



UK & CANADA CYBERCRIME POLICIES -DO THEY PROTECT VULNERABLE PEOPLE?

A Dissertation submitted for the
Criminal Justice and Policing (MA) 2021

Submitted 12/03/2021.

Student: Elis Edward Hilliard Park

Student Number: P149475

Supervisors: Jane Thomas & Wynne Jones

Declaration/Statements

This work has not previously been accepted in substance for any degree and is not being concurrently submitted in candidature for any degree.

Signed Elis Edward Hillard Park (candidate)

Date: 12/03/2021

STATEMENT 1

This thesis is the result of my own investigations, except where otherwise stated. Where correction services have been used the extent and nature of the correction is clearly marked in a footnote(s). Other sources are acknowledged by footnotes giving explicit references. A bibliography is appended.

Signed Elis Edward Hillard Park (candidate)

Date 12/03/2021

STATEMENT 2

I hereby give consent for my thesis, if accepted, to be available for deposit in the University's digital repository.

Signed Elis Edward Hillard Park (candidate)

Date 12/03/2021

Acknowledgements

I would like to acknowledge the University of Wales Trinity Saint David for allowing me to go ahead with my dissertation especially to Jane Thomas and Wynne Jones who approved the work in May 2020; I would also want to acknowledge the support workers who have helped me during the time of this dissertation especially to Clare Rees who spent many hours guiding me and placing me on right path during this research. I finally would like to thank my family from both Canada & the UK who have supported me in my work with providing assistance, motivation and giving me guidance on the right path during the uncertain times of the pandemic.

Abstract

This dissertation explores the UK & Canada's cybercrime policies in how it protects vulnerable people from cybercrime along with areas where both governments can improve and where their policies are successful.

The objectives of this research were to study the age ranges of the vulnerable people, to investigate the policies the UK and the Canadian governments should have in place to protect vulnerable people; to identify charities that exist to help people vulnerable people in the UK & Canada; to study the different types of cybercrime that exist, review the Equality legislation for both nationals; to review responses on the vulnerability of people from cybercrime from the findings; to evaluate how the Canadian and UK governments are looking to protect vulnerable people who may become the victims of cybercrime and finally recommend any changes that are deemed necessary to the cybercrime strategies in the UK & Canada.

The methods chosen for the research followed the research onion model. The primary research consisted of an online questionnaire consisting of both quantitative and qualitative questions to allow a mixed method approach. An examination of the results from each question in the online questionnaire was undertaken in detail; some quotes were compared to show respondents' perceptions of cybercrime, what people think about government roles in combatting cybercrime along with their views on how the government should be protecting vulnerable people.

The secondary research was conducted in the form of a literature review which examined numerous journal articles, government publications, books, newspaper articles and online reports from researchers who have explored the effects of cybercrime. The literature review also carefully examined papers on how Canada and the UK governments are tackling cybercrime and how they are developing strategies to protect their citizens from danger. The secondary research also investigated in detail several aspects of the topic such as the current policies for protecting vulnerable people from cybercrime, the types of cybercrime, a look at both countries' equality policies along with how they came into effect. Cases studies were also examined on where each nation has failed to protect its citizens from the dangers of cybercrime to form a triangulatory view.

It should be noted that during the course of this dissertation there were several limitations placed on the researcher due to the unforeseen situation of the Covid-19 pandemic which impacted on the access to literature and to be able to share the questionnaire as widely as possible.

The key findings of the dissertation give a good indication of what the general public think about various topics relating to cybercrime, for example, their view on some of the policies being put into

place and the new strategies. The findings also point out numerous areas where both governments & police can improve their services. In total, there were 86 questionnaire responses analysed.

The questionnaire participants were asked to self-identify with a number of diverse groups which included mental health, disability or transgender. Further questioning explored whether the participants have ever experienced cybercrime, the rationale is that respondents identifying with any of these categories are deemed as vulnerable.

Recommendations for change or further work include what could be done by both governments to ensure that vulnerable people are protected by cybercrime. Due to the impact of the Covid-19 pandemic, further work could include interviews with police and/or cybercrime organisations, victim support services and related charities. In addition, there are further questions that could be answered through interviews relating to the UK & Canadian police forces' point of view on the current and proposed cybercrime strategies.

