, according to Skidmore, Goldstraw-White, and Gill 2020 police forces have began to see more value in showing support to the victims rather than proceeding with investigations, which was largely influenced by the difficulties to trace the cybercrime culprit.

The implementation of recommendations from the Cyber Strategy 2020 (Police Scotland

and Scottish Police Authority 2020) is also not without its problems. Researchers have taken issue with how "vulnerability" is defined and what it means for those that are suffering with a condition which puts them at the intersection of the mental health and criminal justice system. Namely, Enang et al. 2019 observed that vulnerability is context specific from the law enforcement perspective, which means that anyone can become vulnerable based on the situation that they find themselves in. In contrast, from a public health perspective vulnerability is viewed as a personal quality. The resulting effect of this conundrum is a fragmentation of the definition of "vulnerability" which makes its prioritisation in cybercrime complicated.

Based on the Cyber Strategy 2020 (Police Scotland and Scottish Police Authority 2020), cybercrime remains chronically under-reported. In the case of scam phone calls and viruses between 84% and 79% victims respectively did not report their experiences. In addition, the online theft of bank related details was the type of crime reported by 74% of victims, with approximately 95% from that group reporting to the banks and only 5-8% to the police (Police Scotland and Scottish Police Authority 2020).

The reasons for these discrepancies are debated in the literature in connection to "responsibilisation", which is the shifting of responsibility for cybersecurity from the state onto the citizen. In topical research by Horgan and Ben Collier 2016 the authors argued that security responsibilisation has been taking place since the 1980s. During this period the UK governments supported the privatisation of various policing services. This resulted in competition among private companies to sell more secure locks, CCTV and recently cybersecurity solutions. Moreover, other reasons for the lack of cybercrime reporting in Scotland can be that most government interventions are aimed at awareness raising, which contains victim blaming connotations. These only further alienate people.

The challenges with responsibilisation were further broken down in a research by Renaud, Flowerday, et al. 2018. The latter authors argued that the neoliberalist agenda resulted in governments adopting an approach whereby they advise citizens on cybersecurity issues, but let them face the consequences if they choose not to follow that advice. In the case of cybersecurity, Renaud, Flowerday, et al. 2018 take two main issues with this approach. Firstly, they argue that responsibilisation of cybersecurity is unreasonable because only a percentage of people have the expertise to behave safely online. Secondly, they argue that responsibilisation of cybersecurity is not judicious because the mistake of one person can result in the contamination of countless computers. Hence, one person's mistake can become many people's problem. This is why the state should adopt a more hands on approach to managing cybersecurity risks.

Furthermore, Renaud, Orgeron, et al. 2020 examined responsibilisation in countries from the "Five Eyes" coalition, which entail the United Kingdom, USA, Australia, New Zealand and Canada. They found that these countries impart cybersecurity advice to its individual citizens, but become disengaged thereafter. Critically, Renaud, Orgeron, et al. 2020 found that the "Five Eyes" invest substantial amounts of finances into the protection of businesses and research into cybersecurity, which exemplifies the disparity in their approach to citizens vs. corporations.

Given the findings on responsibilisation, it should not come as a surprise that people struggled to connect their experiences of cybercrime with the Scottish police agenda (Horgan 2021) making them reluctant to report it. This too points to the enduring effects of the discussed problem.

Before I close off this section, I will mention a successful example from the Hampshire Constabulary, which provides a promising avenue for improving cybercrime reporting in Scotland. In the research by Karagiannopoulos, V., Sugiura, L., and Kirby, A. 2019 the researchers examined the Cyber Awareness Clinic, which was a two year university project funded by the Hampshire Constabulary. The aim of the clinic was threefold. Firstly, it was to impart cyber

awareness to vulnerable groups such as young people, the elderly and small and medium sized companies. Secondly, the clinic improved the knowledge of risks that the latter communities faced from cybercrime. Thirdly, the clinic aimed to transfer its approach to clinics in other parts of the country. The pioneering clinic generated positive reviews at the formal assessment and was seen as effective in reducing cybercrime in the community. Hence, to awareness raising clinics akin to the one just described could potentially increase people's reporting behaviour in Scotland.

2.2 Crime numeration

Moving now onto the second purpose of this section, I will discuss selected pieces from the literature on how crime numeration has evolved over time and how it ties into the current research.

In a classical study by Maltz 1977 the author analysed the evolution of crime counting in the USA from the 1930s onward and discovered several trends that defined this domain. Firstly, criminal data has shifted away from the system closer to the crime. This means that initially the source of crime data was court proceedings, gradually the main source of data became police reports, which had given way to victim reports. This change has become enduring as my project is still focused on the connection between the crime and the victim decades after this piece was published. Secondly, in the 1930s the USA dedicated funding to creating crime recording centres, which served to analyse data. Again, in some shape or form I observe this legacy in projects such as Action Fraud, which serve the exact purpose in modern times. Thirdly, when in the 1930s these changes were being put into place they were strongly criticised for their lack of accuracy much like in the 2020s, nearly 100 years later.

It is also worth considering what underlying circumstances prompt victims to report crime. Findings from the developed countries point to the fact that the crime type was the largest predictor of reporting behaviour in victims. Whilst the same researchers hypothesised that this effect may be varied by victim characteristics in developing countries, they were surprised to find no significant effect. Instead, the crime type in developing countries had the largest effect on subsequent reporting behaviour as well (Bennett and Wiegand 1994). This is an important piece of research for the current project because it suggests that low cybercrime reporting is due to the social perceptions surrounding the crime type rather than victims. Hence, to increase cybercrime reporting in Scotland, the way cybercrime is conceived has to become much more salient.

Research by Tarling and Morris 2010 confirmed that the seriousness of the offence played the most important role in the decision to report it. Yet, the ratios have changed. Victims are less likely to report property crime and more likely to report violence than in the past. Interestingly, even though property crime has become more dominant, the reporting rate has plummeted. This lends insight into how society's values have shifted insofar as people have become much more sensitive to violent acts rather than low value scams, which can play into the under-reporting of cybercrime in Scotland.

I will conclude the section on crime numeration with a cautionary paper by Hall 2021, who researched the adherence of police to best practice guidelines and the effect of this on the victims. Whilst the authors found encouraging evidence that the police showed strict adherence to the guidelines, they noted that instances where guidelines were not followed were seen as failing the victims. The authors cautioned against taking the best practices principle too far because they speculated that it could be used to exercise undue control over the police. I think that whilst best practice principles play a role in victim care, it is important to maintain police autonomy as well. Therefore, I believe that Scottish centralised best practice guidelines for cybercrime reporting need to be complemented with police discretion.

2.3 Summary

In summary, Police Scotland has undergone significant evolution since the nationalist's unification reforms in 2013, which have resulted in the amalgamation of the eight regional forces. This has resulted in some tension between the traditional and localised forms of policing versus the reformed centralised best practice approaches. When it comes to improving cybercrime reporting in Scotland, I will seek to exploit the best of both worlds.

Since the numeration of crime is also a part of this research, I have also discussed it. Crime reports have centred around the recorded experiences of the victims since the 1930s albeit with enduring inaccuracies. People are most motivated to report those offences that are morally most salient which changes over time.

As a first step towards achieving these ambitious goals, I have completed this systematic literature review, which collected cutting edge knowledge on topics of 4 What is known about cybercrime research in the UK to date?, 5 What is known about cybercrime victims in the UK to date?, 5.2 Victim experiences and 6 What is known about cybercrime reporting to date?. These topics were researched based on the scientific principles and approaches contained within the upcoming 3 Systematic literature review section.

3 SYSTEMATIC LITERATURE REVIEW

Using the principles of systematic research as outlined by Pickerting, C. et al. 2015, I searched the databases Scopus, Web of Science and ProQuest with the use of Boolean variables and keywords identified below. The geographical scope was the UK and temporal scope was no earlier than 1 January 1999 (start of e-commerce) onward, prioritising the most recent and cutting edge work.

The purpose of this review is to collect and analyse knowledge that will be used to in preparation for studies with the overarching theme of "Improving cybercrime reporting in Scotland." Due to the relative lack of relevant literature from Scotland, this review will use research from the UK and further afield to build a picture about reporting cybercrime which is as close to the Scottish borders as possible. In the 7 Discussion, this research will be tied to policing in Scotland based on the articles from 2 Background with a focus on what gaps in knowledge need to be addressed to support the resolution of this problem in Scotland. In the 8 Conclusion, I will provide the reader with a compendium of the themes within and their utility for the reader.

3.1 Cybercrime research in the UK

This section details the combinations of keywords and Boolean variables that I employed to conduct a systematic database search for analysing the first subtopic of 4 What is known about cybercrime research in the UK to date?, 4.1 Typology with the aim of answering the research question

RQ1 What is known about cybercrime research in the UK to date?

Keywords: "Cybercrime AND UK AND types"

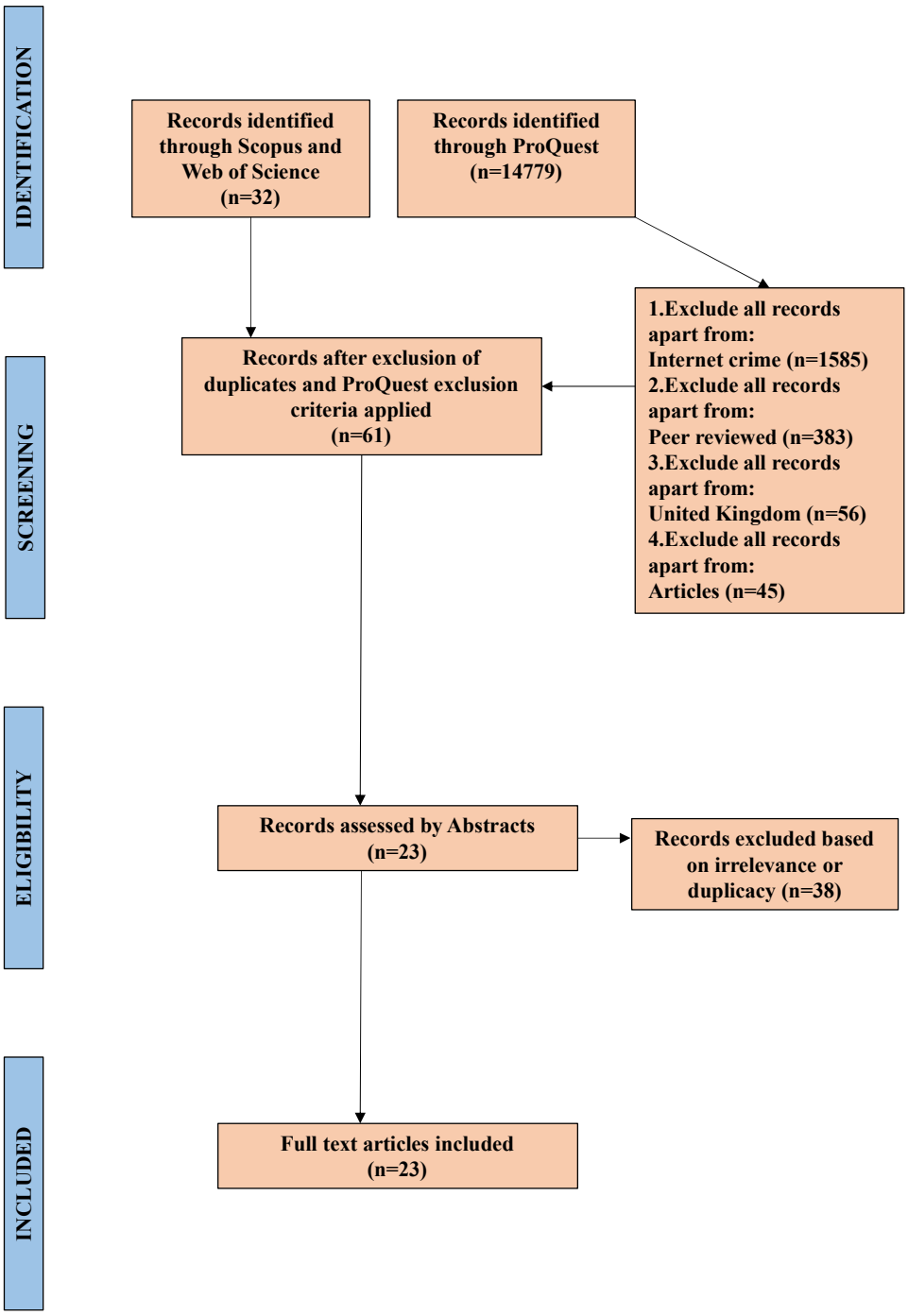
Time range: The systematic search was carried out between 09 October 2021 - 30 October 2021 based on the records retrieved from Zotero.

Scopus: Using the above keywords, I revealed 11 articles in Scopus, which were screened for relevant titles and abstracts, which resulted in 8 articles being included in the review.

Web of Science: Using the above keywords, I revealed 21 documents in Web of Science, which were screened for relevant titles and abstracts, which resulted in the inclusion of 9. Subsequently, I reduced these to 5 after 4 were identified as being replicas of articles from the previous search on Scopus.

ProQuest: Using the above keywords, I revealed 14 779 documents in ProQuest. Due to this number being very high, I applied numerous other filters on ProQuest before I could proceed with a search of titles and abstracts. The additional filters were *Subject: Internet crime*, which reduced the articles to 1 585. This excluded the following subjects: risk 3 389, risk management 2 064, earning per share 1 926, computer security 1 570, stockholders 1 501, crime 1 457, dividends 1 119, corporate profits 1 013, stock exchanges 1 013, financial statements 1 002 as well as other subjects populated by less than 1000 articles per subject. *Limit to peer reviewed*, which reduced the articles to 383. This excluded the category of "Full text." *Location: United Kingdom*, which reduced the articles to 56, *Limit to articles*, which reduced the articles to 45. This also excluded the document types: Feature 363 and others under 10 pieces per document type. Subsequently, I screened the 45 articles for titles and abstracts, which resulted in 11 articles, and as there were no replicas from the previous searches, all 11 were included.

Taken together, using the principles of a systematic literature review, I revealed 23 articles that were included in the literature review.



***PRISMA 1. keywords*: "cybercrime AND UK AND types"**

The next section details the keywords and Boolean variables that I employed to conduct a systematic search for analysing the first subtopic of 4 What is known about cybercrime research in the UK to date?, 4.2 Policing with the aim of answering the research question

RQ1 What is known about cybercrime research in the UK to date?

Keywords: "Cybercrime AND UK AND policing"

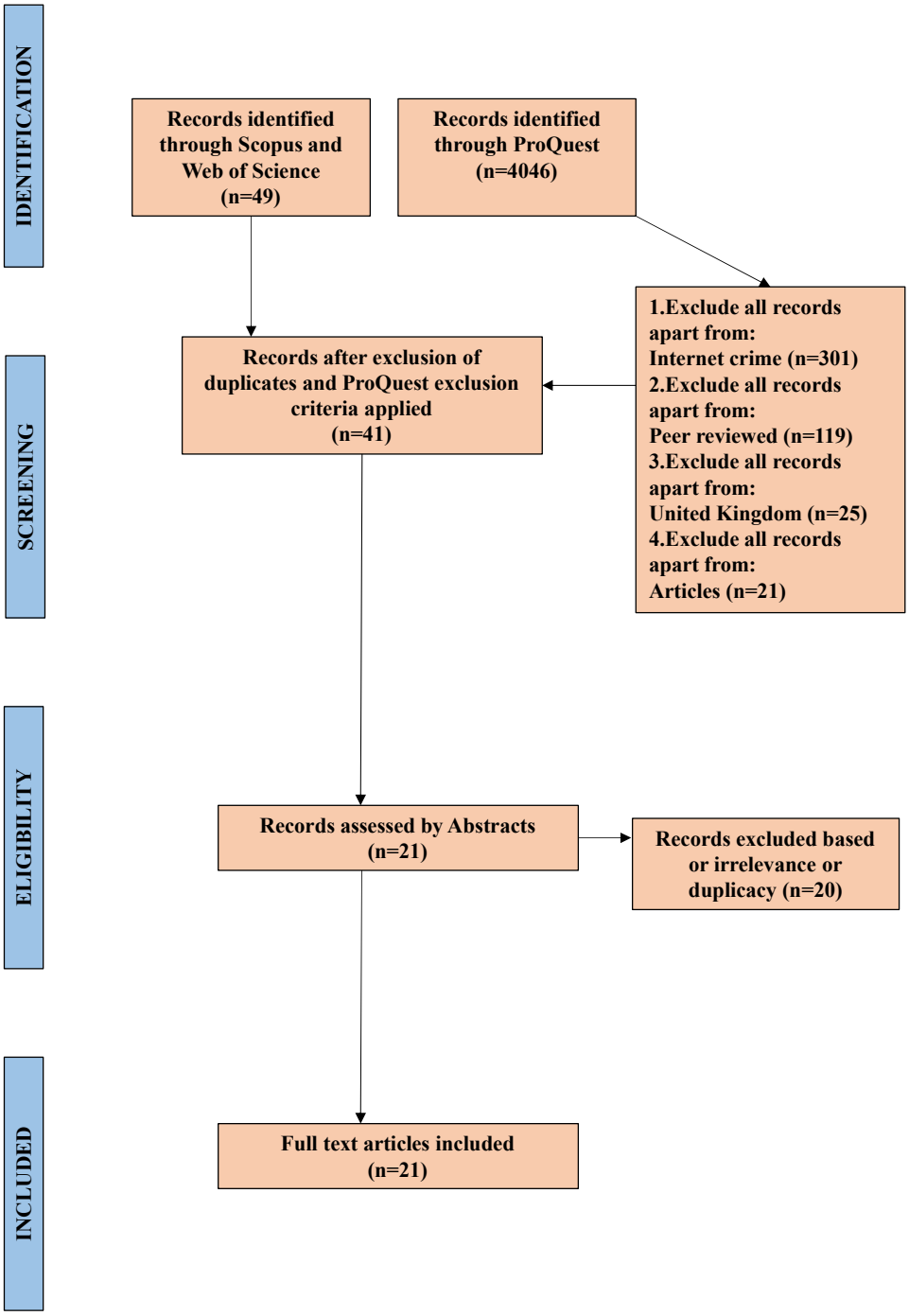
Time range: The systematic search was carried out between 09 October 2021 - 30 October 2021 based on the records retrieved from Zotero.

Scopus: Using the above keywords, I revealed 23 articles in Scopus. These were screened for relevant titles and abstracts, which resulted in 14 articles identified as suitable for the systematic review.

Web of Science: Using the above keywords, I revealed 26 articles in Web of Science. These were screened for relevant titles and abstracts, which resulted in 6 articles being added after the additional exclusion of those that surfaced from the previous search.

ProQuest: Using the above keywords, I revealed 4 046 documents in ProQuest. Due to this number being very high, I applied numerous filters on ProQuest before I could proceed with a search of titles and abstracts. The additional filters were *Subject: Internet crime*, which reduced the articles to 301. This excluded the following subjects: risk 2 095, risk management 1 101, crime 1 087 as well as other subjects populated by less than 1000. *Limit to peer-reviewed*, which reduced the articles to 119. This excluded the category of "Full text." *Location: United Kingdom*, which reduced the articles to 25 and *Limit to articles*, which resulted in 21. This excluded the document types: Feature 23 and others that contained 1 article each. Subsequently, I screened the 21 articles for titles and abstracts, which resulted in 1 article being added after the exclusion of replicas from previous searches.

Taken together, using the principles of systematic literature review, I revealed 21 articles that were included in the literature review.



***PRISMA 2. keywords*: "cybercrime AND UK AND policing"**

3.2 Cybercrime victims in the UK

The subsequent section details the combinations of keywords and Boolean variables that I employed to conduct a systematic database search for analysing the second subtopic of 5 What is known about cybercrime victims in the UK to date?, 5.1 Victim profiles with the aim of answering the research question **RQ2:** What is known about cybercrime victims in the UK to date?

Keywords: "Cybercrime AND UK AND victims"

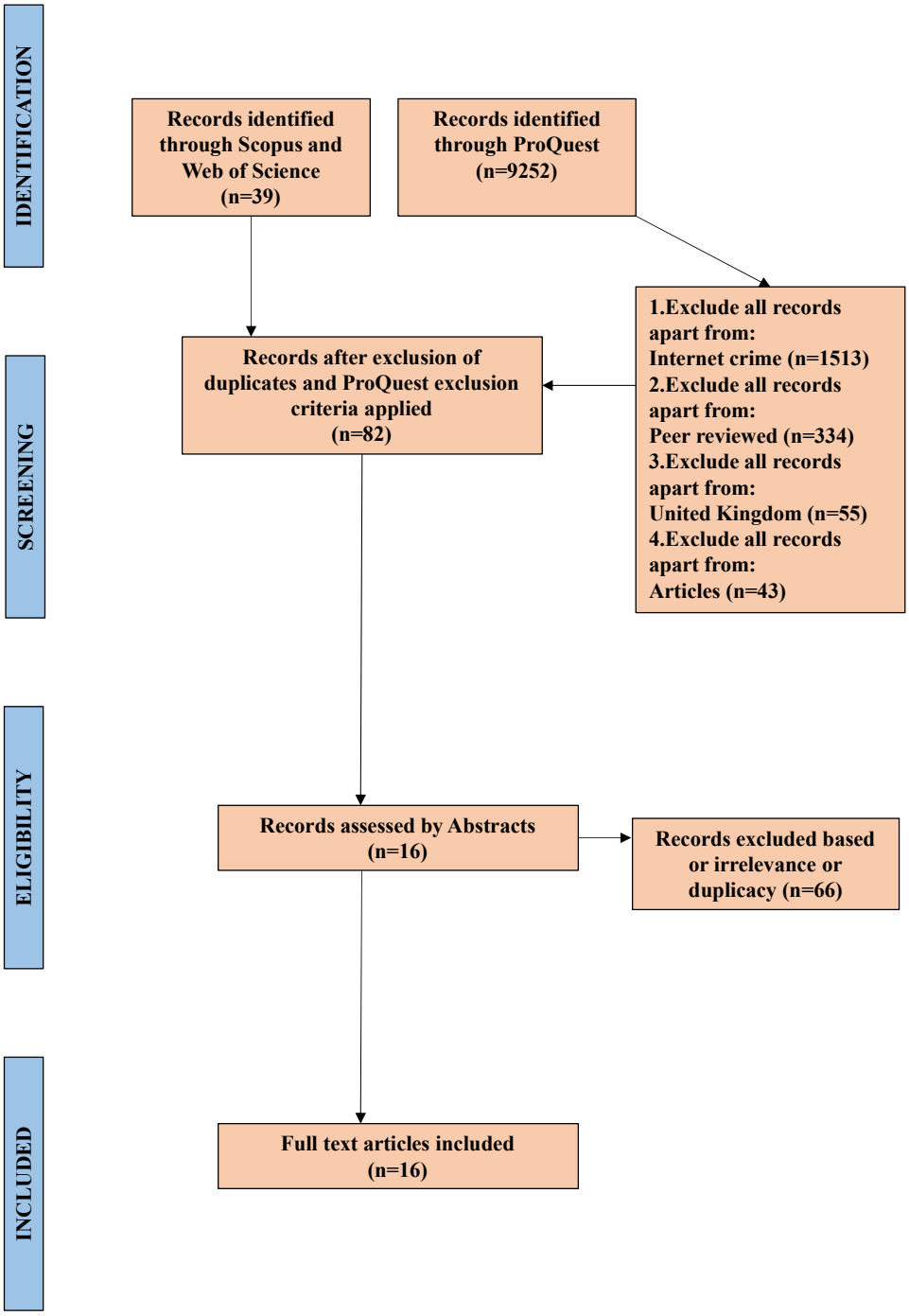
Time range: The systematic search was carried out between 09 October 2021 - 15 November 2021 based on the records retrieved from Zotero.

Scopus: Using the above keywords, I revealed 19 articles in Scopus. These were screened for relevant titles and abstracts, which resulted in 12 articles identified as suitable for the systematic review, 11 of which were added as they were available for free. From the 11 added, 4 already surfaced during the previous searches on the first subtopic, but they are still being treated as new searches in the current one.

Web of Science: Using the above keywords, I revealed 20 documents in Web of Science, which were screened for relevant titles and abstracts, which resulted in the inclusion of 1 article.

ProQuest: Using the above keywords, I revealed 9 252 documents in ProQuest. Due to this number being very high, I applied numerous filters on ProQuest before I could proceed with a search of titles and abstracts. The additional filters were *Subject: Internet crime*, which reduced the articles to 1 513. This excluded the subjects: risk 2 765, risk management 1 498, crime 1 482, computer security 1 261 and other subjects populated by less than 1000. *Limit to peer-reviewed* which reduced the articles to 334. This excluded the category "Full text." *Location: United Kingdom*, which reduced the articles to 55 and *Limit to articles*, which resulted in 43. This excluded the document types: Feature 50 and others that contained 3 to 1 articles each. Subsequently, I screened the 43 articles for titles and abstracts, which resulted in 4 articles being added after the exclusion of replicas from previous searches.

Taken together, using the principles of systematic literature review, I revealed 16 articles that were included in the literature review.



***PRISMA 3. keywords*: "cybercrime AND UK AND victims"**

The consequent section details the combinations of keywords and Boolean variables that I employed to conduct a systematic database search for analysing the second subtopic of 5 What is known about cybercrime victims in the UK to date?, 5.2 Victim experiences with the aim of answering the research question

RQ2: What is known about cybercrime victims in the UK to date?

The abbreviation of "UK" was dropped entirely from this search due to the fact that the searches were coming back with 0 results across the databases. Hence, in this section I will make an extrapolation from research on the Western population (i.e. Europe, USA and Australia) onto the UK population.

Keywords: "Cybercrime AND victim AND experiences"

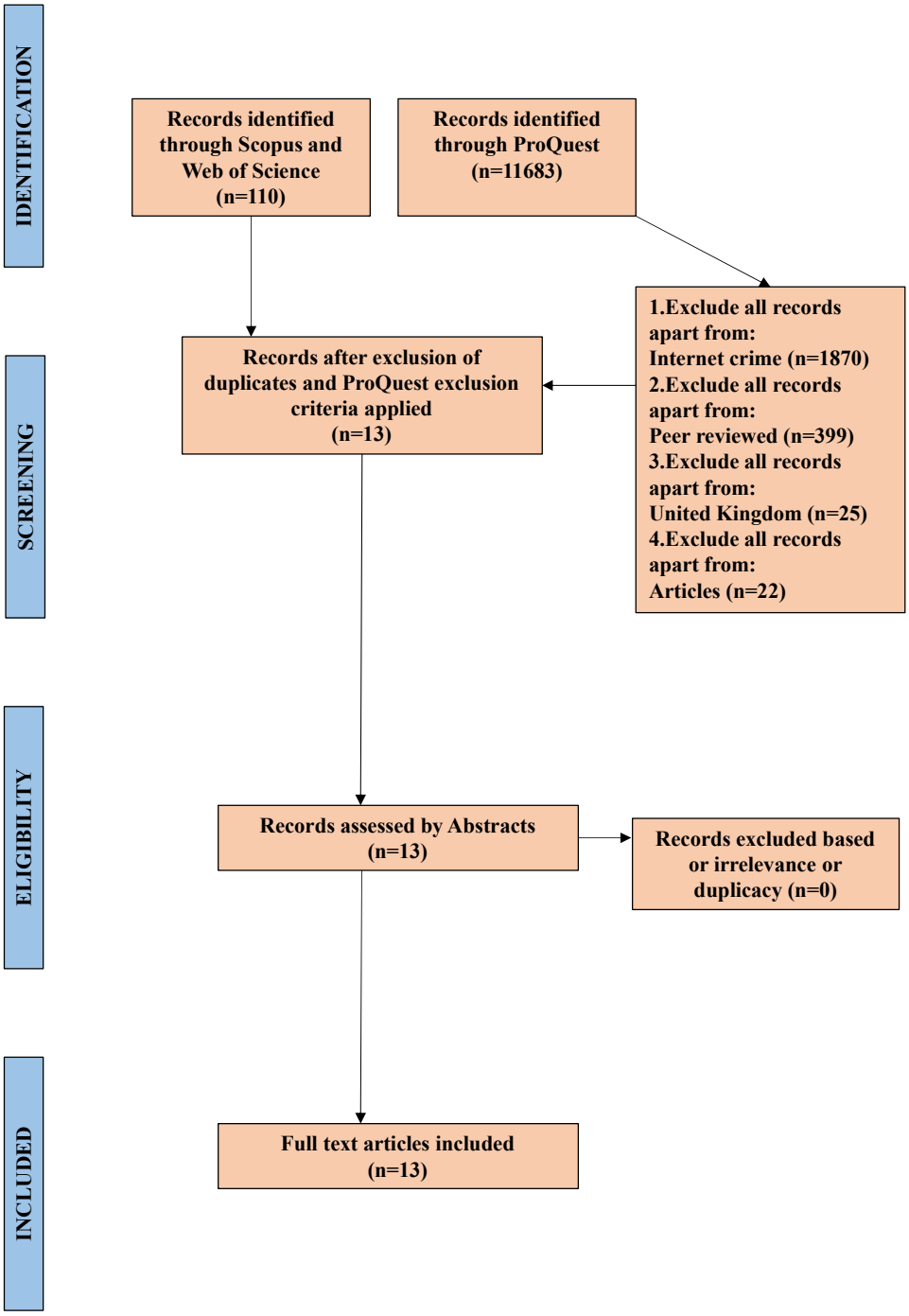
Time range: The systematic search was carried out between 09 October 2021 - 15 November 2021 based on the records retrieved from Zotero.

Scopus: Using the above keywords, I revealed 39 articles in Scopus, which were screened for relevant titles and abstracts, which resulted in 10 articles being included in the review.

Web of Science: Using the above keywords, I revealed 71 documents in Web of Science, which were screened for relevant titles and abstracts, which resulted in the inclusion of 3 articles.

ProQuest: Using the above keywords, I revealed 11 683 documents in ProQuest. Due to this number being very high, I applied numerous filters on ProQuest before I could proceed with a search of titles and abstracts. The additional filters were *Subject: Internet crime*, which reduced the articles to 1 870. This excluded the subjects: risk 2 555, computer security 1 818, crime 1 348 and other subjects populated by less than 1000. *Limit to peer-reviewed*, which reduced the articles to 399. This excluded the category "Full Text." *Location: United Kingdom*, which reduced the articles to 25 and *Limit to articles*, which resulted in 22. This excluded the document types: Feature 23 and others that contained 2 articles each. Subsequently, I screened the 22 articles for titles and abstracts, which resulted in 0 articles being added after the removal of duplicates.

Taken together, using the principles of systematic literature review, I revealed 13 articles that were included in the literature review.



***PRISMA 4. keywords*: "cybercrime AND victims AND experiences"**

3.3 Cybercrime reporting

The next section details the keywords and Boolean variables that I employed to conduct a systematic search for analysing the first subtopic of 6 What is known about cybercrime reporting to date?, 6.1 Cybercrime reporting approaches with the aim of answering the research question

RQ3: What is known about cybercrime reporting to date?

Keywords: "Cybercrime AND reporting"

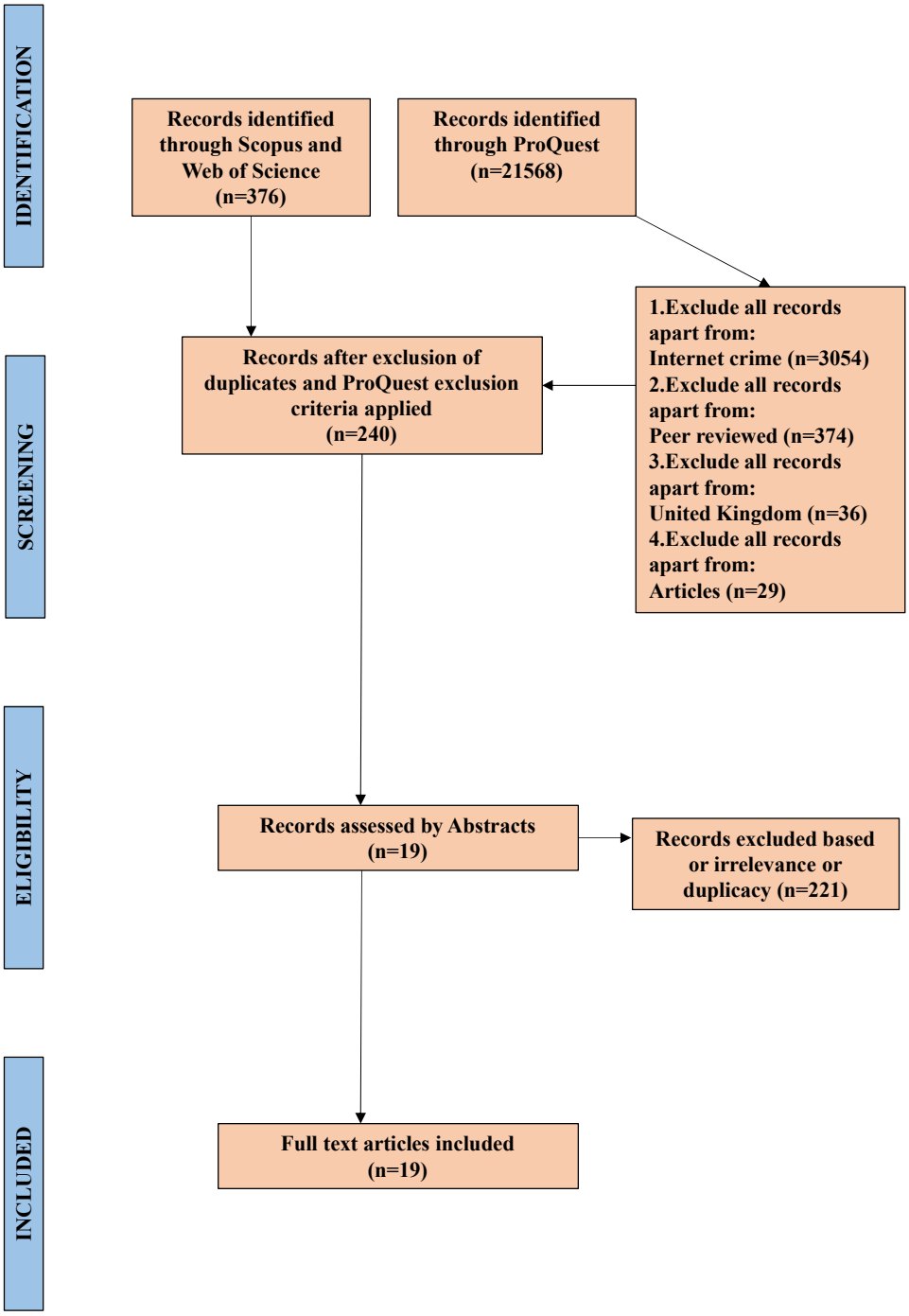
Time range: The systematic search was carried out between 29 November 2021 - 17 December 2021 based on the records retrieved from Zotero.

Scopus: Using the above keywords, I revealed 67 articles in Scopus, which I have screened the titles and abstracts which have resulted in the addition of 13 articles.

Web of Science: Using the above keywords, I revealed 309 documents in Web of Science, these were then filtered down according to the most recent years i.e., 2022 (1), 2021 (31), 2020 (59) and 2019 (48), which together amounted to 144 articles. I have then screened the 144 articles based on their titles and abstracts and included 6 articles.

ProQuest: Using the above keywords, I revealed 21 568 documents in ProQuest. Due to this number being very high, I applied numerous filters on ProQuest before I could proceed with a search of titles and abstracts. The additional filters were *Subject: Internet crime*, which reduced the articles to 3 054.This excluded subjects: risk 3 383, computer security 2 753, earnings per share 2 607, stockholders 2 425, crime 1 894, risk management 1 859, corporate profits 1 588, software 1 536, covid-19 1 392 as well as other economic and investment type subjects unrelated to cybercrime. *Limit to peer-reviewed*, which reduced the articles to 374. This excluded the category "Full Text." *Location: United Kingdom*, which reduced the articles to 36 and *Limit to articles*, which resulted in 29.This excluded the document types: Feature 33 and others that contained 3 articles each. Subsequently, I screened the 29 articles based for titles and abstracts, which resulted in 0 articles being added after the removal of duplicates.

Taken together, using the principles of systematic literature review, I revealed 19 articles that were included in the literature review.



***PRISMA 5. keywords*: "cybercrime AND reporting"**

The next section details the keywords and Boolean variables that I employed to conduct a systematic search for analysing the second subtopic of 6 What is known about cybercrime reporting to date?, 6.2 Cybercrime reporting results with the aim of answering the research question **RQ3:** What is known about cybercrime reporting to date?