Contents

Chapter 1 Introduction	8
Aims	10
Objectives	10
Chapter 2 Literature Review	11
2.1 Introduction to vulnerability and cybercrimes that exist	11
2.1.1 Vulnerability	11
2.1.2 Types of Cybercrime	12
2.1.2.1 Cyber terrorism	12
2.1.2.2 Cyber Extortion	14
2.1.2.3 Online Cyberstalking	14
2.2 National policies.....	15
2.2.1 UK NATIONAL CYBERSECURITY STRATEGY 2016-2021	15
2.2.2 National Cyber Security Strategy (Canada).....	17
2.3 Equality legislation in the UK and Canada	19
2.3.1 UK.....	19
2.3.2 Other legislation offering protection	20
2.3.3 Canadian Human Rights Act 1985.....	20
2.4 New strategies to protect vulnerable people UK & Canada	21
2.5 Charities linking with Cybercrime	22
2.6 Summary/emerging issues.....	23
Chapter 3 Methodology.....	24
Introduction	24
Research Onion	24
Philosophies	24
Approaches	25
Strategies	25
Case studies	26
Online Questionnaire.....	26
Choices	27
Secondary Research	27
Data Collection.....	27
Time horizons.....	28
Techniques and procedures.....	28
Resources and planning	28
Data reliability.....	29

Data validity	29
Coding	29
Triangulation	30
Limitations of the Study	31
Covid 19 limitations	31
Ethics	32
Chapter 4 Data Analysis	33
4.1 Introduction	33
4.2 Findings	34
Q1. Are you the UK or Canadian Citizen? What nationality are you? UK Canada Other	34
Q2. Age of Respondents.....	34
Q3. Respondents by Gender	35
Q4. Diversity of respondents	35
Q 5 Understanding of the term vulnerable individual	36
Q6 Types of Cybercrime	37
Q7. Opinions on whether cybercrime is a current threat.....	37
Q 8. Impact of a personal cybercrime incident.....	38
Q9. How many times have you been involved in a cybercrime incident?	39
Q 10. Handling of cybercrime incidents by the police	39
Q 11. Number of times police were contacted about cybercrime incidents.....	40
Q 12. Charities approached for support	40
Q 13. Effectiveness of the police in combatting cybercrime	41
Q 14. UK Government strategies to protect vulnerable people from cybercrime	42
Q 15. Opinions on what the Canadian government should be doing to protect vulnerable people adequately from cybercrime.....	43
Q 16. How UK & Canadian governments can inform the public of measures to protect vulnerable people from cybercrime	43
Q 17. Parental responsibility for their children's online activities (up to the age of 15).....	44
Q. 18. Opinions on whether Shamima Begum should be allowed to re-enter the UK following her involvement with ISIS	45
Q 19. Views on the UK Online Harm White paper and the Canadian National Cyber Security Action Plan (2019-2024)	46
Q20. Opinions on what the UK & Canadian governments should be doing about the current Cybercrime legislation.....	46
4.3 Summary of findings	47
Chapter 5 Discussion, Conclusion, and Recommendations.....	48
5.1 Introduction	48

5.2 Discussion.....	48
5.3 Data reliability	49
5.4 Data validity	49
5.5 Deductive approach	50
5.6 Conclusion.....	50
5.7 Recommendations	52
References	54
Appendix 1 Protected characteristic.....	66
Appendix 2 – Gantt Chart	70
Appendix 3 - Online Questionnaire.....	71
Appendix 4 – Milestone Table (Government of Canada)	75
Appendix 5 - Vulnerable people Case study (UK & Canada).....	76
Case Study One - Breck Bednar.....	76
Case Study Two - Shamima Begum.....	77
Third Case Study - York University cyber attack	78

List of Figures

Figure 1 Internet Safety & Digital Piracy.....	13
Figure 2 ISIS Is Expanding Its Reach On Twitter	13
Figure 3 ‘How concerned are you about experiencing being asked for a payment in return for getting back control of your device?’	14
Figure 4 Proportion of women aged 16 to 24 who experienced cyber stalking in the last year	Error! Bookmark not defined.
Figure 5 Should the government be doing more to help people manage their own and their children’s online safety and, if so, what? Note: Online portal respondents only.	21
Figure 6 Research Onion	24
Figure 7 Illustration of direct realism and critical realism	25
Figure 8 Bar chart Most popular social networks worldwide as of July 2020, ranked by number of active users	26
Figure 9 Elis Park (P149475) Gantt Chart.....	28
Figure 10 UK, Canadian or Other pie Chart.....	Error! Bookmark not defined.
Figure 11 Age Groups.....	34
Figure 12 Genders Groups	35
Figure 13 Categories Groups.....	35
Figure 14 Types of Cybercrime	37
Figure 15 Cybercrime a Threat.....	37
Figure 16 Involved in a cybercrime incident	39
Figure 17 Number of times police were contacted about cybercrime incidents	40

Chapter 1 Introduction

Like many other countries around the globe, the UK & Canada are at a high point in the digital age. The digital age allows people and economies to be effective with communication and other online services, but there is a harmful aspect in a digital environment where terrorist groups or activist organizations will recruit vulnerable people for their gain (Lakmoy, 2017). Also, vulnerable individuals are being groomed online by older people (Internet Matters, 2020). This dissertation will be evaluating United Kingdom (UK) & Canada's Cybercrime Policies, whether they protect vulnerable people and whether they are relevant today. It will also be looking into what type of persons are vulnerable to cybercrime.

Terrorism needs to be mentioned as it plays a part of cybercrime as many terrorist groups will use the internet to plan attacks, to fund themselves, and to recruit new people to join. There is currently no worldwide definition of terrorism as many countries have different views on the subject.

"Terrorism is the use or threat of an action, both in and outside of the UK, designed to influence any international government organization or to intimidate the public. It must also be to advance a political, religious, racial or ideological cause." (CPS, 2017). While in Canada is definition of terrorism "section 83.01 of the Criminal Code defines terrorism as an act committed "in whole or in part for a political, religious, or ideological purpose, objective, or cause" with the intention of intimidating the public "...with regard to its security, including its economic security or compelling a person, a government or a domestic or an international organization to do or to refrain from doing any act." (Government of Canada, 2015).

In 2018 the Dutch government alongside the Dutch police conducted research which discovered that young people were more likely to become a victim to cybercrime (CBS, 2019). The study involving young people was 18- 24 years old young adults which found that 12.7% are likely to be victims of cybercrime because many people in this age group use technology devices for work or personal reasons compared to older generations who are less likely to use technology in their spare time. It was also revealed that the most common type of cybercrime is property crime, in Dutch law, this relates to money or property which stood at 4.6%, also within property cybercrime the additional factor found in the data was that 2.7% of young people were scammed via online shopping fraud, however, in the report, only one-quarter of shopping fraud crimes are reported to the police (CBS, 2019).

These statistics indicate that less intervention was needed by the police as the banks acted upon the fraud before the police took action to investigate and prosecute the crime. The report from the Dutch government lists who is most likely to be vulnerable to cybercrime. This would-be teenager

and young adults who are the main group most likely to be targeted by cybercriminals however other age groups can be victims too and this should be kept in mind. Government of the Netherlands is carrying out more research on how they will combat the issue and what support they can offer to help young adults in the future.

Cybercrime first became known during the 1970s when computer technology was widely available for families to operate at home during their leisure time (Moore, 2005). In 1807 there was evidence of cybercrime where telephones were tapped; also, during World War II where the British deciphered the German enigma codes; the code breakers developed the first computer which was better known as Christopher (Fell, 2017). However, it is believed that the first recording of a cybercrime by the police happened in 1988 when the first internet virus was discovered called the Morris Worm which would affect the speed of a computer. The person behind the worm virus attack was arrested under the “Computer Fraud and Abuse Act” in the United States (Fell, 2017).

There are many forms of cybercrime within the digital world where vulnerable people may fall victim. According to Chesnay & Anderson (2008), vulnerability is defined as a state where a person is likely to be influenced or harmed by a particular individual or communities; vulnerable people tend to disagree on this because they focus on their strengths rather than their weaknesses. An example of this can be young children/teenagers using the internet because they know how the cyberspace technology works (which is a strength), however within some gaming environments, internet, chat rooms, and social media they may not be aware that they are being groomed by someone as they think the person is being kind to them, which can be perceived as a weakness.

It is important to understand what cybercrime is and how it links with crime; the UK CPS defines cybercrime as an umbrella of mixed crimes of which there are two distinct categories. The first category of cybercrime is known as “Cyber-dependent crimes” –the crime must be committed through Information and Communication Technology (ICT) using devices such as mobile phones, laptops, computers, or other devices. The second category is known as “Cyber-enabled crimes”. This is where a conventional offense can be committed on a wider scale, where the offender uses technology to assist them to expand and widen the scale of the offense. An example of this could be cyber-enabled fraud and data theft (CPS, 2020).