Keywords: "Cybercrime AND reporting AND results"

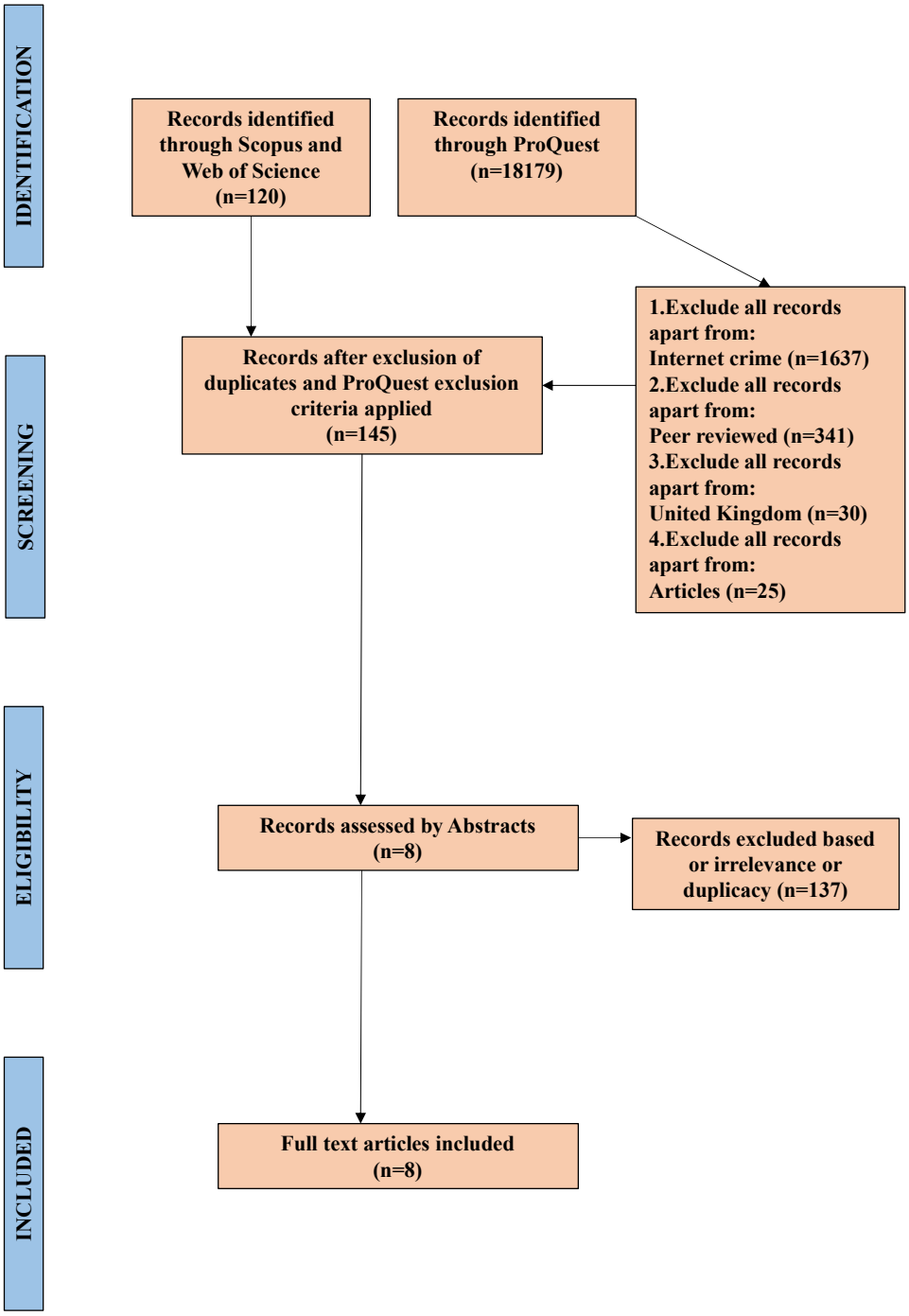
Time range: The systematic search was carried out between 29 November 2021 - 17 December 2021 based on the records retrieved from Zotero.

Scopus: Using the above keywords, I revealed 16 articles in Scopus. These I have screened for their titles and abstracts which have resulted in the addition of 4 articles.

Web of Science: Using the above keywords, I revealed 104 documents in Web of Science. I have then screened the 104 articles based on their titles and abstracts and included 4 articles.

ProQuest: Using the above keywords, I revealed 18 179 documents in ProQuest. Due to this number being very high, I applied numerous filters on ProQuest before I could proceed with a search of titles and abstracts. The additional filters were *Subject: Internet crime*, which reduced the articles to 1 637.This excluded subjects: risk 3 374, earning per share 2 593, stockholders 2 399, computer security 1 920, risk management 1 834, crime 1 704, corporate profits 1 571, financial statements 1 367 as well as other economic and investment type subjects unrelated to cybercrime. *Limit to peer-reviewed*, which reduced the articles to 341. This excluded the category "Full Text." *Location: United Kingdom*, which reduced the articles to 30 and *Limit to articles*, which resulted in 25.This excluded the document types: Feature 27 and others that contained 3 articles each. Subsequently, I screened the 25 articles based for titles and abstracts, which resulted in 0 articles being added after the removal of duplicates.

Taken together, using the principles of systematic literature review, I revealed 8 articles that were included in the literature review.



***PRISMA 6. keywords*: "cybercrime AND reporting AND results"**

4 What is known about cybercrime research in the UK to date?

The following subsection is thematically organised as follows: 4.1 Typology and 4.2 Policing.

4.1 Typology

Whilst the creativity of cybercriminals is prolific, I have used this systematic review to reveal specific categories of offences that have affected the UK: 4.1.1 Cybercrime against individuals, 4.1.2 Cybercrime against private institutions and 4.1.3 Cybercrime against public institutions.

4.1.1 Cybercrime against individuals

This type of cybercrime is most prominently represented in the literature search in connection to the UK. A summary of the crimes committed against individuals is provided in Levi, M. 2017 who states that individuals were most likely to experience bank card fraud (66% of all incidents) and online shopping fraud (28% of all incidents). In contrast, 12 months prior to this research being conducted in 2014-15, 5% of people in Scotland reported incidents of bank card fraud (Levi, M. 2017). Other research has identified that Denial of Service Attacks (DoS) also feature prominently as a cybercrime against individuals who are usually gamers (Collier, B. et al. 2019). There are at least two actors involved in this modus operandi. The illegal booter service where the customer can purchase the attack and then the actual customer who launches the attack on their victim. This type of crime can result in a simple nuisance that requires the gamer to postpone the game until the attack ceases, but it can also cause actual harm in the household (or to other bystanders) depending on what other technology is affected.

Moreover, people can be targeted by criminals using a romantic or sexual incentive. Victims can be scammed into sending money to attractive people in exchange for sexual photos and videos as a form of a transactional sexual encounter. In fact, they are communicating with a cybercriminal who has purchased a packet of fake photographs via a criminal network to commit an offence referred to as eWhoring (Hutchings, A. and Pastrana, S. 2019; Pastrana, S. et al. 2019). Whilst eWhoring is the communication with a fake profile, romantic scams can involve interactions with actual attractive offenders who exploit the emotional needs of potential victims into sending them finances (Whitty, M.T. 2018).

Previous research by Correia, S.G. 2019 and Correia, S.G. 2020 also draws attention to the varied effect of cybercrime on individuals. For example, data shows that females are significantly likelier to report Advance fee fraud, whereas as the effect is more pronounced in older people. In contrary, individuals reporting crimes of Hacking, Computer software service fraud, Malware and DoS tended to be younger. The details of cybercrime victims will be covered robustly in the upcoming section 5 What is known about cybercrime victims in the UK to date?.

Individuals have been affected by cybercrime even more due to increased loneliness and isolation brought on by the COVID-19 pandemic (Buil-Gil, D. and Zeng, Y. 2021). Crimes against the elderly during the pandemic also received attention in UK research (Cross, C. 2021). She found that the elderly were subjected to the same fraud techniques as in the pre-pandemic period, but that the pandemic was used as ruse to practice those techniques. Lastly, an unusual form of fraud that surfaced during the COVID-19 pandemic was devised to respond to people searching for their lost pets online. As a part of this scam, the offender contacts the owner of a pet that has been advertised as lost and falsely claims that they have found it and will return it for a fee (Levi, M. and Smith, R.G. 2021).

4.1.2 Cybercrime against private institutions

In the past, these included attacks on banks, which meant submitting forged cheques which were electronically scanned and cashed before being identified as fake (Fisher 2008). Increasingly, companies are targeted also via the vulnerabilities of their staff. In a fraud type referred to as Business E-mail Compromise (BEC), also known colloquially as "CEO Fraud", cybercriminals successfully impersonate the e-mail of a CEO requesting a speedy transfer of funds from the employee (Lord, J. 2016). At the end of the day, the companies lose substantial amounts of money on reimbursements. In connection to this, SMEs were identified by Levi, M. and Williams 2013 as particularly vulnerable to cybercrime due to the having limited cyber safety awareness and dispensable funds.

Another type of cybercrime is when cybercriminals steal customer data and the firm's intellectual property which results in losses that are profound, but also very difficult to calculate precisely (Lord, J. 2016). According to a financial analysis by Levi, M., Doig, A., et al. 2017 the largest financial losses were incurred to companies rather than individuals via crimes such as business trading fraud, pension fraud, financial investments and insolvency and bankruptcy frauds. In terms of the situation in the UK, Leukfeldt, E.R., Kleemans, E.R., and Stol, W.P. 2017 identified that criminal networks are most likely to carry out high tech crime against institutions, but also that their outreach is more international in comparison to other criminal networks elsewhere in the world. Yet a cautionary note is in place when referring to criminal networks as Lavorgna, A. 2019 warned against overestimating the extent of organised cybercrime in the UK lest public funds be unnecessarily depleted. Also, In her critical piece, the author pointed out that the media use the term "organised crime" alongside "cybercrime" to amplify the emotional effect of their message. In my personal opinion, this is an important analysis because the arbitrary use of strong language amplifies a sense of threat in society, which leads to anxiety. This type of anxiety can also influence people's decisions to withdraw from the use of technology, which can have a detrimental impact as well.

4.1.3 Cybercrime against public institutions

A significant example of the latter cybercrime comes from Wirth, A. 2018 who explained the devastating effect of the WannaCry ransomware on the National Health Service (NHS) in 2017. Specifically, WannaCry impacted 81 from 236 hospital trusts and 597 out of 7 545 GP surgeries, which resulted in the cancellation of 20 000 appointments. It is perhaps cases like this one that prompted some reflection regarding the importance in distinguishing between traditional crime and cybercrime as there has been a tendency to label the adjunct cyber- as something 'sexy' rather than explanatory (Cross, C. 2019). I also uncovered that employees from within organisations were responsible for criminal behaviour albeit with a weak or non-existent financial motive. In this regard, previous research by Hutchings, A. and Collier, B. 2019 lists women as being responsible for 32% data breaches in the Police and 67% data breaches in the Health and public sector. Men were responsible for 66% of data breaches in the Police and 33% of data breaches in the Health and public sector. Whilst this analysis is insightful on the one hand, what is lacking in the research by Hutchings, A. and Collier, B. 2019 is the gender ratio in the Police and Health and public sector, which would allow for more precise conclusions. Instead, the authors supply that the Police participants were a total of 51 people, 13 people from health services and 11 from other public bodies. Additionally, men were responsible for 2% of malware attacks against the Police with the other 98% of attacks lacking a financial incentive. Both sexes were found to have committed no offences against their public sector employer, which would have had a clear monetary incentive (Hutchings, A. and Collier, B. 2019).

4.2 Policing

I grouped the various aspects of cybercrime policing in the UK using the following research themes: 4.2.1 Models, 4.2.2 Organisation, 4.2.3 Human resources and 4.2.4 Jurisprudence.

4.2.1 Models

Research by Hunton, P. 2011 has developed a model for cybercrime policing which contains eight stages. In Stage 1 the investigation of the offence is started and what is known about the cybercrime becomes established. During Stage 2 the cybercrime is modelled which also includes the technology that was used throughout the offence. During Stage 3 a specialist assessment of what is known takes place. The purpose of Stage 4 is risk assessment of the potential harms. Investigation planning takes place as a part of Stage 5. The activities in Stage 6 are focused on assessing how to handle the technological data to prevent the interference with evidence. Stage 7 is the carrying out of the intervention and Stage 8 is the reporting on the results.

Hunton, P. 2012 also identified five policing roles within the investigation framework. Here they are presented in an ascending order in terms of the expertise and risk requirements. Role 1 is the technical enquirer who can perform less sophisticated tasks as well as open-source searches. Role 2 is the network investigator, who covers networked technology. Role 3 is the forensic technician who can perform a range of expert skills including the retrieval of evidence. Role 4 is the digital forensic examiner who will be capable of conducting advanced analysis of the data including running experiments on it. The technical domain expert is role 5, which is an expert in a particular field of cybercrime.

The main strengths of Hunton, P. 2012's model are its functional specialisation and seemingly effective division of labour. Yet, it seems to me as if the model was based on a fixed hierarchical principle. This may be effective with traditional crime where the modus operandi evolves only very gradually over time and therefore radical shifts in tactics are rarer. With cybercrime however, a fixed hierarchical model can tempt team leaders to become rigid and constrained by the hierarchically organised roles. Cybercrime confers more opportunities for creativity than more traditional crimes and hence teams should operate on a flexible rather than a fixed principle. As a part of this flexible principle, even the most junior roles should have an opportunity to contribute to the investigation strategy.

4.2.2 Organisation

A major organisational challenge to policing cybercrime is that the police were not originally set-up for this kind of work. According to Wall 2013 the police are navigating their activity in a sector that originally fell under the private sector, who used responsibilisation to shift cybersecurity onto the users thereby creating victims of cybercrime. The use of the term "responsibilisation" by Wall 2013 is an adaptation from its original meaning. The original meaning denotes a shift of responsibility from the government towards the citizens. Take an example as a refresher of the canonical meaning: The local council refuses to invest in traffic lights, so that people learn to be more careful when crossing the road. The local council has made people responsible for road safety in a way that they were formerly responsible to avoid purchasing a new set of lights. In contrast, Wall 2013 uses responsibilisation to signify a shift of responsibility from the commercial sector onto the consumer. This denotes a shift where corporations take on many of the roles previously filled by the government whilst developing the same techniques used by the latter.

In an example of the increasing controversy surrounding this merger, Johnson, D. et al. 2020 observed a trend whereby the police rely on the private sector to assist with cybercrime

policing- an initiative promoted to the force. Yet, the members of the police were aware that private companies who receive potential access to data lacked the legal mandate to handle it.

Another organisational challenge comes from the Northeast of England, where the police have evaluated the effectiveness of local policing, which is supposed to be embedded within the broader national framework such as with the National Crime Agency (NCA) (Doig, A. 2018). The researcher found that the force deals with frauds as well as DoS attacks and malware attacks, yet it does not have an established line of communication with NCA. From an organizational perspective the local police are left to their own devices when tackling the evolving challenges of cybercrime.

It is also worth noting examples from the literature which highlight the strengths of the organisation in policing cybercrime (Shan-A-Khuda, M. and Schreuders, Z.C. 2019). The researchers used statistical analysis to draw connections between demographics and cybercrime victimisation, which resulted in significant results. Indeed, they found that victims of economic cybercrime were more likely to be male (56%) and from areas populated by full-time students and the Asian minority. The extent to which this a true reflection of the situation can be debated. I would argue that what is reported in research is an under-representation of the problem. Instead, I would expect that the actual figures are considerably higher as suggested by the following research piece.

Herein, the under-reporting of cybercrime was seen as an important issue in policing research (Johnson, D. et al. 2020). The lack of effective reporting resulted in the police being unable to measure the extent of crime and compile robust statistics to assess the problem. Constructively, Horgan, S. et al. 2021 envisioned a way out of this conundrum by exploiting the negatives brought on by the COVID-19 pandemic. Examples of tCOVID-19 related negatives included a 72% increase in fraud 52% increase in other, predominantly narcotic offences, between the year 2019 and 2020 in Scotland. Specifically, they suggested that the links between the local police and communities provide a network that can work together to improve cybercrime reporting in a democratic way. These points will be further elaborated on in a separate section devoted to 6 What is known about cybercrime reporting to date?.

As a part of the organisational assets in policing cybercrime, the role of Action Fraud (AF), the UK National Fraud and Cybercrime Reporting Centre occupies an important place in the policing system that covers England, Wales and Northern Ireland, but not Scotland anymore. The role of AF is to serve as the nation's key centre for reporting economic cybercrime such as fraud. AF will not conduct enquiries into reports of other crimes such as thefts of vehicles, hate speech or suspicious behaviour towards a minor. As mentioned in the 2 Background in 2.1 Police Scotland, Police Scotland have separated from AF and therefore a separate procedure needs to be followed when people are victimised by fraud in Scotland. As a part of its reporting function, AF publishes monthly statistics about fraud and cybercrime data. These have served the important purpose of highlighting the dramatic spike in cybercrime against individuals during COVID-19 (Buil-Gil, D., Miro-Llinares, F., et al. 2021).

Lastly, it is worth considering some of the organisation's unique approaches to policing cybercrime such as 'influence policing' which is based around the idea that the digital footprint of at-risk Internet users is used to tailor deterrence ads that are meant to discourage the engagement in cybercrime. If this intervention fails, then on the next level at risk Internet users are approached by officers from the NCA in their homes who offer guidance on how to avoid criminality online (B. Collier et al. 2021).

This approach raises some ethical questions, which I contrast with an analogy from the non-online domain. Imagine an 18 y.o. male whom I will refer to as "X." X goes to his local supermarket nearly every day to buy a single chocolate bar. Unbeknown to anyone apart from X, the protagonist has been tempted to shop lift. Therefore, his daily visits to the supermarket

are actually a reconnaissance mission. He is not tempted by need or poverty. He is loved by his close ones both emotionally and materially. X simply has a nihilistic propensity towards boredom and risk taking behaviour. Ultimately, X's fear of reprisal takes over and he abandons his intention. Yet, the supermarket keeps a log of visits, which it analyses to make inferences about customer behaviour. Security decides that X was acting suspiciously. Therefore, they warn him about what lays ahead for those who shop lift. How would we, as a society, feel about X being spoken to by security if he was well within his rights to behave in the way that he did?

From my perspective, a miss is as good as a mile and this applies to the use of influence policing as well. I do not believe that it is the role of the police to make assumptions about people's thoughts based on their online behaviour when it comes to economic cybercrime. Also, the act of being spoken to by the police may alienate X even further, which can then lead to an offending pathway. As someone who has worked in criminal mental health, I appreciate the elusive distinction between anti-social thoughts and actions. Why some people have thoughts of scamming and fraud, but never do, whilst others act to the contrary, remains, for lack of a better word, a mystery. The role of the police is not to disentangle this mystery, but to collect evidence of economic cybercrime post hoc.