In Canada, they define cybercrime as cybercriminals whose main aim is to target vulnerabilities in computer software, computer hardware, and vulnerable people’s online behavior. The goal of the criminals is to use technologies to steal personal and commercial information by fraud or extortion; cybercriminals who target Canadians also operate around the world and tend to be out of reach for Canadian law enforcement (Government of Canada, 2020).

The reason why the research is needed is to have a better understanding and how both governments protect vulnerable people from the cyber world; because the cyber world keeps moving at a fast pace where new things are happening, and it can lead governments around the world to fall behind the curve. The reason why both Canada & the UK have been selected for this study is that these are among the leading nations within the digital world. There have been some cases where both governments have failed to protect their citizens' safety from online threats, for the UK that would be the case of Breck Bednar & Shamima Begum with Canada it is the case of York University. The need for this research was addressed by an online questionnaire, an examination of three case studies, and a literature review, all of which were evaluated.

Aims

To assess whether the UK & Canada Cybercrime Policies can protect vulnerable people and if these strategies are relevant today.

Objectives

The following goals have been recognized for the investigation applying the SMART theory for the target to be achieved (Day & Tosey, 2011, p 518):

- To research which policies and Equality legislation the UK and the Canadian governments have in place for vulnerable people
- To identify charities that exist to help vulnerable people in UK & Canada
- To examine different types of cybercrime that exist and to which age ranges of vulnerable people
- To evaluate how UK & Canadian Governments are looking to protect vulnerable people who may become the victims of cybercrime.
- To recommend any changes that are deemed necessary to the cybercrime strategies in the UK & Canada.

Chapter 2 Literature Review

2.1 Introduction to vulnerability and cybercrimes that exist

This literature review will cover five key themes, which are what is vulnerability/cybercrime exists, policies that the UK and the Canadian governments have in place to protect vulnerable people from cybercrime, whether the Equality Act 2010 in the UK and the Equality Right Act 1977 in Canada protect vulnerable people, how the UK & Canadian Governments are looking to protect vulnerable people who may become the victims of cybercrime and vulnerable people case studies (UK & Canada). At the end of the literature review, there will be a summary and discussion of emerging issues.

2.1.1 Vulnerability

There are many forms of cybercrime within the digital world where vulnerable people may fall victim. According to Chesnay & Anderson (2008), vulnerability is defined as a state where a person is likely to be influenced or harmed by a particular individual or communities; vulnerable people tend to disagree on this because they focus on their strengths rather than their weaknesses. An example of this can be young children/teenagers using the internet because they know how the cyberspace technology works (which is a strength), however within some gaming environments, internet, chat rooms, and social media they may not be aware that they are being groomed by someone as they think the person is being kind to them, which can be perceived as a weakness.

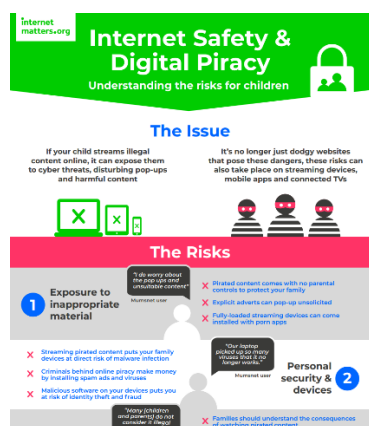


Figure 1 Internet Safety & Digital Piracy

The poster from Internet Matters (2018) backs up the fact that the children are vulnerable online as they do not understand how the cyber world works, for example, digital and online grooming.

The Children's Commissioner for England (2018) illustrates how modern technologies that use Wi-Fi can be compromised. Devices such as CloudPets and baby video monitors can be intercepted – data suggests that 5% of UK homes now have these devices.

Worryingly, these devices can capture children's voices and even their video images for later circulation within the paedophile

community. A solution could be where the homeowners change the passwords, but there are still questions about limiting or preventing the children from having access to the toys. The CloudPets' CEO Mark Myers denied that all voices of children were obtained from devices as the hardware made it difficult for hackers to gain access to the files of the children's voices however if they did bypass the password, then they would only be able to hear sound recordings without personal

identifiers (Hern, 2017). This statement strongly contrasts with the report by the Children Commissioner, presumably because of the business interest in the CloudPet range of products.