The chances are that we will never know how many people planned to carry out a fraud, but at the last minute turned back and did not. In contrast, the thing that we find out about eventually, is approximately how many people were snooped on by the state via one of its extended arms to keep the rest of us safe. That ratio, defined as zero public knowledge about who chooses to be good when driven to be bad, versus thousands of people that can be placed under surveillance, is the essence of what could go wrong if the majority's safety is prioritised over the individual's freedom to think and act as he or she chooses.

4.2.3 Human resources

Some of the literature available on the subtopic is best understood as issues in HR. A candid piece by Sommer, P. 2017 says that what gets in the way of cybercrime policing can range from interagency competition to lack of resources to hire specialised staff. According to Sommer, P. 2017 people would struggle if taxes increased to fund additional cyber specialists.

Whilst citizens want to avoid higher taxes, the way their current taxes are redistributed should also be taken into account. It may not be the responsibility of the citizens to pay more tax if they want better policing, or the responsibility of the police to carry out a first class volume service on a tight budget. Rather, the government should consider how to redistribute taxes in a way that improves policing without increasing the economic burden on the citizen. Sommer, P. 2017 also states that companies who have been victimised by fraud should not blame the police for collapsed investigations if they have not collected the evidence of the crime precisely enough. Once again, this is an example of responsibilisation where the author automatically presumes that victims will proceed more pedantically in cases of cybercrime than they would if they were burgled. I cannot imagine a police officer telling off a burglary victim for accidentally interfering with a crime scene, so why is it acceptable in cases of economic cybercrime?

An integral part of HR is staff development and the London Met have rolled out the Ncalt training package, which is an online training to educate officers in how to deal with cybercrime. Critical research has revealed various caveats in how this training was harnessed (Forouzan, H., Jahankhani, H., and McCarthy, J. 2018). Most police officers from their study did not feel adequately trained to respond to cybercrime challenges and felt that the Ncalt training was not an effective way to upskill the workforce. About one third of the police officers were not even aware that the Ncalt package existed. The authors perplex over the fact that the London Met

does not monitor the training uptake since it is the only training on the subject that is meant to be used by the entire force.

Problems with training are a theme that re-emerges in Forouzan, H., Jahankhani, H., and McCarthy, J. 2018 and Schreuders, Z.C. et al. 2020 the former of which also identifies that HR problems stretch to recruitment and working across agencies. Interestingly, Loveday, B. 2018 supplies an example where a local police force boosted its expertise by hiring a former hacker as a staff manager and resolving staff shortages by engaging with qualified volunteer groups. Apart from such innovative HR solutions, since 2003 the problem of cyber fraud was also policed by vigilantes who congregated on forums of concerned citizens and publicly shamed people whom they assumed to be committing fraud (Button, M. and Whittaker, J. 2021).

More optimistic evidence has emerged, which found that constables did engage in some level of cybercrime training and this increased their feelings of preparedness and competence when responding to cyber frauds (Bossler, A.M. et al. 2020). Nevertheless, these successes seem to be localised as time and time again in other research a lack of training, knowledge, resources, and improper cybercrime recording come up as obstacles in the way of effective policing (Buil-Gil, D. and Zeng, Y. 2021). The paper by Cockroft, T. et al. 2021 sheds light on the issues with the training in policing cybercrime. The latter authors have found that training that is delivered face-to-face as opposed to online is viewed as more effective by the force. The evidence from within the research suggests that the effectiveness was actual rather merely perceived. This conclusion can be drawn based on the thematic analysis, which showed that 58.77% of the attendees appreciated clarification as the most important component of face-to-face learning. When evaluating online training, 33.5% stated that they liked the flexibility, but 28.31% said that online training was superficial. Hence, the conclusion that face-to-face training is more effective seems justified although more detailed information about the content of online training would be helpful.

In terms of the macro level in HR, previous research has found that police forces would benefit from clear policies and procedures when responding to cybercrime as a form of best practices approach (Bossler, A.M. et al. 2020). The difficulty with this, according to Johnson, D. et al. 2020, is that the English system is highly decentralised and therefore there is a lack of consensus as to who should have the final say over what best practices in cybercrime policing should look like. This approach has some pros and cons. The pros of decentralisation are that different approaches can be trialled in different regions to see what works best. The cons of decentralisation are that if regions do not communicate effectively, then important lessons get missed.

The last piece that fits within the HR section is from Wilson-Kovacs, D. 2021 who explored the new role of 'Digital Media Investigator' (DMI) in England and Wales. The DMIs were created by upskilling police officers to use technology to relieve the specialised teams from the more unsophisticated tasks. Whilst the idea was seen as pioneering by some, issues concerning the role content were raised by others. Specifically, the lack of rigorous recruitment, the lack of support to sustain digital skills, the lack of supervisors' cyber awareness and tensions between DMIs and accredited forensic specialists were all critiqued.

4.2.4 Jurisprudence

In Sampson, F. 2014, the author argues that current legal approaches focus on conceptualising the systems of crime but struggle to catch up with individual offenders, hence what might be required are dedicated police constables that will patrol the cyber area in a similar fashion as they do physical spaces. In the online domain, this would require dedicated offices that are populated with people that can use specialised software to monitor behaviours on the most prominent chat forums and domains. There are however various unanswered questions in re-

gards to this approach. For example, would the constables identify themselves via a username so that they could be approached by the chat users? Even if they did identify themselves via a username, would it be possible to effectively safeguard the identifiers of police constables from impersonation? These questions were not answered in the article, but are key for the implementation of police constables online.

Furthermore, the current legal approaches can also create various pitfalls for policing cybercrime, which can have unintended negative consequences for the police (Lyle, A. 2016). Examples of pitfalls include using a fake social media profile to access information on social media, which is an offence under the Computer Misuse Act 1990 or the seizure of a family PC for investigation purposes, which can violate the privacy rights of the rest of the family. To minimise the risk of this happening, Lyle, A. 2016 articulated six rules as guidance. Firstly, the police must apply the correct legislation to specific offences rather than a one-size fits all approach. Secondly, caution is urged when carrying out open-source investigations because different laws apply when this information is used by the police as opposed to the regular person. Thirdly, open-source investigations may conflict with privacy rights, which is why the justification must be rigorously established beforehand. Fourthly, the collection and storage of data needs to comply with relevant legislation whereby the data protection principles have the overriding power. Fifthly, the taking, analysis and display of evidence must be highly regulated in an evidenced way. Sixthly, all such activity must be appropriately recorded so that it can be scrutinised in the interest of transparency.

Additionally, specific national differences in legal definitions impact not just on the how but also if an offence will be investigated by the police and subsequently prosecuted in court. Take for example the problem of organised cybercrime (Leukfeldt, E.R., Lavorgna, A., and Kleemans, E.R. 2017). Imagine an organised cybercrime group of three individuals who coordinate an attack on bank customers. Investigating these individuals as an organised crime group in the UK would not be possible unless their offence was punishable with at least seven years in prison because the organised crime laws would not apply to them. Therefore, the police must remain extremely careful in how they bring forward charges because an organised group of cybercriminals in the UK may not legally constitute a form of organised crime.

The last article concerned the effects of Brexit on jurisprudence in cybercrime (Stevens, T. and O'Brein, K. 2019). Among the various concerns of Stevens, T. and O'Brein, K. 2019 were that Brexit will affect UK's capabilities in terms of policing and sentencing cybercrime. The former will be affected by the loosening of ties with Europol and the latter will come into effect as a result of severing ties with the European court system. The authors highlight that the UK alongside Germany is the highest contributor to cybercrime intelligence in Europol. Whilst the UK is not exiting the security alliances associated with the EU, its position within them will change as a result of Brexit. The question remains how this will effect the vulnerable users of technology regardless of what they voted for in Brexit? In my view, the reconfiguration of cybersecurity ties with the EU is likely to increase cybersecurity threats to the UK and the EU during the implementation phase of the transition.

5 What is known about cybercrime victims in the UK to date?

The following subsection is thematically organised as follows: 5.1 Victim profiles and 5.2 Victim experiences.

5.1 Victim profiles

I will dedicate this subheading to compiling the characteristics of the various victim profiles. Due to our evolving understanding of cybercrime victims, we currently define victims based on a very limited number of characteristics, for example as individuals or private sector institutions. In contrast, we tend to attribute many characteristics to victims, particularly individuals, in traditional crime. For example, in the latter type of crime, society stresses that a victim was "a loving mother", "a passionate and bubbly teen" or "a reliable and quirky grandad." I want to use this section to emphasise the humanity of cybercrime victims and put them at the centre of this subheading, which will be organised using the following themes: 5.1.1 From elites to the masses, 5.1.2 Routine Activity Theory (RAT), 5.1.3 Psychological perspective and 5.1.4 Correlation with age.

5.1.1 From elites to the masses

I feel that it is fitting of the world we are living in to commence this review by a high profile case. It takes a high profile victim to bring attention to the adversity affecting the masses. Specifically, in 2008, the shadow home secretary David Davis, criticised the UK government for being ineffective in tackling cybercrime after he became a victim of it himself (Hunter, P. 2008). The situation in 2008 bears some resemblance to the present situation. Then, cybercrime reporting was also a problem with Hunter, P. 2008 critiquing the lack of a dedicated centre for tackling cybercrime and the police's tendency to investigate only high value crimes. Things have since changed. The centre of cybercrime reporting was established under the name Action Fraud. However, the problem with investigating only high value offences persists. The difference being that Hunter, P. 2008 complained that only offences above £500 are investigated by the police. In 2019 that figure has increased to offences above £100 000 (Correia, S.G. 2019). The rhetorical question withstands the test of time: "Who are the current cybercrime reporting mechanisms really serving if not those that can afford to police themselves?"

The literature in connection to victims' profiles was also centred around the quantitative aspects of what it meant to be a victim in terms of defence costs (Bohme, R. 2013). In other words, the victims were defined in terms of what happened to them (e.g. the type of fraud they succumbed to) and how much it cost in pounds. Speaking of the victims' distress, the authors argued, is a practical matter that will be discounted because victims cannot sue for distress and hence it cannot be meaningfully connected to remuneration. I agree with Bohme, R. 2013 that it is difficult to put a price tag on distress. Yet, what victims go through tells us a lot about who they are as people. Discounting phenomenology means diminishing the victims' profile and humanity. Not only is this a problem from an ethical standpoint, but also because without accurate victims' profiles it is difficult to devise strategies to engage with victims in a way that would improve cybercrime reporting.

In their piece Bana, A. and Hertzberg, D. 2015 started by highlighting that between 2012 and 2014 a survey into the UK's top law firms showed that their prioritisation of cybersecurity doubled from 23% to 46%. This increase may have been influenced by an attack on ACS:Law,

a prominent UK law firm, in 2010. The hacker group Anonymous attacked the firm based on knowledge that they were defending people accused of accessing illegal pornography, which resulted in the clients' confidential e-mails being made public. The law firm received a fine of £1000 reduced from £20 000 after it declared bankruptcy. This article is more informative about victim profiles than meets the eye. In chronological order, the first victims were the lawyers who were paid for upholding the law. The second victims of the crime were the clients of the law firm who were vulnerable because the state has accused them of committing a crime and hence they were in a vulnerable position because their liberties and reputation were under threat. Thirdly, and these are the victims Anonymous have ignored, are any victims of molestation by proxy contained within illegal pornography. The latter are not molested once but every time when such a medium is viewed for sexual gratification. The only retribution for these victims is the chance that the creators and consumers of such media will be brought to justice. If, however, the right to a fair trail is compromised by publicising confidential information pertaining to the accused, the entire trial can collapse. Conclusively, what started as an attempt to punish elite lawyers may have easily resulted in damaging vulnerable victims of online molestation.

5.1.2 Routine Activity Theory (RAT)

In an attempt to compile an accurate victim profile, the research by Nasi et al. 2015 is helpful. The researchers discussed the RAT which stands for Routine Activity Theory. The core assumption of the theory could be summarised as follows, people who behave less than safely online by opening links from unknown e-mail addresses and having insecure passwords such as "12345" are more likely to become victims of crime than those who avoid opening links from unknown e-mail addresses and who use complex passwords such as "Xde9Fq14."

In the study by Nasi et al. 2015 the authors surveyed 999 respondents from the UK and matched their data with the assumptions from RAT. They found that being male, young, migrant, urban, not living with parents, unemployed with more social life online vs. offline were all predictors of becoming a victim of cybercrime such as slander and violent threats. Economic cybercrime was represented as well, specifically 28% of respondents have become victims of fraud and a further 23% were victims of identity theft.

When using the RAT, caution should be exercised when discussing victim profiles so that the rhetoric does not slide into victim-blaming. For example, Waldrop, M.M. 2016 uses the example of GCHQ to highlight, what I will refer to as, a person-centred strategy to cybersecurity. GCHQ advised its managers to be thoughtful when requiring the workforce to constantly update their passwords to prevent exhaustion. In this respect, when talking about victim profiles, I want to re-emphasise that it is important to strike a balance between security and freedom. Anybody can become a victim regardless of how secure their passwords are. If people are going dedicate too much time to securing their computers, then that will interfere not only with their ability to work, but ultimately to live a meaningful risk tolerant life.

Remaining with the RAT, subsequent research discussed the unexpected dip in the amount of victims from the private sector despite the increased amount of attacks (CFS 2018). Small and medium sized companies (SMEs) that invested in cybersecurity experienced a marked decrease in harm during 2017, a year throughout which there was an increase in cybercrime attacks. The specific figures are interesting for illustrating how victims can effectively increase their locus of control by going down this route. In particular it was found that the amount of companies using a network perimeter firewall went up from 54% in 2016 to 75% in 2017. Additionally, the amount of companies enforcing cybersecurity policies went up from 26% to 51% from 2016 to 2017. Lastly, the sum of businesses with cybcerinsurance went up double the amount resulting in 38% for small sized companies and 54% for medium sized ones. This

is evidence that RAT holds water in the private sector so long as companies invest in their own cybersecurity.

A question worth asking with respect to the findings by CFS 2018 is: What is it about the victim profiles of SMEs that made them such desirable targets in 2017? The findings by Donegan, M. 2019 state that SMEs are specifically profiled by cybercriminals due to having several vulnerabilities. Firstly, they often communicate payment correspondence via e-mails. Secondly, SMEs use of systems such as Office365 is another source of vulnerability. Thirdly, often SMEs have publicly available information on the web that pertains to information about staff. Cybercriminals will compile this information to inform their deception strategy.

Further support for RAT can be gathered from the results of Akdemir, N. and Lawless, C.J. 2020 who found that victims' online lifestyles were connected to the threat of cyber victimisation, which included the use of insecure Internet connections and public access computers. The risk of becoming a phishing victim was increased in people who both voluntarily and involuntarily shared personal information through social networking sites and online advertisement sites. Lastly, illegal activities such as downloading pirated media and streaming via illegitimate sites also increased the likelihood of becoming a cybercrime victim.

To conclude on the subject of RAT, Buil-Gil, D., Miro-Llinares, F., et al. 2021 examined the effect of COVID-19 on increased victimisation. It was found that people spend more time online and less time on the street, which resulted in a decrease of street violence and increase in cybercrime. Therefore, the COVID-19 pandemic created a novel set of circumstances that played into the core assumptions of the RAT theory, but also placed it into the online domain.

5.1.3 Psychological perspective

Next, I will analyse the research with the use of a psychological perspective to victims' profiles. In research by Jones, H.S. et al. 2019 the authors measured several psychological constructs to identify the hallmarks of a profile most susceptible to economic cybercrime. They found that people who were able to proceed with cognitive reflection (i.e. suppress incorrect information vs. correct information) were moderately less prone to opening fraudulent e-mails. Additionally, people who scored high on sensation seeking were more inclined to give into automatic processes and open fraudulent e-mails. The authors have also argued that sensation seeking might be mediated by impulsivity, which triggered the erroneous responses.

Another route into the psyche of the cybercrime victims can be taken with the use of Rational choice theory (RCT) (Connolly, A.Y. and Borrison, H. 2020). The latter scientists examined the trade-offs in victims' decision making processes when deciding whether or not to pay off a ransomware attacker. Connolly, A.Y. and Borrison, H. 2020 found a rational basis for victims' decision making processes which they summed up in the following way. The first cluster of victims that paid ransom usually had ineffective backups, the data was critical to the business, there was a real risk of bankruptcy and they followed the advice of the IT consultant. The second cluster of victims that did not pay the ransom had effective backups, the data was not critical to the business, the police advised against paying the ransom, they found the perpetuation of crime unethical and the negotiations with the cybercriminal broke down.

In my opinion, this pattern of results is interesting because it can be interpreted as attesting to various rationalisations. For example, the survival motive was prominent in the first cluster, whereas this motive was absent in the second cluster. Hence, I would speculate that the moral reasoning behind refusing to perpetuate crime stemmed from the staff's basic survival needs being met despite being victimised.

The study by Connolly, A.Y. and Borrison, H. 2020 was followed up by research examining the impact of attacks on organisations (Connolly, A.Y., Wall, D.S., et al. 2020). The latter authors corroborated the findings from the previous article by finding the private institutions

suffer much greater harm than public institutions and this was not only due to the former facing greater redundancies, but also because public institutions invested more in security. I would critique this side of the argument because I find its assumptions narrow. Whilst, yes, a public institution is going to carry on regardless of the size of the attack, what about the population its meant to be serving? I would have welcomed an emphasis on the suffering of those affected by the lack of service during a ransomware attack on a public institution. Moreover, Connolly, A.Y., Wall, D.S., et al. 2020 found that made-to-measure attacks were more severe than generic ones based on the utilisation of background information about the victim's profile.

I feel it is suitable to round up with a qualitative psychological study that entails victims' phenomenological perspective. Indeed, the research by Button et al. 2021 uncovered evidence of both psychological and psychosomatic effects of becoming victimised. It was found that people experienced, headaches, flare ups of existing conditions such a fybromyalgia and Crohn's disease, withdrawal from relationships, isolation, depression, anxiety, and suicidality. People with existing mental health conditions reported a resurgence of difficulties. As can be seen from this information, the distress of the victims is profound. In some cases, unlike in the conclusions by Bohme, R. 2013, victims' adversity contains a measurable component such as a resurgence of an existing condition post-victimisation. Take for example the effect of victimisation on mental health. Changes in mental health can be empirically measured in a range of ways starting with psychometric questionnaires. If the expert witness willed it, psychometric questionnaires can contain concealed malingering questions to assess for instrumentality in responses. A less robust, but admissible way to measure changes in mental health can be via keeping a diary and recording changes in sleeping patterns to name but a few measures available to the general public. Justifiably, real measurable harm that can be proven through court is taking place.

5.1.4 Correlation with age

An important characteristic to consider during the compilation of victims' profiles is age and its effects. Thus, Correia, S.G. 2020 examined the demographics of repeat victims of economic cybercrime in the UK. The researcher found that in cases where repeat victimisation has occurred, more incidents were reported by men rather than women. An average repeat victim was older than an average single case victim. Both the median and the mean ages are higher for the repeat (median is 57, mean is 53.6) vs. single case victims (median is 50, mean is 49.93). The advantage of this research is that it can be used to direct preventative resources more effectively. I would argue that these statistically significant findings are of a nuanced nature where both groups, that is repeat victims vs. single case victims, are essentially people in their fifties. In my opinion, setting up an effective economic cybercrime reporting system is key before we move on to more nuanced differences within the victim groups.

Age was argued to play a significant correlation with respect to romance fraud during the COVID-19 pandemic (Buil-Gil, D. and Zeng, Y. 2021). An opposite pattern relative to the previous piece by Correia, S.G. 2020 was found. Mainly, younger people vs. older people were more susceptible to romance fraud as a result of loneliness and isolation, which was reflected in their increased use of the Internet. The use of Internet for communication was the highest for the over 16s and then gradually toned down across the groups until reaching a minimum in the over 70s.

5.2 Victim experiences

In this section I will make an extrapolation from research on the Western population (i.e. Europe, USA and Australia) onto the UK and hence Scottish population due to there being an insufficiency of research from the UK. This section will be subdivided according to the geographical jurisdictions from which the respective research originates: 5.2.1 European Union, 5.2.2 Australia and Canada, 5.2.3 United States of America and 5.2.4 International collaboration.

5.2.1 European Union

At the beginning of this section, I will supply an overview of cybercrime in the European Union since 2010 based on previous research that surfaced via the systematic analysis (Reep-van den Bergh and Junger 2018). In regards to economic cybercrime in the European Union it was found that online shopping fraud affected between 0.6-4% people annually. In comparison, online banking fraud was found to be less common at around 1-2%. Moreover, less than 1% of the population were victimised via advance fee fraud or identity fraud. Britain being in the EU at this point was also included in the research with the finding that 0.5% Brits were victims of an "Online Romance Scam." To complement these figures, the research by Huaman et al. 2021 into Germany's SMEs found that 45.1% of interviewed employees reported that their SME had to respond to at least one cyber attack. Additionally, more than 50% (i.e., 1 842) were attacked on multiple occasions.

Bohme and Moore 2012 wrote an intriguing article concerning the experiences of people in the EU who have either been victimised by cybercrime or have heard about the threat of it. Bohme and Moore 2012 found that in people who have been victimised there was a 4-5% decrease in shopping and banking online. Moreover, people who have been exposed to information about the threats of cybercrime were twice as likely to diminish their online activity in comparison to those directly victimised. What I find interesting is that anticipatory anxiety is a stronger behavioural modifier than a crime actually occurring. This matters because anticipatory anxiety is not necessarily protective from economic cybercrime unless a person were to completely abstain from the Internet. Rather than suffering from anticipatory anxiety, the state should split the responsibility with its citizens. One the one hand, people should be supplied with easy to understand guidance on how to use the internet. On the other hand, the state, banks and all of those that can really afford it, should make the Internet a safer place for all of those who cannot. This type of information could be imparted via regular state-sponsored awareness raising campaigns.

Another perspective considering Dutch victims' experiences is found in a study by (Van De Weijer and E.R. Leukfeldt 2017). This study examines how "The Big Five Model" of personality influences people's susceptibility to becoming victims of cybercrime. The aforementioned model is a contemporary and empirical model of personality, which presumes that every personality can be conceptualised with five factors, which are: Openness (to experience), Agreeableness, Neuroticism, Conscientiousness and Extraversion. The main idea is that every personality has all these traits to some degree, but the extent to which the traits are expressed defines the characteristics of the personality. Based on the results of Van De Weijer and E.R. Leukfeldt 2017 the authors concluded that people high on Neuroticism, low on Conscientiousness and high on Openness (to experience) were likelier to become victims of cybercrime. Whilst the research offers an interesting insight into the phenomenological experience of victims, clearer causal links between particular personality facets and types of cybervictimisation would have been beneficial to avoid making assumptions about people based on their personality make-up. Another critique is that future studies should also entail the concept

of self-awareness into their design. Whilst someone can be very open to experience and very low in conscientiousness, they may also be aware of these traits, which can result in making safer choices.

When discussing victims' experiences it makes logical sense to connect these with their needs as was done by ER Leukfeldt, Notte, and Malsch 2020 on a diverse sample of Dutch victims. They evidenced that victims of economic cybercrime have pronounced emotional needs, which revolve around receiving recognition from society and the police for their ordeal, which is linked to being able to tell their story. Fraud victims in particular have a need to remain informed about the court proceedings with all victims citing retribution as an important need. Victims also need to receive detailed information from the police about the processes that are triggered by their report. Then, victims also experience a range of practical needs that relate to requirements to liaise with banks, social media platforms, etc. to mitigate the effects of the crime. Understandably, financial needs are particularly high among victims of fraud, which can culminate into the endangerment of primary needs. ER Leukfeldt, Notte, and Malsch 2020 described an example of a woman who lost all of her saving to dating fraud and could not afford to stay in her house and hence had to move in with her social circle to avoid homelessness.

How the victims' experience the crime also plays into whether they decide to report it or not. In particular, S. van de Weijer, R. Leukfeldt, and Van der Zee 2020a found that the type of cybercrime influences Dutch victims' motivation to report. Victims of various forms of economical cybercrime (e.g., fraud, romance scams etc.) were more likely to report the incident to the police, especially if they incurred some type of financial loss. This effect was more pronounced in serious vs. less serious offences.

5.2.2 Australia and Canada

Despite the geographical distance between Australia and Canada, they have been collapsed in this section due to a significant piece of research included within that has been concurrently run in both countries.

The effectiveness of the calculative trust marker in phishing was explored by the subsequent piece (Lacey, Salmon, and Glancy 2015). Using the example of a phisher impersonating Australia's post, the authors show how victims are misled into experiencing trust in forced choice paradigms. For instance, the phisher will force the victim to click on a link impersonating Australia's post because the link will purport to provide more information about a parcel, which will otherwise not be delivered. The victim is then drawn to believe that by clicking on the link they will merely receive additional information, which becomes the access point for the phisher. Hence, the experience of trust is an important antecedent to become a victim of phishing.

The next article by C. Cross and Kelly 2016 is an interesting example of the disassociation that victims experience between warnings regarding cybercrime and their experience of it. It was found that educating people about the specific types of cyberfraud was an ineffective protection strategy mainly because the recipients struggled to apply the messages into their lives. Citing examples of Ruth and Hazel, the researchers uncovered that in the first instance Ruth sent sums of money oversees to a person she thought she was in a relationship with despite knowing about romance fraud. The emotions Ruth invested in this pseudo-relationship stopped her from making the connection between what she knew about romance fraud and her specific situation. In the case of Hazel, she knew about investment fraud. Nevertheless, when she was approached by a scammer who disguised the crime as a contracted business opportunity, Hazel did not apply her knowledge of investment fraud to her situation and ended up loosing £300 000. C. Cross and Kelly 2016 advise that people should not be overloaded with informa-

tion during awareness raising campaigns. Instead they should receive two key messages: First, do not share your details with anyone online. Second, never transfer money to anyone you met online. I agree with the general gist of C. Cross and Kelly 2016's advice because it takes into account people's preference to enjoy online communication, be it romantic or otherwise, whilst supporting them to do it safely.

Moving to a study of victims' experiences of reporting cybercrime to the Australian authorities, C. Cross 2018 identified that people's experiences were often influenced by unrealistic expectations. The author referenced the "Merry-Go-Round effect" when victims approach an agency for assistance with fraud. Victims in this situation experience being referred from one agency onto the next one without getting any closure about what they have been through. Victims also experience confusion with respect to how the jurisdiction of the crime is assigned to the police jurisdiction. Victims do not realise that police forces with broad competencies, such as the Australian Federal Police in this instance, cannot investigate international fraud. As well as experiencing significant trauma, the victims often overestimated the force's information sharing capabilities expecting that their reports will quickly be sent to the correct addressee. Lastly, victims in Australia experienced what C. Cross 2018 coined the "CSI" effect based on the popular TV show. This refers to the victims' expectations that the police have far greater technological and investigatory powers than is really the case.

Weighing against each other students' experiences of cybercrime victimisation vs. knowledge of cybercrime and demographics Abdulai 2020 examined a sample of 462 students to compare fear of credit card fraud. According to Abdulai 2020, demographics have no effect on the amount of fear a person experiences in anticipation of a crime. The author takes this as evidence for the assumption that everybody is fearful of cybercrime in a similar way. Whilst one can, to some extent, control safety in the physical world (i.e., live in a better neighbourhood with burglar alarms), one finds it much harder to gain the same sense of safety in a world that is governed by online principles. Moreover, Abdulai 2020 found that, understandably, this effect was more pronounced in people who were victimised by cybercrime.

The pattern of result from a study by Cross et al. 2021 added to the generalisability of people's erroneous perception that they can effectively protect themselves against economic cybercrime. Cross et al. 2021 found that communities perceived their risk of victimisation as low whilst at the same time most have reported being victimised by some form of cybercrime. The police, who were a control group, stated that they perceived people's ability to safeguard themselves as low, whereas the community members experienced high confidence to stay safe online. Hence, this is evidence of the type of disassociation that is present in other studies where people's perceptions of themselves differ from the evidence supplied by reality.

5.2.3 United States of America

A study from the USA on international students who were targeted by phone scams and Craigslist scams revealed some important components of the victims' experiences, in particular how a victim's lack of relevant knowledge can be used against them (Bidgoli and Grossklags 2017). On the one hand the majority of international students did not feel targeted because of their background. On the other hand, the participants felt targeted by the phone scams because the latter was connected to their immigration status in a threatening manner. Due to their lack of experiences with the FBI and the IRS, the students did not know that the agencies would not phone people to threaten them. In hindsight, the participants acknowledged that whilst they did not feel specifically targeted, being an international student put them in a vulnerable position. In my opinion this is a valuable piece of research because it goes some way to show that particularly vulnerable groups do not see themselves in that light, which can increase their vulnerability. There also seems to be some conceptual overlap with the findings by C. Cross

and Kelly 2016 who also stated that the victims did not feel vulnerable albeit with a different argument in mind.

5.2.4 International collaboration

The last piece of research that will conclude the section on victim experiences is the result of an international collaboration between the U.S.A., Germany, Canada and UK. It is fitting of the subject matter that this piece by Monteith et al. 2021 concerns the connection between victims' experiences and psychiatry because mental health is likely to be affected by economic cybercrime. Starting from the beginning Monteith et al. 2021 found that the the COVID-19 pandemic caused a change in how people socially interact for professional, educational, health, financial and personal reasons. These changes interact with people's mental health in two cardinal ways. Firstly, even otherwise mentally unaffected individuals may slide into mental illness as a result of falling victim to cybercrime. This can be the result of anything from suffering dire financial consequences post-victimisation to not being able to effectively grieve after the loss of a romantic relationship with the cybercriminal. Secondly, people with pre-existing mental health conditions are particularly vulnerable to economic cybercrime. For instance, people with emotional instability can engage in risky behaviours but also people of an older age can become more vulnerable as their short term memory and cognitive abilities become affected. Taken together, the COVID-19 pandemic presented new risk factors for developing a mental illness as a result of cybercrime victimisation as well as an increase in risky behaviours by people with pre-existing psychiatric conditions.

6 What is known about cybercrime reporting to date?

The following subsection is thematically organised as follows: 6.1 Cybercrime reporting approaches and 6.2 Cybercrime reporting results.

6.1 Cybercrime reporting approaches

The literature on this subsection is best grouped according to three classifications, which denote distinct approaches to reporting. The Human To Human (H2H) approach refers to traditional forms of reporting which are based on interactions between human actors. Human To Machine (H2M) approach relates to those forms of reporting and interventions where a human navigates a computer to report cybercrime. Machine To Machine (M2M) approach relates to automated interventions for improving cybercrime reporting and analysis.

Based on my knowledge, this taxonomy is entirely original and if it became established, then it would make a functional contribution to systematic analysis.

Being able to use abbreviations such as "H2H" in their keyword search would transport social psychologists to research, which is related to the interpersonal aspects of cybercrime reporting. In contrast, an IT engineer seeking to secure a system against breaches will key in "H2M" or "H2H" to focus on the intersection between human to machine, or machine to machine respectively.

6.1.1 Human To Human (H2H)

To begin this subsection, the research by Bidgoli, Knijnenburg, and Grossklags 2016 serves as a series of explanatory case studies of how some of their participants reported economic cybercrime using the H2H approach. For example, one victim reported online shopping fraud to their bank in order to cancel their card, but also to Abercrombie & Fitch because the fraudulent website was mimicking the designer brand. A victim from another case study reported the computer virus to Dell customer service. Yet, none of Bidgoli, Knijnenburg, and Grossklags 2016's participants reported the crime to the police.

As I highlighted in the previous subsections, 4.2.2 Organisation and 4.2.4 Jurisprudence, responsibilisation resulted in changes to societal expectations as to who is responsible for making the Internet a safe space, which is free from economic cybercrime. In an interesting article by Jhaveri et al. 2017 the authors put forward a framework for understanding the voluntary response to economic cybercrime. By using the phrase "voluntary response" I am referring to the reporting and resolving of cybercrime in an predominantly H2H manner amongst actors from private institutions. The incentives for participation are the protection of the brand and service reputation. It was argued in the article that the protection from disrepute outweighs the direct financial losses. Moreover, the private institutions participate willingly in sharing information about attacks among other firms because they receive intelligence about how their counterparts were attacked. Taken together, economic cybercrime has created solidarity among private sector institutions who were able to put competitive advantage to the side and assist each other with self-policing this toxic phenomenon.

H2H poses novel demands on the reporting infrastructure, which is accustomed to accepting complaints about traditional crime. Take C. Cross 2020a and the problems of jurisdiction that victims and police have to face. As pointed out by the researcher herself, a criminal from country A can target a victim in country B by getting them to wire finances to country C. In what jurisdiction has the crime taken place? As a result victims who report cybercrime often

have misconceptions about the various policing bodies in Australia. In order to mitigate this, The Australian Cybercrime Online Reporting Network (ACORN) was established in 2014 as centre for processing the aforementioned complaints. Yet, C. Cross 2020a concludes by saying that greater transparency is needed about how ACORN processes individual reports as well as more awareness raising about the competencies and limitations of various police forces.

In a similar vein, Popham et al. 2020 explored the extent to which economic cybercrime was reported by police based on complaints that they received from the public. The research found considerable variations in police reported cybercrime across Canada's jurisdictions with under-reporting being the overarching theme. One reason for this can be legislative. The authors argued that cyberlegislation is just traditional criminal law, which has received a jargon revamp whilst resting on unchanged principles. They argue that this causes problems for reporting due to the constantly evolving field of economic cybercrime. The latter cite an exception to the rule taken from a manual by the Canadian Centre for Justice statistics, which states that: "any fraud that involves the unauthorised use of a computer or use of a computer for illegal means" constitutes the basis for cybercrime reporting. Moreover, a dismissive viewpoint of cybercrime reporting was also considered as a source of variation.

Using a hypothetical and simulated setup, S. van de Weijer, R. Leukfeldt, and Van der Zee 2020b presented 595 participants with vignettes about cybercrime to explore who they would report to predominantly. Several interesting patterns of responses surfaced as a result. Within I will be concerned with just those connected to economic cybercrime. In all cases of economic cybercrime (i.e., malware, ransomware, phishing, online consumer fraud, online dating fraud) people were more likely to report the offence to an organisation other than the police. The exception being identity theft where people were equally likely to report the offence to the police and another organisation. The distinction at hand is especially obvious in the case of phishing where 49.7% respondents would rather report to an organisation other than the police and only 9.4% would report to the police. Online consumer fraud, which is one of the most common economic cybercrimes, would get reported 36.7% to another organisation and 25.6% to the police. S. van de Weijer, R. Leukfeldt, and Van der Zee 2020b conclude that the take home message for the police is to strike up more effective multi-agency cooperation to increase people's reporting to the police.

In stark contrast to the hypothetical setup by S. van de Weijer, R. Leukfeldt, and Van der Zee 2020b the study by Yadav et al. 2021 is based on a real world case study. The study is interesting because it illustrates the grey area when talking about cybercrime in a strictly economical sense. In fact, I prefer to think of crime as form of anti-social relationship between people where one party or multiple parties incur some form of harm. Yadav et al. 2021 talked about the case of a cyberstalker by the name of Jason White who owned an art gallery in Los Angeles. The offender created abusive websites to target various actors in the business and managed to extort over $3 000 000 from his victims. Eventually, Jason White was apprehended and sentenced to 60 months behind bars. This study is powerful because it uses a story to convey its point. It also contains an important weakness, which is the lack of specific details about the processes of reporting and investigation, which would allow me to align it with the systems under debate.

Sitting somewhere in between studies about H2H and H2M is a piece from Saudi Arabia by Alzubaidi 2021, who touched upon reporting cybercrime among nationals. Based on the research findings, in a sample of 1230 respondents, 267 (21.7%) were victimised. From this percentage only 78 (29.2%) reported the offence to an agency. Alzubaidi 2021 found that 31% would not know whom to report to, but would ask their friends, 15% would use the Saudi government e-portal and only 7% would report to the police directly. These data can be taken to mean that much like elsewhere in the world, people are confused about who to report to.

Nevertheless, government's oversight in Saudi Arabia is more pronounced as a portion of the participants would report directly to its portal. Yet, as has been the case in previous research, people were not particularly likely to associate cybercrime victimisation with police reporting.

6.1.2 Human To Machine (H2M)

Heinonen, Holt, and Wilson 2012 described the reporting to the U.S. Internet Crime Complaint Center (IC3). The IC3 receives complaints via its online interface from the public, but also other organisations such as PayPal for example. The IC3 also maintains a presence on the websites of the FBI and the National White Collar Crime Center (NW3C). The IC3 holds its own academic and industrial conferences but also engages with local communities and senior citizens to warn them about economic cybercrime. In addition, a diversified critique of IC3 was supplied by Bidgoli and Grossklags 2016 who highlighted the systems main strengths and weaknesses. The main strength is that it provides helpful advice and tips on how people should protect themselves online so that they do not fall into a trap and become victims of economic cybercrime. The main weakness is that the IC3's work is insufficiently publicised so people do not have as much access to the information as they would require. Also, Bidgoli and Grossklags 2016 argue that the IC3 is a federal platform, whereas a substantial amount of cybercrime is localised. Hence, reporting channels that serve particular communities would be better equipped to respond to the localised nature of economic cybercrime.