A report from Internet Matters (2019) highlights many key areas on why children are the most vulnerable when online; one section of the report says that children who are cared for are seven more times likely to have their details hacked. The report also explains that children with special needs or who are young carers are more likely to be vulnerable within the digital world, due to a lack of education about the internet. The authors want to see all parents educated on online safety to ensure any children with special needs are kept safe from cybercrime. Whilst the authors of the report have recommended a form of a framework as a new perspective about young people within the care system or with special needs, the drawback of the report is how the authors have not given any advice to parents outside the disadvantaged groups.

2.1.2 Types of Cybercrime

2.1.2.1 Cyber terrorism

Torok (2010) explains cyber-terrorism and how Al – Qaeda (AQ) recruits' people online. In his research, AQ's strategy is to use a wide range of networks and platforms to reach a worldwide audience. In his explanation of why AQ uses cyberspace platforms, the rationale is that it gives the AQ leaders more control over their "message" (propaganda) compared to using traditional media such as the radio and TV. AQ prefers cyberspace as it allows them to publish propaganda nonstop for their supporters.

In Torok's research, there are three areas that AQ uses to recruit people from online sources known as Hosted sites. Those websites are hosted by AQ themselves, second Non-Hosted sites; AQ will have Facebook groups, Twitter accounts, Myspace, and other social platforms. AQ's third area is the publication of the Inspire magazine which teaches their supporters how to make bombs and other devices. In the UK AQ have been known to target many vulnerable groups of people, especially young adult males at UK universities because they know males are more likely to join their cause, for example back in 2007 four young British males were arrested under the terrorism act for planning an attack on the UK during, the police found a huge amount of terrorist propaganda on computer hard drives (Livingstone, 2007). In this important study, Torok makes the interesting point that the greatest threat in cyberterrorism is the recruitment because western governments take the threat of cyberterrorism more seriously than the recruiting process, which has left some western countries at a disadvantage in combatting the recruitment aspect.

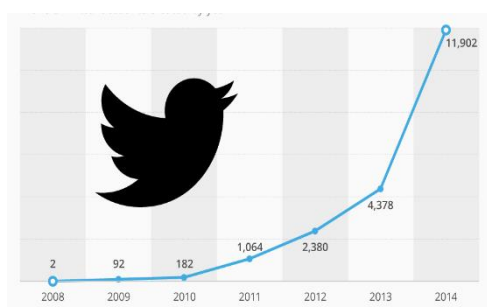


Figure 2 ISIS Is Expanding Its Reach On Twitter

There is currently no status on how many social media accounts AQ have at this moment, this line graph showed the growth of how many ISSI accounts there are from the past six years, this backups Torok on how AQ uses social media (McCarthy, 2015).

The strength of Torok's research is that it highlights the three key areas on how terrorist groups such as AQ and other terrorist organizations recruit people and how they are now using the internet and social media platforms to their advantage. He also identifies vulnerable groups within society who are likely to be targeted. Another valid point to his research is that Torok has highlighted weaknesses where various western countries have fallen behind on combatting cyberterrorism recruitment and therefore are not taking the threat seriously.

There are three drawbacks to Torok's research, the first weakness is that it only examines one terrorist group within his research. This limits the study as it only focuses on one terrorist organization's strategy on cyberterrorism and how they use internet networks and social platforms to recruit people, for example, Torok should have included other groups such as ISIS who are well known for recruiting supporters online via social media platforms. A second weakness of the paper is that there is no identified methodology so there is no clarity on how the research was collected. A third issue of the paper is information based on references that were seven years out of date when Torok wrote his paper.

An opportunity for improvement of the paper is that Torok could have included a wider range of terrorist factions, for example, he could have compared how AQ and ISIS were recruiting people via online social media platforms. It would have also widened the range of sources and information to compare the two different groups and viewpoints. Also, the paper could have included a methodology section, which would have improved his research as there would have been a clearer structure regarding research methods and how the data was collected.

Overall, the research is clear as it refers to the recruitment of university students, but because the paper is from 2010, it is out of date; for example, a lot has happened during the past 10 years. Torok makes a number of valid points like the fact that some western countries are falling behind in dealing with the recruiting of people. However, this may no longer be the case as western governments have invested in combatting the issue.