In a paper by Bidgoli, Knijnenburg, Grossklags, and Wardman 2019 the authors streamlined a procedure for reporting cybercrime in the PayPal service. The outcome of their study was a reporting interface that was user-friendly for the lay person from the street. Apart from the latter, the interface achieved two important goals. Firstly, it effectively connected reports within PayPal and outwith PayPal with the relevant entities. Secondly, the interface raised awareness of cybercrime among the company's customers. The model itself was tested using 523 Amazon Mechanical Turks who offered positive feedback. The interface was structured around three key criteria. The first criterion was that it had to match the real world, which meant that the creators defined relevant jargon (e.g., phishing) and used lay language wherever possible. The second criterion was higher user freedom and control, which was programmed into the system by allowing users to undo any mistakes by pressing the "Back" button at the bottom of the page. The third criterion was minimalism, which meant that the authors included only the minimum amount of information on the interface that was required by the user to progress through the report.

Similarly, Mapimele and Mangoale 2019 devised a H2M platform, which they named the cybercrime combating platform (CP3). The algorithms of the CP3 allow users to use the search bar to check whether any of their data has been compromised. The system, which is serviced by people makes use of databases to crawl through data of cybercrime activity online. The databases it engages are: HaveIBeenPwnd, Phishtank, Dshield and Breach Level Index.

Yet not all research that is out there is about how specialists can improve cybercrime reporting. To the contrary, Baror, Ikuesan, and Venter 2020 realised that low cybercrime reporting can be caused by a lack of clear criteria that victims can follow when reporting a crime. Therefore, Baror, Ikuesan, and Venter 2020 used their research to put forward a set of transparent criteria that could be utilised from the victim's end when inputting data into the designated platform. The criteria are: *1. Physical location*, which pertains to where the victim was physically in space when she was targeted by the scam text message. An example of a physical location is Glasgow (Scotland). *2. ISP/Cloud Provider* relates to the unique digital gateway via which the attack has occurred. *3. Nature of cybercrime*, which is the type of offence that has taken place such as cyberfraud. *4. Cybercrime description* refers to what is known about the attacks such as the language used by the offender as well as any other discernible

characteristics that can be used to specify what has happened. *5. Estimated start time & end time* refers to the approximate time windrow during which the crime has happened. *6. Other specifiers* relates to any other material retained by the victim which can be used to assist with the investigation such as screen shots of chat logs. Lastly, *7. Digital investigation artefacts* are loose types of data such as registry keys, timestamps, files and so on. I consider these criteria to be a meaningful guide when designing reporting systems to ensure a high degree of specificity.

Returning to some of the information from the previous section 6.1.1 Human To Human (H2H) by C. Cross 2020a a follow up study by the same author offered an independent analysis of the ACORN system, which has since been decommissioned (C. Cross 2020b). She found that the victims who reported to the ACORN online system experience high levels of dissatisfaction, specifically 77% of complainants were unhappy with the outcome of their complaint. Also, according to the author, the data captured by ACORN was of poor quality and there were numerous reasons for this. Many people logged that someone attempted to scam them, but not actually succeeded. Also, victims viewed money that they were promised vs. money that they lost as a form of crime. Moreover, victims inflated their actual losses to get the police's attention and victims submitted multiple reports in the hope of having a greater impact. Lastly, C. Cross 2020b found that people struggled to keep within the remits of what ACORN was designed for, i.e. the reporting of economic cybercrime. In fact, out of the 65 000 incidents, 16% of reports related to illegal content found online such as sexual abuse and exploitation material, which further muddied the data.

Additionally, cybercrime reporting should not be reduced to merely passing on information about about an offence to a relevant body. Rather the way the information is stored and subsequently analysed should be included in the equation about reporting (Das et al. 2021). The latter research identified the problem of how reports were stored. In the case of cybercrime, reports were stored in an unorganised text form where one document pertained to different criminal activities, which made the investigation of patterns very problematic. To make a step towards resolving this issue, Das et al. 2021 used principles from Natural language processing to create a set of graphs that makes connections about offences in an analysis supportive way.

Preparing the ground for some of themes in the next subsection 6.1.3 Machine To Machine (M2M), Mackey et al. 2020 investigated the proliferation of fake COVID-19 related health products on Twitter and Instagram. In order to report and analyse the scams, the authors first scraped Instagram and filtered through Twitter for keywords that are connected to the selling of fake COVID-19 remedies and tests. During the second stage, the data was analysed with the use of deep learning and Natural language processing (NLP), which is a multidisciplinary domain dedicated to teaching computers how to analyse large chunks of language. In total, Mackey et al. 2020 analysed 6 029 323 tweets and 204 597 Instagram posts. After the application of deep learning and NLP, the authors identified 1 271 tweets and 596 Instagram posts connected to the dubious sales of questionable COVID-19 related health products.

6.1.3 Machine To Machine (M2M)

A novel approached pioneered by Carpineto and Romano 2020 designed an automated pipeline with two machine learning stages to identify sellers of counterfeit luxurious clothes. This prototype was found to be more effective than established trustworthiness systems and non-expert humans. This piece is included because it closely ties to two forms of economic harm caused by dishonesty. Firstly, the sellers of genuine brands lose profits to the fraudsters, but secondly people who think that they have landed a good deal on a designer purse, are actually scammed out of money. Taken together, this research shows a promising new direction in cybercrime reporting whereby automation of the reporting process can be streamlined.

Similarly, in a technical piece by Sheikhalishahi et al. 2020 the authors offered an exploration and resolution of the problem of spam e-mail automated analysis and classification. In their article the authors put forward an automatic method and resulting framework founded on pioneering categorical divisive clustering, utilised for both classification as well as grouping of spam e-mails. Specifically, the grouping is harnessed to diagnose campaigns of comparable spam e-mails, whilst classification is used to name particular messages according to their intended purpose (e.g., phishing). The authors put forward the CCTree algorithm for grouping and classification in batch and dynamic forms to navigate via both large data sets and data streams. Subsequently, the CCTree was applied by the authors to spam to fulfil its intended purpose.

In remaining with the subject of phishing, a technological development by Singh et al. 2020 delved into identifying the difference between the latter and a classical web page. This task was found to pose challenges due to the semantic structure involved. Singh et al. 2020 managed to apply a phishing detection system with the utilisation of deep learning mechanisms to safeguard against these cyber assaults. The framework works using URLs via an application of the convolutional neural network (CNN) with an accuracy of 98%. The CNN is a type of deep learning algorithm capable of inputting, analysing and differentiating between images. Feature engineering, the process of using speciality knowledge to extract features, has been removed as the CNN pulls out features from the URLs via an automatic process through its hidden layers.

6.2 Cybercrime reporting results

The purpose of this subsection was to scrape up any remaining literature via the systematic approach and highlight any gaps not covered by the previous searches in this section. In doing so, a collage of findings surfaced which is presented chronologically below.

Closely tying into the previous subsection, the research by Nappa, Rafique, and Caballero 2015 looked at the results of cybercrime reporting in a design that explored drive-by downloads. These types of downloads refer to two main types of downloading. Firstly they are concerned with downloads triggered consciously but without an understanding of the consequences, secondly the download is triggered illicitly to install some form of malware. Drive-by downloads are rolled out via cloud based servers with 60% of servers hosted by specialised cloud hosting services. According to Nappa, Rafique, and Caballero 2015 the designated servers fall into two types. The first one is called a short-lived server, which launches attacks for about 16 hours, the second one is called a long-lived server which can carry on for multiple months. The researchers analysed reports to ISPs and hosting providers for 19 long-lived server. The result was that 61% of the reports did not even receive acknowledgement. For the reports that were acted upon, it was found a server lives for another 4.3 days after the report was submitted.

An interesting take on the results of cybercrime reporting was considered in a piece that analysed the effects of reports by technological specialists adapted by the media (Winder and Trump 2015). The authors found that the sensationalist reporting has shifted the focus in an unhelpful way. This was best expressed by a historical quote used in the paper, according to which: "The one that defends everything, defends nothing." Let me unpack the argument that is hidden behind this eloquent principle. They specifically argue that people's reluctance to disclose specific system vulnerabilities results in reports about grand attacks. Whereas, if people were more open about reporting what aspects of their systems were permeable, then this would allow a much more fine grained discussion about how to defend against such attacks. Therefore, Winder and Trump 2015 recommend that reports about cybercrime should be less grandiose and more specific if they are to result in an effective defence.

Returning to a more common perspective, on cybercrime reporting results, Prislan et al. 2019's work can be used to speculate about what results people expected to see post-reporting. In their student sample, the vast majority experienced cybercrime as a form of psychological aggression (e.g., stalking). However, only 26.7% experienced cybercrime with an economic incentive such as online scams, bank frauds and sextortion. Most people expected to see positive results if they reported to a friend in hope of getting advice (77.9%) followed by the police (76%). The interesting aspect of Prislan et al. 2019's findings was that whilst 38.4% of respondents would seek help from the Slovenian Computer Emergency Response Team (SI CERT), a a reporting system similar to Action Fraud in England, 33.7% of participants had never heard of this centre. This is critical because it is another piece of research that highlights the international theme of people not interacting with cybercrime reporting centres. Consecutively, it can be difficult to follow-up on the results of cybercrime reporting, not just in Slovenia, but globally if citizens do not engage with the dedicated tools.

As I have shown before, various factors influence people's expectations of whether cybercrime reporting will bring about the desired results. In this respect, S.G.A. van de Weijer, R. Leukfeldt, and Bernasco 2019 used a Dutch population to show that males vs. females reported fraud to the police more often, whereas females vs. males reported identity theft more frequently to organisations other than the police. Furthermore, there was a general trend to report repeat victimisation to other organisations, but this trend was reversed when reporting to the police. Once again, this pattern of findings suggests that people do not expect the police to be deliver on the results of their cybercrime reports. Instead, if I were to be optimistic, I

would say that people feel that this responsibility is shared between the police and other organisations. The latter research connects effectively to its Belgian counterpart by Kimpe et al. 2021 who found that only 28% of respondents reported cybercrime in an official way and only 10.8% reported to the police.

A piece that carried out the painstaking task of tracing individual cybercrime reports to the offenders brought forward some interesting results (Buil-Gil and Saldana-Taboada 2021). The authors have focused on Bitcoin to investigate economic related cybercrimes such as blackmail, fraud, sextortion etc. It was evidenced that a relatively small number of offenders are responsible for a relatively large number of offences in cybercrime. A deeper analysis of these reported results revealed that the offenders that attracted the most reports are not always the same ones as the offenders which made most money. This is evidence of the type of results that can be generated when cybercrime reports are analysed as well as the kind of conclusions that can be gleaned. From this, I can also see that there is significant skills diversification among offenders whereby ones tend to launch multiple attacks as kind of fishing expedition whilst others are more sophisticated and precise.

In a rare qualitative article revealed via the systematic approach, Hadlington et al. 2021 interviewed sixteen frontline police officers in order to examine the crucial aspects of cybercrime. The police staff found that they continued to struggle with how to define cybercrime, its constantly evolving nature and lack of appropriate training that would help them remain on the cutting edge. From this research it is clear to me that the police are in a similar place to the public when it comes to economic cybercrime. Also, in my view, I get the sense that the police have low self-confidence in their abilities based on the responses provided to the interviewers. If I think about some of the earlier studies from this section, where people said that they were unlikely to report cybercrime to the police, it seems plausible that the police's lack of confidence may have been a contributing factor.

Lastly, it seems fitting to conclude with a study that analyses the results of reports from Action Fraud during COVID-19. I say it is fitting because Action Fraud and its critique is responsible for driving some of my current research and, of course, COVID-19 remains the most pertinent challenge faced by society today. A research paper by Kemp et al. 2021 analysed the changes in cybercrime during the pandemic and found, as anticipated, that there was a significant increase in this type of offending. However, their findings were nuanced and warrant a couple of concrete examples. For instance, Kemp et al. 2021 found that the closing of physical shops resulted in people shopping for clothes online, which resulted in increased shopping fraud. On the opposite side, a reduction in ticket related leisure activities and aviation resulted in a decline of ticket fraud. Additionally, the researchers found that organisations as opposed to individuals experienced decreased cybercrime. The explanations for this are speculative, but relate to the closing down of businesses and restructuralisation, which resulted in an inability to detect crime. Taken together, the article by Kemp et al. 2021 is a fitting concluding statement because it brought this research right back to Action Fraud, which is partially effective at supplying descriptive data, but less effective at providing explanatory data.

7 Discussion

At the beginning of the 1 Introduction I put forward three research questions with the aim of illuminating the cybercrime landscape where economical crimes of dishonesty prevail. I have answered these questions exhaustively by discussing the articles revealed by the systematic approach. Now, I will discuss the research from the systematic literature review in connection to the situation in Scotland as I analysed it in the 2 Background. The subsections are subdivided according to the three research questions. I will discuss only a small number of selected relevant articles from the main body.

7.1 What is known about cybercrime research in the UK to date?

My research seeks to address the improved reporting of high volume low value crimes, which is the type most likely to affect individuals (Levi, M. 2017). The modus operandi can stretch to involve a sexual incentive (Hutchings, A. and Pastrana, S. 2019; Pastrana, S. et al. 2019) or a romantic one (Whitty, M.T. 2018). Moreover, the modus operandi will target particular vulnerabilities in the individual ranging from loneliness brought on by the COVID-19 pandemic (Buil-Gil and Saldana-Taboada 2021; Cross, C. 2021) to scamming people into sending money by falsely claiming to have found their beloved pet (Levi, M. and Smith, R.G. 2021). What these examples share in common is that all victims were targeted via their emotional needs. Improving cybercrime reporting in Scotland could entail an awareness raising campaign in community venues, which will help potential victims understand their needs and how those can be used against them by criminals (Karagiannopoulos, V., Sugiura, L., and Kirby, A. 2019).

When comparing these findings with Police Scotland's Cyber Strategy (Police Scotland and Scottish Police Authority 2020) it becomes clear that the callous criminals will target people who are vulnerable by a combination of age or disability, and loneliness. Therefore, to improve the reporting of cybercrime, effective identification of at risk people needs to take place. Such a risk assessment would include information about those in the community that are lonely and isolated as the two factors are major contributors to victimisation. Yet, identifying the latter type of people will be especially challenging as, by definition, if someone is lonely and isolated, then people are less likely to be aware of their existence, needs and vulnerabilities. Community police officers in combination with community mental health teams (CMHTs) are best placed to identify these people in Scotland. It is through their collaboration cybercrime can be prevented and reported more effectively. Indeed, prior research has shown that local officers possess significant background knowledge of the localities that they police, which can enable them to devise tailored policing measures (Wooff 2015; Wooff 2016).

In 4.2.1 Models I also engaged with Hunton, P. 2012's five policing roles investigation framework as a way of dividing functional specialisation within investigations into economic cybercrime. I said that the approach had a potential pitfall because team leaders could become constrained by the boundaries of the roles where a creative fully-flexible approach would be more helpful. In the context of the Scottish situation, models of functional specialisation support the 2013 centralisation reforms by the nationalists. This is owing to the fact that functional specialisation creates the conditions for accountability far more than fully-flexible teams. That is to say, if an officer has to meet the specific requirements of their role description, then it becomes easy to measure whether she has succeeded or failed based on a simple box ticking exercise. In contrast, if I were to take a fully-flexible team where everyone can offer their ideas, then I might find that some people are always driving the investigations whilst others are merely free-riding in the system whilst wasting tax payers' money. If improved

cybercrime reporting is to take place in Scotland, then a balance needs to be struck between the need to remain flexible and open to new ideas on the one hand, but also having clear systems of accountability on the other.

Johnson, D. et al. 2020 evidenced the enduring problem with the accurate counting and compilation of cybercrime reports. As I mentioned in the 2 Background in 2.2 Crime numeration the accurate recording and counting of crime has been a problem since the 1930s (Maltz 1977) and endures despite the dramatic advances in technology. This might be due to the fact that we have been looking at the problem of counting crime purely mathematically. Counting crime is very different from counting the amount of grain collected by an industrial agricultural machine. When we speak about "counting crime" we are inevitably describing a social interaction, which is why counting crime may be more of a qualitative exercise than meets the eye. I argue that it is these interpersonal complexities that result in poor cybercrime recording strategies because every crime is slightly different and hence capturing "the right information" is impossible if the police officer does not know what the complete mosaic will look like once it is finished. This is why it is important that police officers are not made to feel as if they let down their victims (Hall 2021) if the systems that they are required to operate within are not setup for purpose. It follows that improving cybercrime reporting in Scotland will entail a discussion about the social components of reporting crimes and how to engage those for the benefit of accuracy and robustness.

In connection to problems with reporting and recording cybercrime, Horgan, S. et al. 2021 suggested harnessing the power of community links with the police. I can only add that the insider's view of the community police might be useful in filling many of the holes that are contained within cybercrime reports as the complaint taker may be less likely to make assumptions about the complainant concerning issues such as demographics and the like. This argument is in line with the favourable view that Wooff 2015 and Wooff 2016 have towards community policing as mentioned in 2.1 Police Scotland.

Subsequently, I supplied several relevant pointers for adjusting the people's side of improving cybercrime reporting in Scotland. I discussed how Forouzan, H., Jahankhani, H., and McCarthy, J. 2018 and Schreuders, Z.C. et al. 2020 found that a one-size-fits all online cybercrime training by the London Met was ineffective. In fact, over 33% of the police force did not even hear about it. Illuminatingly, the usefulness of the social element in cybercrime training was corroborated by Cockroft, T. et al. 2021 who found that face-to-face training delivery was more effective in preparing the police for responding to cybercrime. Hence, if cybercrime reporting is to improve in Scotland, then it is preferable that the training of police officers is face-to-face and interactive.

I believe that online cybercrime training perpetuates the problem it is meant to be solving by playing into the narrative of cybercrime being something that happens on a computer. I argue that the computer is just a medium, cybercrime can happen between people with personalities and life stories. The successful improving of cybercrime reporting will also require an ability to reclaim this social landscape from a purely technical interpretation. Much like in my proposed taxonomy for cybercrime reporting (i.e., H2H, H2M and M2M), actual cybercrime reflects a similar pattern. Whilst some crimes are carried out from human-to-human, such as when a malicious ex-partner goes on a shopping spree via an Amazon account of their ex, others can be human-to-machine, such as when a hacker attacks a computer with ransomware. Lastly, in a case of machine-to-machine, malware that incorporates computers into botnets is criminally making unauthorised use of computers, but the computers' authorised users may not know that this has happened or be directly impacted.

Finally, I have considered the research by Bossler, A.M. et al. 2020 who argued that cybercrime reporting could be improved with a set of best practice procedures and guidelines that

would be rolled out across the board. To the contrary, this was disputed by Johnson, D. et al. 2020 who wrote that the decentralisation of the English force would make this difficult. Importantly, this is no longer applies to Scotland, which has undergone the centralisation of the eight regional divisions under one Police Scotland. In a research by Murray and Harkin 2017 this was lauded as a step towards more effective scrutiny and higher accountability of police staff as I have said in 2.1 Police Scotland. Whilst I do believe that cybercrime reporting is a distinctly social phenomenon, I also think that a set of democratically negotiated best practice procedures would improve the situation across Scotland. This is a residual benefit from the nationalists' reforms that has yet to be harnessed.

7.2 What is known about cybercrime victims in the UK to date?

I have used the systematic approach to reveal information about the victims' profiles and experiences. Starting with a stark piece from 2008, Hunter, P. 2008 reported on a case study where a prominent MP was victimised by cybercrime, which prompted him to prioritise the problem as a part of public discourse whilst also critiquing the absence of a dedicated cybercrime reporting centre. As I wrote in 2.1 Police Scotland, the cybercrime reporting centre has been established as Action Fraud, however in 2019 Scotland chose to discontinue its membership with the centre due to receiving an overpriced and poor service (Kenny MacDonald 2019). Leaving AF was a wise strategic move on behalf of Scotland which will enable it to set-up systems (both social and technological) that will improve cybercrime reporting whilst respecting its unique cultural landscape.

Next, I have discussed the research by Bohme, R. 2013 who discussed the quantitative aspects of victimisation in terms of how much victims could sue for in court. The research by Bohme, R. 2013 argued that victims' distress is difficult to account for in legal terms. I have argued that without considering the victims distress and their phenomenology it will be difficult to construct improved cybercrime reporting systems in Scotland. I find it hard to imagine how one could follow through with the Police Scotland's Cyber Strategy 2020 and focus on "vulnerability" whilst not seeing its connection to increased distress (Police Scotland and Scottish Police Authority 2020).

Then I have shifted the discussion to the Routine Activity Theory (RAT) as a framework that explains the probability of online victimisation based on insecure online behaviours. Take the following two examples. Firstly, the article by Nasi et al. 2015 was used to shed light on what traits make people more vulnerable to cybercrime. It was found that being male, young, migrant, urban, not living with parents, unemployed with more social life online vs. offline were all predictors of becoming a victim of cybercrime. Secondly, it was found that during the pandemic people spent more time online, which increased their risk of victimisation albeit decreasing the risk of being a victim of a violent crime in the street (Buil-Gil, D., Miro-Llinares, F., et al. 2021).

Subsequently, I was able to garner that victims of cybercrime often engage in sensation seeking behaviours with their cognition being less likely to suppress incorrect information when they come across it in phishing emails (Jones, H.S. et al. 2019). This research tied into findings by Button, M. and Whittaker, J. 2021 where the authors found that victims of cybercrime experienced a range of psychosomatic symptoms ranging from physiological deterioration all the way to psychiatric deterioration thereby suggesting that victimisation also increases vulnerability to serious illnesses.

Lastly, the systematic search revealed age to be a predictor of vulnerability towards cybercrime with older people being more likely to be victimised by economic scams (Correia, S.G. 2020) and younger people who were lonely during the COVID-19 pandemic were likelier to

fall prey to romance scams (Buil-Gil, D. and Zeng, Y. 2021).

Conclusively, these findings should be linked in with the Police Scotland's Cyber Strategy 2020 as they all feed into the concept of "vulnerability" and as such are instrumental in understanding the victims of cybercrime (Police Scotland and Scottish Police Authority 2020).

An important theme from the 2 Background that stretches throughout this research is that of responsibilisation which is closely connected to cybercrime victims. As I have stated before, due to there being an insufficiency of research on cybercrime victims from the United Kingdom, I have chosen to extrapolate findings from the West onto the UK and from the UK onto Scotland. For example, Bohme and Moore 2012 found that people who have been victimised by cybercrime or received information about its threat depressed their online activity. This points to the unintended effects of responsibilisation as Renaud, Flowerday, et al. 2018 and Renaud, Orgeron, et al. 2020 found that Western governments merely impart cautionary information onto their citizens but disengage thereafter. I would argue that people's decrease in activity points to feeling alone, vulnerable and unprotected whilst online, which is why they decrease their activity rather than seek protection. It is crucial to create such cybercrime reporting mechanisms that citizens will feel emboldened to come out of anonymity and share what has happened to them with the police without a fear of being judged.

Also, ER Leukfeldt, Notte, and Malsch 2020 found that cybercrime victims have a real need to receive recognition from society and the police for the ordeal that they have been through. This includes receiving regular updates regarding the investigative process. The notion of recognition is something that I connect to responsibilisation because it suggests that recognition is still not a given. Rather, cybercrime victims are made to feel responsible for what has happened to them, which is why they do not receive the recognition that they deserve. Improved cybercrime reporting in Scotland is inevitably connected to helping victims restore their dignity and turn their adversity into a story of resilience.

Ironically, the very governments that responsibilise their citizens may be reluctant to admit that it is fake government websites that are used to target victims. This is important because on the one hand all Western governments enforce the law and expect citizens to abide by it, but if citizens are tricked by a scammer, then they run the risk of being blamed. Take for example the discussed study by Lacey, Salmon, and Glancy 2015 who found that fraudsters impersonate the post office to force people to open phishing links purporting to provide extra information about a delivery. People should not be made to feel responsible for complying with the request. It is a similar scenario as if a criminal was to impersonate a post man in order to commit a burglary. In response, the victim would be blamed for not scrutinising their ID card in more detail via the key hole before they opened the door. The majority would not blame the burglary victim, so why do we do we blame cybercrime victims?

As I have shown throughout, the cybercriminals do not stop there. Indeed, in the USA they readily impersonate the IRS or the FBI in order to get international students with minimal knowledge of national laws to give up their details under the threat of criminalisation (Bidgoli and Grossklags 2017). This is another example of why the governments cannot bypass their responsibility to protect the innocent victims. The predatory behaviours of scammers will use the fear of the law against citizens if they know that their victims will be blamed for giving in. In order to improve cybercrime reporting in Scotland, people need to receive this information in places and from people that they know they can trust as the internet can be full of deception. This is why the social element of coming together and talking about these challenges in a community venue with the police can be so helpful. The citizens will know that the police officers are who they claim to be as they will have many years worth of memories with them being genuine police.

The ineffectiveness of responsibilisation strategies can also be seen in the research by C.

Cross and Kelly 2016 which used two case studies that of Ruth and Hazel. They illustrate that whilst people receive information about how to protect themselves against cybercrime, they fail to do so if their emotions are invested in a pseudo-relationship or a pseudo-enterprise. Moreover, these single cases were backed up by community research where most people perceived the risk of cybercrime as being low whilst reporting widespread victimisation (Cross et al. 2021), which suggests that the problem is societal rather than that of Ruth and Hazel. This is evidence that the Western governments' approach to merely educating citizens about cybercrime is simply an insufficient.

It is ironic that governments which responsibilise their citizens invest finances into awareness raising campaigns on how to avoid cybercrime but do not invest in raising awareness of how to report crime and what to expect from authorities. This was illustrated by C. Cross 2018 which described that people had unrealistic expectations from the police and were often moved on from one agency onto the other. If I were to conduct an awareness raising campaign as a part of this research, then I would focus it on who citizens should contact to report cybercrime and what they can expect thereafter.

7.3 What is known about cybercrime reporting to date?

Responsibilisation correlates negatively with people's desire to report cybercrime. As can be seen in studies by Bidgoli, Knijnenburg, and Grossklags 2016 and S. van de Weijer, R. Leukfeldt, and Van der Zee 2020b people readily associate private companies with providing a resolution. Likewise, Jhaveri et al. 2017 found that government's unwillingness to tackle cybercrime has brought together business rivals to form security coalitions with the aim of protecting businesses.

It is also important to consider findings from countries where responsibilisation is likely to be lower and control of the state higher. The research from Saudi Arabia by Alzubaidi 2021 was interesting because whilst most of his participants did not report cybercrime to anyone, from those that did, most consulted a friend and then the government's e-portal. This raises interesting questions about trust towards governments in countries with distinct values. Citizens in the West are more inclined to report cybercrime to those agencies that aspire to sell them as much products as possible rather than the government to which they are paying taxes. This is a case of responsibilisation, which needs to be reversed. To the contrary, citizens in Saudi Arabia are slightly likelier to report to their government. The reasons for this distinction warrant further, ideally cross-cultural, research.

A key finding for my research comes from C. Cross 2020a, which debated the challenges of jurisdiction in cybercrime reporting. She also explained the ACORN project, Australia's version of Action Fraud. The similarities between ACORN and AF are striking. Just like in the case of AF, ACORN was criticised for lack of transparency and poor customer service and poor incident recording. This rings all too familiar with the piece from in 2.2 Crime numeration by Maltz 1977 who wrote about the problems with crime recording centres in the 1930s. It also corresponds closely to the strategic thinking behind Police Scotland's desire to separate from AF due to receiving a poor service (Kenny MacDonald 2019). As I have argued before, I think that one reason these systems have problems is because they discount the social element of crime. I believe that if crime recordings engaged the person more holistically by including their emotions and so forth, then people would be more encouraged to provide accurate reports.

At least of the surface, the reporting centre IC3 in the USA (Heinonen, Holt, and Wilson 2012) fares better than both ACORN in Australia and AF in the United Kingdom. As stated by Bidgoli and Grossklags 2016 its main advantage is that it provides awareness raising campaigns, but its main weakness is that it operates on a federal level whereas most cybercrime

is localised. Out of three reporting centres discussed here (AF, ACORN, and IC3), I am most sympathetic to the IC3 because of its effort to interact with the citizens, which are most likely to need it rather than just dispersing information in the hope it finds its way to the correct receivers. In this respect, I see the IC3 as making very explicit steps to increase the social dimension in cybercrime reporting which I have spoken about.

I have also presented several studies that could be used to inspire a cybercrime reporting system in Scotland, which I summarise as follows. Firstly, cybercrime reporting systems must increase user cyber-awareness, provide user autonomy and avoid cognitive overload (Bidgoli, Knijnenburg, Grossklags, and Wardman 2019). Secondly, to make cybercrime reporting more objective, systems must supply people with clear criteria regarding what information is sought (Baror, Ikuesan, and Venter 2020). The second example might be helpful for those that prefer to communicate with a system rather than a police officer. However, people who are already intimidated by technology will miss the social element I have referred to before.

8 CONCLUSION

I conducted a systematic review to explore questions around economic cybercrime. I have contextualised current state of the art knowledge on the subject within the changing political landscape of Scottish policing. In this respect I have sought to connect much of my research to the notion of vulnerability to cybercrime. I have also looked at how crime numeration has evolved over time and that, despite unquestionable technological advancements, the problems with reporting remain unchanged for nearly 100 years. This lead me to postulate that cybercrime reporting needs to be treated as a social phenomenon rather than a strictly numerical one. A common thread that stretched throughout the literature was that of responsibilisation and its damaging effects on cybercrime reporting. I explained that the paradigm needs to change and the state has to take ownership of policing cybercrime. Moreover, I have supplied an original taxonomy for classifying cybercrime, which could aid researchers in searching through the literature if it became widely adopted. Moreover, this taxonomy will be effective in understanding the literature on cybercrime reporting, which could aid the development of interventions.

REFERENCES

Abdulai, M.A. (2020). "Examining the effect of victimization experience on fear of cybercrime: University students' experience of credit/debit card fraud". In: *International Journal of Cyber Criminology* 14.1, pp. 157–174.

Akdemir, N. and Lawless, C.J. (2020). "Exploring the human factor in cyber-enabled and cyberdependent crime victimisation: a lifestyle routine activities approach". In: *Human Factor in Cybercrime Victimisation* 30.6, pp. 1665–1687.

Alzubaidi, A. (2021). "Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia". In: *Heliyon* 7.1.

Bana, A. and Hertzberg, D. (2015). "Data Security and the Legal Profession: Risks, Unique Challenges and Practical Considerations". In: *Business International Law* 16.3, pp. 247–264.

Baror, S.O., R.A. Ikuesan, and H.S. Venter (2020). "A defined digital forensic criteria for cybercrime reporting". In: Proceedings of the 15th International Conference on Cyber Warfare and Security, ICCWS 2020, pp. 617–626.

Bennett, RR and RB Wiegand (Feb. 1994). "OBSERVATIONS ON CRIME REPORTING IN A DEVELOPING-NATION". In: *CRIMINOLOGY* 32.1, pp. 135–148. ISSN: 0011-1384.

Bidgoli, M. and J. Grossklags (2016). "End user cybercrime reporting: What we know and what we can do to improve it". In: 2016 IEEE International Conference on Cybercrime and Computer Forensic, ICCCF 2016.

— (2017). "'Hello. This is the IRS calling.': A case study on scams, extortion, impersonation, and phone spoofing". In: eCrime Researchers Summit, eCrime, pp. 57–69.

Bidgoli, M., B.P. Knijnenburg, and J. Grossklags (2016). "When cybercrimes strike undergraduates". In: eCrime Researchers Summit, eCrime. Vol. 2016-June, pp. 42–51.

Bidgoli, M., B.P. Knijnenburg, J. Grossklags, and B. Wardman (2019). "Report Now. Report Effectively. Conceptualizing the Industry Practice for Cybercrime Reporting". In: eCrime Researchers Summit, eCrime. Vol. 2019-November.

Bohme, R. and T. Moore (2012). "How do consumers react to cybercrime?" In: eCrime Researchers Summit, eCrime.

Bohme, R. (2013). *The Economics of Information Security and Privacy*. Springer Heidelberg New York Dordrecht London: Springer. ISBN: 978-3-642-39498-0.

Bossler, A.M., Holt, T.J., Cross, C., and Burruss, G.W. (2020). "Policing fraud in England and Wales: examining constables' and sergeants' online fraud preparedness". In: *Security Journal* 33, pp. 311–328.

Buil-Gil, David and Patricia Saldana-Taboada (2021). "Offending Concentration on the Internet: An Exploratory Analysis of Bitcoin-related Cybercrime". In: *DEVIANT BEHAVIOR*. ISSN: 0163-9625.

Buil-Gil, D., Miro-Llinares, F., Moneva, A., Kemp, S., and Diaz-Castano, N. (2021). "Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK". In: *EUROPEAN SOCIETIES* 23 (S1), S47–S49.

Buil-Gil, D. and Zeng, Y. (May 10, 2021). "Meeting you was a fake: investigating the increase in romance fraud during COVID-19". In: *Journal of Financial Crime*. ISSN: 1359-0790.

Button, M., Blackbourn, D., Sugiura, L., Shepherd, D., Kapend, R., and Wang, V. (2021). "From feeling like rape to a minor inconvenience: Victims' accounts of the impact of computer misuse crime in the United Kingdom". In: *Telematics and Informatics* 64, pp. 1–11.

Button, M. and Whittaker, J. (2021). "Exploring the voluntary response to cyber-fraud: From vigilantism to responsibilisation". In: *International Journal of Law, Crime and Justice* 66.

Carpineto, Claudio and Giovanni Romano (Apr. 2020). "An Experimental Study of Automatic Detection and Measurement of Counterfeit in Brand Search Results". In: *ACM TRANSACTIONS ON THE WEB* 14.2. ISSN: 1559-1131.

CFS (2018). "Number of cybercrime victims falls". In: *Computer Fraud & Security*, p. 20.

Cockroft, T., Shan-A-Khuda, M., Schreuders, Z.C., and Trevorrow, P. (Mar. 2021). "Police Cybercrime Training: Perceptions, Pedagogy, and Policy". In: *POLICING-A JOURNAL OF POLICY AND PRACTICE* 15.1, pp. 15–33.

Collier, B., Thomas, D.R., Clayton, R., Hutchings, A., and Chua, Y.-T. (Jan. 25, 2021). "Influence, infrastructure, and recentering cybercrime policing: evaluating emerging approaches to online law enforcement through a market of cybercrime services". In: *Policing & Society An International Journal of Research and Policy*.

Collier, B., Thomas, D.R., Clayton, R., and Hutchings, A. (Oct. 21, 2019). "Booting the Booters: Evaluating the Effects of Police Interventions in the Market for Denial-of-Service Attacks". In: *Internet Measurement Conference (IMC '19)*. IMC'19. Amsterdam, New York, p. 15.

Connolly, A.Y. and Borrison, H. (2020). *Your Money or Your Business*.

Connolly, A.Y., Wall, D.S., Lang, M., and Oddson, B. (2020). "An empirical study of ransomware attacks on organizations: an assessment of severity and salient factors affecting vulnerability". In: *Journal of Cybersecurity*, pp. 1–18.

Correia, S.G. (2019). "Responding to victimisation in a digital world: a case study of fraud and computer misuse reported in Wales". In: *Crime Science* 8.4, pp. 1–12.

— (2020). "Patterns of online repeat victimisation and implications for crime prevention". In: *2020 APWG Symposium on Electronic Crime Research (eCrime)*. Boston, MA, USA: IEEE.

Cross, C, T Holt, A Powell, and M Wilson (Aug. 2021). "Responding to cybercrime: Results of a comparison between community members and police personnel". In: *TRENDS AND ISSUES IN CRIME AND CRIMINAL JUSTICE* 635, pp. 1–20. ISSN: 1836-2206.

Cross, C. (2018). "Expectations vs reality: Responding to online fraud across the fraud justice network". In: *International Journal of Law, Crime and Justice* 55, pp. 1–12.

— (2020a). "'Oh we can't actually do anything about that': The problematic nature of jurisdiction for online fraud victims". In: *Criminology and Criminal Justice* 20.3, pp. 358–375.

— (2020b). "Reflections on the reporting of fraud in Australia". In: *Policing* 43.1, pp. 49–61.

Cross, C. and M. Kelly (2016). "The problem of "white noise": Examining current prevention approaches to online fraud". In: *Journal of Financial Crime* 23.4, pp. 806–818.

Cross, C. (May 5, 2019). "Is online fraud just fraud? Examining the efficacy of the digital divide". In: *Journal of Criminological Research, Policy and Practice* 5.2, pp. 120–131.

— (2021). "Theorising the impact of COVID-19 on the fraud victimisation of older persons". In: *The Journal of Adult Protection* 23.2, pp. 98–109. ISSN: 1466-8203.