2.1.2.2 Cyber Extortion

A worrying threat for individuals and organizations is on the increase, for example, the NHS WananCry cyber-attack which placed the NHS as an organization and the patients in a vulnerable place (Smart, 2018). Cyber Extortion is where hackers will intrude into an individual's electronic device then withholds the victim's data and threatens to release information if they do not produce some form of payment (Simmons & Simmons, 2018). A newspaper report from the independent from 2020 who have information from the National Crime Agency (NCA) there have been 9,473 cases of sextortion which is another form of cyber extortion (Oppenheim, 2020).

An analysis of the research carried out by (Johnson, 2020), one of the strengths of the bar graph

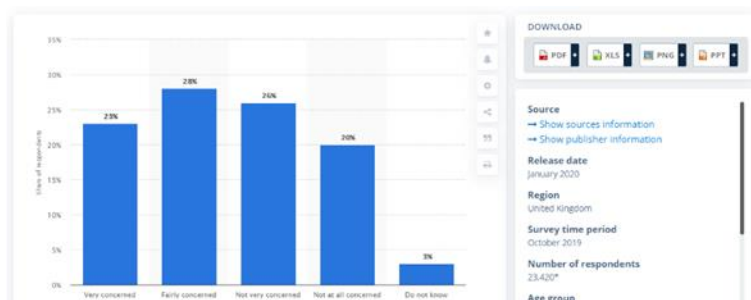


Figure 3 'How concerned are you about experiencing being asked for a payment in return for getting back control of your device?'

shown in Fig 3 illustrate how people would react if they were placed in the situation in which 23% of people would be vulnerable at this point and would pay the hackers to reinstate their data without going to the Police to explain their issue. Other groups

would think about other routes to take first. An additional strength of the research is that it was published in 2020 meaning the research is new. The weakness of the graph is that he did not show the age range from each of the charts, only shown was that ages from 15 upwards took part in the research, but this does not give a clear picture of what age group is most vulnerable. A threat of the bar graph again does not give a clear image of the investigator work about their topic.

2.1.2.3 Online Cyberstalking

Norton (2020) defined online cyberstalking as threatening behaviour and unwanted attention from an individual or a community of people.

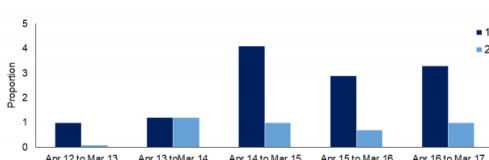


Figure 4 Proportion of women aged 16 to 24 who experienced cyber stalking in the last year.

Online cyberstalking has become a new issue for the UK and Canadian governments to consider. A vulnerable group affected by this are females who have been involved in domestic abuse cases (Davidson et al., 2019). Fig.4 displays the age ranges of females who are victims of cyberstalking over a period of four

years. The strengths of this research are that it illustrates females are more vulnerable to cyberstalking than males. It also identifies key aspects of cyberstalking, for example, Davidson points out the legislation that protects victims. In his report, he suggested that more detailed research is needed about the victims for example their sex, ethnic group or whether they have a

disability which would provide a better understanding of which females are likely to be more vulnerable to this kind of behaviour. A weakness of the bar chart is that it does not show current data or older age groups as it refers to only younger females. There is no methodology within the report explaining how the statistics were collected. Another weakness is the outdated references, for example, Davidson used sources from 2002 which in 2014 is 12 years out of date. An opportunity that the researcher should have undertaken is allowing their work to carry on as they published their report two years later in 2019. A second opportunity to report is that there should be a methodology section to report explain how data was going to be collected and from which sources. Moreover, the report does not give a clear picture of other age groups who could be victims of cyberstalking (Davidson, et al, 2019). In contrast, Short et al (2015) argue that the vulnerable group is the cyberstalker themselves as most of them are young males in their teens or early twenties, suffering from some form of mental health illness mainly depression, anxiety, or stress. Yet, both authors make strong cases by identifying who is vulnerable, whilst Davidson points out that young females are mainly the victims of this type of crime.

2.2 National policies

2.2.1 UK NATIONAL CYBERSECURITY STRATEGY 2016-2021

In 2016 the UK government updated the UK National Cybersecurity Strategy 2016-2021, which aims to protect the UK and its citizens from cyberspace (Home Office, 2016). It states that the UK aims to be at the forefront of the cyberworld.

In analysis of the policy, section 2: Tackling cybercrime, the policy identifies that all 43 police forces in England and Wales are trained and assembled into specialist units to deal with local levels of cybercrime - this is a policy strength for vulnerable people as the police can use their known intelligence to help them at a local level. Another strength of the policy is that it highlighted that terrorist factions no longer pose a threat to UK cyberspace; however, it does mention that the UK will monitor terrorist groups' activities, this is to ensure that nothing is targeted like key buildings or companies in the UK. Thirdly, this policy has identified vulnerabilities in some areas of cyberspace, for example in 'Availability of hacking resources' the UK policy explains that hackers will always have tools ready to attack UK citizens and companies no matter how prepared the UK is for this. This means the UK has acknowledged there will always be a continued threat from hackers. Another positive aspect of the policy is that by 2021, the government has three aims: to deter any threats from other nations; to investigate cybercrime incidents; will also take action to disrupt hostile activity. This means the UK will try to prevent international and national threats and if needed, will

use measures to stop other nations and other groups from damage to the UK infrastructure or putting its citizens into a vulnerable place as mentioned in the WannaCry NHS attack.

An evaluation exposes the weakness of the policy. The first issue is that it does not explain any of the measures that will be put into place for vulnerable people, for example, the West Yorkshire police force has published guidelines called “A Guide to Cyber Crime and Online Safety” (West Yorkshire Police, 2018). This guideline document informs readers how to avoid becoming a victim of cybercrime and how to protect themselves. However, it only refers to how the government and other public sector organizations are dealing with cybercrime by seeking to protect UK companies and businesses against cyber-attacks. A second issue relating to the strategy is that it generally focuses on how the UK wants to protect its economy more than its citizens; worryingly the policy provides no information about vulnerable people. Next, there are no theoretical links that it uses to examine the problem. In identifying an opportunity, the policy could have shown future planning similar to the one used by the Canadian government to measure achievement of an objective or when currently working towards achieving an objective as shown in Appendix 3 which lists the cybercrime strategy published by the Canadian Government. It lists key dates by when it wants to achieve the objectives or when the objective has been deferred (Government of Canada, 2018). A better example is the UK National Crime Agency (NCA) which published a cybercrime strategy to protect vulnerable people, they also published a video explaining the danger of cybercrime, the possible impact on children and young people, and their vulnerability to becoming hackers unknowingly (NCA, 2020). By producing the strategy in a number of formats, making the content more accessible to young people and diverse groups. Another opportunity where the West Yorkshire guidelines could improve is by including data showing key areas where cybercrime has increased. There is a potential risk in that there will always be incidents where the UK government cannot fully protect its citizens. The general overviews are that both governments want to protect their economy rather than their citizens. Protecting its citizens is the job of both police forces according to the government.

Mori & Goto (2018) reviewed the new government cybersecurity policy for 2016 – 2021; the article mainly talks about the UK’s aims to protect the UK economy. Oath Inc., as cited by Mori & Goto (2018) refers to the accounts hack in 2017 of Yahoo who had had three billion customs accounts compromised. The only accounts affected were those created in 2013. They also highlight that cybercrime attacks can occur anywhere in the world that can affect individuals. To combat the issue, Yahoo told their users to change passwords as the only action necessary. Also, the head of Yahoo cybersecurity was told to stay silent when he first heard about the incident (Dilipraj, 2016). Eventually, when US law enforcement intervened, Yahoo was told that they were obliged to enlist

support as the company had broken laws in the US; Yahoo then employed a Cybersecurity company (Esteves et al., 2017). Unfortunately, this makes other smaller companies vulnerable to cyber-attack as some small companies would be unable to afford the investment for cybersecurity protection.

The article has merits in that it explains how the government has improved upon its UK Cyber Security Strategy since its publication for 2011 – 2015. In the article, both authors agreed that the UK government should be doing more to protect its UK citizens from cyberattacks. They believe the policies are good for the government which is mainly to protect the private sector for example companies. Importantly, they do suggest that the UK government should increase the protection of vulnerable people.

A weakness of the journal is the methodology, there is no clear method on how the research was carried out for their quotation 'review national cybersecurity strategies and used it to review the UK cybersecurity' However, they mentioned that they did use the capability maturity model which is used by software developers to find out results during their research according to Paulk, et al (1993). There are gaps in this research, for example, it only briefly explains what the government is doing to protect UK citizens who are vulnerable from cyberspace, whilst its main focus is how the UK government is going to protect big corporations as they are deemed more important.