Das, Ankur, Janmenjoy Nayak, Bighnaraj Naik, and Uttam Ghosh (May 2021). "Generation of overlapping clusters constructing suitable graph for crime report analysis". In: *FUTURE GENERATION COMPUTER SYSTEMS-THE INTERNATIONAL JOURNAL OF ESCIENCE* 118, pp. 339–357. ISSN: 0167-739X.

Doig, A. (2018). "Implementing national policing agendas and strategies for fraud at local level". In: *Journal of Financial Crime* 25.4, pp. 984–996.

Donegan, M. (2019). "Crime script for mandate fraud". In: *Journal of Money Laundering* 22.4, pp. 770–781.

Dyson, I. (Mar. 12, 2019). *Chief Constables/PCCs*.

Enang, Iniobong, Jennifer Murray, Nadine Dougall, Andrew Wooff, Inga Heyman, and Elizabeth Aston (2019). "Defining and Assessing vulnerability within law enforcement and public health organisations: A scoping review." In: *Health and Justice* 7.2. Publisher: BMC.

Fisher, Jonathan (Jan. 1, 2008). "The UK's faster payment project: avoiding a bonanza for cybercrime fraudsters". In: *Journal of Financial Crime* 15.2, pp. 155–164. ISSN: 1359-0790. (Visited on Oct. 28, 2021).

Forouzan, H., Jahankhani, H., and McCarthy, J. (2018). "An examination into the level of training, education and awareness among frontline police officers in tackling cybercrime within the metropolitan police service". In: *Advanced Sciences and Technologies for Security Applications*, pp. 307–323.

Hadlington, Lee, Karen Lumsden, Alexandra Black, and Fenia Ferra (Mar. 2021). "A Qualitative Exploration of Police Officers' Experiences, Challenges, and Perceptions of Cybercrime". In: *POLICING-A JOURNAL OF POLICY AND PRACTICE* 15.1, pp. 34–43. ISSN: 1752-4512.

Hall, Matthew (Mar. 3, 2021). "Counting crime: Discounting victims?" In: *International Review of Victimology*. Publisher: SAGE Publications Ltd, p. 0269758021995909. ISSN: 0269-7580. (Visited on Dec. 17, 2021).

Heinonen, J.A., T.J. Holt, and J.M. Wilson (2012). "Product Counterfeits in the Online Environment: An Empirical Assessment of Victimization and Reporting Characteristics". In: *International Criminal Justice Review* 22.4, pp. 353–371.

Henry, A, A Malik, and A Aydin-Aitchison (Sept. 2019). "Local governance in the new Police Scotland: Renegotiating power, recognition and responsiveness". In: *EUROPEAN JOURNAL OF CRIMINOLOGY* 16.5, pp. 573–591. ISSN: 1477-3708.

Horgan, Shane (2021). *The reality of 'cyber security awareness': findings and policy implications for Scotland*. Series: Scottish Justice Fellowship Briefing Papers, pp. 1–12.

Horgan, Shane and Ben Collier (2016). "Barriers to a Cyberaware Scotland". In: *Scottish Justice Matters* 4.3. Publisher: Scottish Consortium on Crime and Criminal Justice (SCCCJ), pp. 19–20. ISSN: 2052-7950.

Horgan, S., Collier, B., Jones, R., and Shepherd, L. (2021). "Re-territorialising the policing of cybercrime in the post-COVID-19 era: towards a new vision of local democratic cyber policing". In: *Journal of Criminal Psychology* 11.3, pp. 222–239. ISSN: 2009-3829.

Huaman, N., B. von Skarczinski, C. Stransky, D. Wermke, Y. Acar, A. Dreißigacker, and S. Fahl (2021). "A large-scale interview study on information security in and attacks against small and medium-sized enterprises". In: Proceedings of the 30th USENIX Security Symposium, pp. 1235–1252.

Hunter, P. (2008). "UK shadow home secretary victim of online card fraud". In: *Computer Fraud & Security*, p. 4.

Hunton, P. (2011). "A rigorous approach to formalising the technical investigation stages of cybercrime and criminality within a UK law enforcement environment". In: *Digital Investigation* 7.3, pp. 105–113.

— (2012). "Managing the technical resource capability of cybercrime investigation: A UK law enforcement perspective". In: *Public Money and Management* 32.3, pp. 225–232.

Hutchings, A. and Collier, B. (June 17, 2019). "Inside out: Characterising cybercrimes committed inside and outside the workplace". In: *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. Stockholm, Sweden: IEEE. ISBN: 978-1-72813-026-2.

Hutchings, A. and Pastrana, S. (2019). "Understanding eWhoring". In: *2019 4TH IEEE EUROPEAN SYMPOSIUM ON SECURITY AND PRIVACY (EUROS&P)*. Stockholm, Sweden: IEEE, pp. 201–214.

Jhaveri, M.H., O. Cetin, C. Gañán, T. Moore, and M. Van Eeten (2017). "Abuse reporting and the fight against cybercrime". In: *ACM Computing Surveys* 49.4.

Johnson, D., Faulkner, E., Meredith, G., and Wilson, T.J. (2020). "Police Functional Adaptation to the Digital or Post Digital Age: Discussions with Cybercrime Experts". In: *Journal of Criminal Law* 84.5, pp. 427–450. ISSN: 0022-0183.

Jones, T, T Newburn, and DJ Smith (1996). "Policing and the idea of democracy". In: *BRITISH JOURNAL OF CRIMINOLOGY* 36.2, pp. 182–198. ISSN: 0007-0955.

Jones, H.S., Towse, J.N., Race, N., and Harrison, T. (2019). "Email fraud: The search for psychological predictors of susceptibility". In: *PLOS ONE* 14.1, e0209684.

Karagiannopoulos, V., Sugiura, L., and Kirby, A. (Oct. 2019). *The Portsmouth Cybercrime Awareness Clinic Project: Key Findings and Recommendations*. University of Portsmouth. 26 pp.

Kemp, Steven, David Buil-Gil, Asier Moneva, Fernando Miro-Llinares, and Nacho Diaz-Castano (2021). "Empty Streets, Busy Internet: A Time-Series Analysis of Cybercrime and Fraud Trends During COVID-19". In: *JOURNAL OF CONTEMPORARY CRIMINAL JUSTICE*. ISSN: 1043-9862.

Kenny MacDonald (June 12, 2019). *Action Fraud*. V3-A0718. SPC, Tulliallan.

Kimpe, L. de, M. Walrave, T. Snaphaan, L. Pauwels, W. Hardyns, and K. Ponnet (2021). "Research Note: An investigation of cybercrime victims' reporting behavior". In: *European Journal of Crime, Criminal Law and Criminal Justice* 29.1, pp. 66–78.

Lacey, D., P. Salmon, and P. Glancy (2015). "Taking the Bait: A Systems Analysis of Phishing Attacks". In: *Procedia Manufacturing* 3, pp. 1109–1116.

Lavorgna, A. (2019). “Cyber-organised crime. A case of moral panic?” In: *Trends in Organized Crime* 22, pp. 357–374.

Leukfeldt, ER, RJ Notte, and M Malsch (Jan. 2, 2020). “Exploring the Needs of Victims of Cyber-dependent and Cyber-enabled Crimes”. In: *VICTIMS & OFFENDERS* 15.1, pp. 60–77. ISSN: 1556-4886.

Leukfeldt, E.R., Kleemans, E.R., and Stol, W.P. (2017). “Origin, growth and criminal capabilities of cybercriminal networks. An international empirical analysis”. In: *Crime, Law and Social Change* 67, pp. 39–53.

Leukfeldt, E.R., Lavorgna, A., and Kleemans, E.R. (2017). “Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime”. In: *European Journal on Criminal Policy and Research* 23.33, pp. 287–300.

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”. In: *Crime, Law and Social Change* 67, pp. 3–20.

Levi, M., Doig, A., Gundur, R., Wall, D., and Williams, M. (Feb. 1, 2017). “Cyberfraud and the Implications for Effective Risk-Based Responses: Themes from UK Research”. In: *Crime, Law and Social Change* 67.1, pp. 77–96.

Levi, M. and Smith, R.G. (Aug. 6, 2021). “Fraud and pandemics”. In: *Journal of Financial Crime*. ISSN: 1359-0790.

Levi, M. and M.L Williams (2013). “Multi-agency partnerships in cybercrime reduction: Mapping the UK information assurance network cooperation space”. In: *Information Management & Computer Security* 21.5, pp. 420–443.

Lord, J. (June 2016). “Fifty Shades of Fraud”. In: *Computer Fraud & Security* Volume 2016.6, pp. 14–16.

Loveday, B. (2018). “The Shape of Things to Come. Reflections on the potential implications of the 2016 Office of National Statistics Crime Survey for the police service of England and Wales”. In: *POLICING-A JOURNAL OF POLICY AND PRACTICE* 12.4, pp. 398–409.

Lyle, A. (2016). “Chapter 17 Legal Considerations for Using Open Source Intelligence in the Context of Cybercrime and Cyberterrorism”. In: *Open Source Intelligence Investigation. Advanced Sciences and Technologies for Security Applications*. Springer International Publishing AG 2016, pp. 277–294. ISBN: 978-3-319-47671-1.

Mackey, T.K., J. Li, V. Purushothaman, M. Nali, N. Shah, C. Bardier, M. Cai, and B. Liang (2020). “Big data, natural language processing, and deep learning to detect and characterize illicit COVID-19 product sales: Infoveillance study on Twitter and Instagram”. In: *JMIR Public Health and Surveillance* 6.3.

Maltz, Michael D. (Jan. 1, 1977). “Crime Statistics: A Historical Perspective”. In: *Crime & Delinquency* 23.1. Publisher: SAGE Publications Inc, pp. 32–40. ISSN: 0011-1287. (Visited on Dec. 17, 2021).

Mapimele, F. and B. Mangoale (2019). “The cybercrime combating platform”. In: 14th International Conference on Cyber Warfare and Security, ICCWS 2019, pp. 237–242.

Monteith, S., M. Bauer, M. Alda, J. Geddes, P.C. Whybrow, and T. Glenn (2021). “Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry”. In: *Current Psychiatry Reports* 23.4.

Murray, K and D Harkin (July 2017). “POLICING IN COOL AND HOT CLIMATES: LEGITIMACY, POWER AND THE RISE AND FALL OF MASS STOP AND SEARCH IN SCOTLAND”. In: *BRITISH JOURNAL OF CRIMINOLOGY* 57.4, pp. 885–905. ISSN: 0007-0955.

Nappa, A., M.Z. Rafique, and J. Caballero (2015). “The MALICIA dataset: identification and analysis of drive-by download operations”. In: *International Journal of Information Security* 14.1, pp. 15–33.

Nasi, M., Oksanen, A., Keipi, T., and Rasanen, P. (2015). “Cybercrime victimization among young people: a multi-nation study”. In: *Journal of Scandinavian Studies in Criminology and Crime Prevention* 16.2, pp. 203–210.

Pastrana, S., Hutchings, A., Thomas, D.R., and J. Tapiador (Oct. 21, 2019). “Measuring eWhoring”. In: *IMC ’19: Proceedings of the Internet Measurement Conference*, pp. 463–477.

Pickerting, C., Grignon, J., R. Steven, D. Guitart, and Byrne, J. (2015). "Publishing not perishing: how research students transition from novice to knowledgeable using systematic quantitative literature reviews". In: *Studies in Higher Education* 40.10, pp. 1756–1769.

Police Scotland and Scottish Police Authority (2020). *Cyber Strategy 2020*. (Visited on Oct. 8, 2021).

Popham, J., M. McCluskey, M. Ouellet, and O. Gallupe (2020). "Exploring police-reported cybercrime in Canada: variation and correlates". In: *Policing* 43.1, pp. 35–48.

Prislan, Kaja, Igor Bernik, Gorazd Mesko, Rok Hacin, Blaz Markelj, Simon L. R. Vrhovec, and ACM (2019). "Cybercrime victimization and seeking help: A survey of students in Slovenia". In: THIRD CENTRAL EUROPEAN CYBERSECURITY CONFERENCE (CECC 2019). ISBN: 978-1-4503-7296-1.

Reep-van den Bergh, CMM and M Junger (Dec. 2018). "Victims of cybercrime in Europe: a review of victim surveys". In: *CRIME SCIENCE* 7.1. ISSN: 2193-7680.

Renaud, K, S Flowerday, M Warkentin, P Cockshott, and C Orgeron (Sept. 2018). "Is the responsibilization of the cyber security risk reasonable and judicious?" In: *COMPUTERS & SECURITY* 78, pp. 198–211. ISSN: 0167-4048.

Renaud, K, C Orgeron, M Warkentin, and PE French (July 2020). "Cyber Security Responsibilization: An Evaluation of the Intervention Approaches Adopted by the Five Eyes Countries and China". In: *PUBLIC ADMINISTRATION REVIEW* 80.4, pp. 577–589. ISSN: 0033-3352.

Sampson, F. (2014). "Cyberspace: The new frontier for policing?" In: *Cyber Crime and Cyber Terrorism Investigator's Handbook*, pp. 1–10.

Schreuders, Z.C., Cockroft, T., Elliott, J., Butterfield, E., Soobhany, A.R., and Shan-A-Khuda, M. (2020). "Needs Assessment of Cybercrime and Digital Evidence in a UK Police Force". In: *International Journal of Cyber Criminology* 14.1, pp. 316–340. ISSN: 09742891.

Shan-A-Khuda, M. and Schreuders, Z.C. (Dec. 2019). "Understanding Cybercrime Victimisation: Modelling the Local Area Variations in Routinely Collected Cybercrime Police Data Using Latent Class Analysis". In: *International Journal of Cyber Criminology* 13.2, pp. 493–510. ISSN: 09742891.

Sheikhalishahi, Mina, Andrea Saracino, Fabio Martinelli, Antonio La Marra, Mohammed Mejri, and Nadia Tawbi (Oct. 2020). "Digital Waste Disposal: an automated framework for analysis of spam emails". In: *INTERNATIONAL JOURNAL OF INFORMATION SECURITY* 19.5, pp. 499–522. ISSN: 1615-5262.

Singh, Shweta, M. P. Singh, Ramprakash Pandey, and IEEE (2020). "Phishing Detection from URLs Using Deep Learning Approach". In: PROCEEDINGS OF THE 2020 5TH INTERNATIONAL CONFERENCE ON COMPUTING, COMMUNICATION AND SECURITY (ICCCS-2020). ISBN: 978-1-72819-180-5.

Skidmore, M., J. Goldstraw-White, and M. Gill (July 3, 2020). "Understanding the Police Response to Fraud: The Challenges in Configuring a Response to a Low-Priority Crime on the Rise". In: *Public Money & Management* 40.5, pp. 369–379. (Visited on Oct. 8, 2021).

Sommer, P. (2017). "The future for the policing of cybercrime". In: *Crime and Deviance in Cyberspace*, pp. 541–546. ISBN: 978-1-315-09532-5.

Stevens, T. and O'Brein, K. (2019). "Brexit and Cyber Security". In: *The RUSI Journal* 164.3, pp. 22–30. ISSN: 1744-0378.

Tarling, R and K Morris (May 2010). "Reporting Crime to the Police". In: *BRITISH JOURNAL OF CRIMINOLOGY* 50.3, pp. 474–490. ISSN: 0007-0955.

Van De Weijer, S.G.A. and E.R. Leukfeldt (2017). "Big Five Personality Traits of Cybercrime Victims". In: *Cyberpsychology, Behavior, and Social Networking* 20.7, pp. 407–412.

Waldrop, M.M. (May 12, 2016). "The Human Side of CYBERCRIME". In: *NATURE* 533, pp. 164–167.

Wall, D.S. (2013). "Policing identity crimes". In: *Policing and Society* 23.4, pp. 437–460. (Visited on Oct. 28, 2021).

Weijer, S. van de, R. Leukfeldt, and S. Van der Zee (2020a). "Reporting cybercrime victimization: determinants, motives, and previous experiences". In: *Policing* 43.1, pp. 17–34.

— (2020b). "Reporting cybercrime victimization: determinants, motives, and previous experiences". In: *Policing* 43.1, pp. 17–34.

Weijer, S.G.A. van de, R. Leukfeldt, and W. Bernasco (2019). "Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking". In: *European Journal of Criminology* 16.4, pp. 486–508.

Whitty, M.T. (Nov. 2, 2018). "Do You Love Me? Psychological Characteristics of Romance Scam Victims". In: *Cyberpsychology, Behavior, And Social Networking* 21.2, pp. 105–109.

Wilson-Kovacs, D. (2021). "Digital media investigators: challenges and opportunities in the use of digital forensics in police investigations in England and Wales". In: *Policing: An International Journal* 44.4, pp. 669–682. ISSN: 1363-951X.

Winder, D. and I. Trump (2015). "Mitigating Cybercrime Through Meaningful Measurement Methodologies". In: *EDPACS* 52.5, pp. 1–8.

Wirth, A. (June 2018). "The Times They Are a-Changin': Part Two". In: *Biomedical Instrumentation & Technology*. Included in review., pp. 236–240.

Wooff, Andrew (2015). "Relationships and responses: Policing anti-social behaviour in rural Scotland". In: *Journal of Rural Studies* 39. Publisher: Elsevier, pp. 287–295. ISSN: 0743-0167.

— (2016). "'Soft' Policing in Rural Scotland". In: *Policing* 11.2. Publisher: Oxford University Press, pp. 123–131. ISSN: 1752-4512.

Yadav, H., S. Gautam, A. Rana, J. Bhardwaj, and N. Tyagi (2021). *Various Types of Cybercrime and Its Affected Area*. Vol. 164. Lecture Notes in Networks and Systems. 305 pp.

It takes a high profile victim to bring attention to the adversity affecting the masses. Specifically, in 2008, the shadow home secretary David Davis criticised the UK government for being ineffective in tackling cybercrime after he became a victim of it himself. The situation in 2008 bears some resemblance to the present situation. Then, cybercrime reporting was also a problem with research critiquing the lack of a dedicated centre for tackling cybercrime and the police's tendency to investigate only high value crimes. Things have since changed. The centre of cybercrime reporting was established under the name Action Fraud. However, the problem with investigating only high value offences persists. The difference being that prior authors complained that only offences above £500 are investigated by the police. In 2019 that figure has increased to offences above £100 000. The rhetorical question withstands the test of time: "Who are the current cybercrime reporting mechanisms really serving if not those that can afford to police themselves?"

- Juraj Sikra

Recipient of the national award SICSA Cyber Security Research Theme: Online Cyber Security PhD Student Forum 2021

- SICSA

DOI: https://doi.org/10.17868/79836