Overall, the journal talks about how the UK only wants to protect the private sector, not UK citizens, the journal also explains how anyone is vulnerable to cyberattack. The journal is written from the point of view of someone in the IT sector as the journal contains many technical terms. The authors fail to make recommendations regarding the 2016-2021 UK Cybercrime government strategy to protect vulnerable UK citizens. A solution could be for the UK Government to undertake further research to consider how to protect these vulnerable groups and review what resources could be allocated.

2.2.2 National Cyber Security Strategy (Canada)

The strength of the National Cyber Security Strategy for Canada is that the Royal Canadian Mounted Police (RCMP) has more resources to combat cybercrime, this gives the RCMP more cybercrime teams, more training in dealing with sensitive cases (Government of Canada, 2019). An additional merit of the strategy plan is there is a policy-making team, this policy team in the Canadian government reviews cybersecurity and cybercrime cases, for example, if there is a rise in the cases of cybercrime in Canada the policy team can advise the government to bring in new laws this asset should be in place by the end of 2022. An advantage of the strategy for Canada is the government has laid out when they are going to meet their targets and when they have achieved them. The

Canadian government does this by having reviewing sessions and meetings and looking at reports which then decides if the object has been met or if it needs to be pushed back.

There are however weaknesses of the National Cyber Security Strategy as it only explains how the Canadian government only wants to protect the interests of private companies as they benefit the government more than vulnerable people (Government of Canada, 2019). The government has not put forth any programs to protect vulnerable people in cyberspace, this means the vulnerable are continuously at risk online unaware of what can be done to protect them.

This could be remedied by the Canadian government amending their strategy plan to include measures on how they will protect vulnerable people, such as the UK'S Online Harms White Paper (2019) which sets out the strategy to protect vulnerable people in cyberspace. The Canadian government could easily layout the steps it could take to better regulate cyberspace from harmful content.

Overall, the Canada National Cyber Security Strategy fails to protect vulnerable people. Yet the Canadian government have acknowledged that cybercrime is a growing problem within their nation and is trying new ways to combat it, for example citizens of Canada are able to report cybercrime incident more easily (Government of Canada, 2019). But this is not a preventative measure in reducing the increasing number of incidents.

When compared with the current UK government cybercrime strategy, it is vastly similar as the Canadian government's concern is to protect private companies rather than its most vulnerable citizens.

Research carried out by Roll and Huey (2015) on cyberbullying would disagree with the Canadian government as both researchers interview Canadian police officers & school officers on their view on cyberbullying showed a different point of view from the side of law enforcement. There is numerous key area: the strength the research brings out first is the paper asks children their point of view on cyberbullying and how they deal with it in their lives which government white papers often ignore. The second strength of the paper gives the parents view, asking them how they want to cyberbully to be dealt with. A third strength of the research is the methodology that was undertaken during their investigation both authors used in-depth qualitative interviews with 12 police officers who were currently involved in cyberbullying incidents to find out from the point of view of police officers how they wanted cyberbullying to be dealt with. The results showed many of the police officers believed that cyberbullying was a problem within the school system in Canada but, however, it issues that police officers cannot deal with due to the fact there were no life threats may towards

the children; the only time a police officer can step in is when someone has threat towards the person online.

There are numerous weaknesses in the methodology used by Roll & Huey; the researchers wrote a letter to the Head of the Canadian police force asking for interviews with the officers although this action was necessary for prior permissions, an email with an attached letter would have been more appropriate. In that letter time frame, important information could have been forgotten or the officers could have been handpicked to give answers that put the police force in a positive light. The second weakness is that it does portray the Canadian police officers in a negative view, as many officers believed that they could not deal with cyberbullying. They thought it was a pointless task forcing civility between children, because no life threat was being made towards the victim which meant that the bully was not offending. Also, as these incidents occurred outside school hours, nothing could have been done about it. This shocked the researcher as they believed that officers should protect everyone regardless of the type of incident. The weakness of the findings is that the researcher mainly viewed the officer's side of things which meant that children who are deemed vulnerable had little opportunity to discuss the issues and what could have been implemented. Again, the results paint a negative light on the police officers as they do not seem to care about the issues that occurred.

To conclude, the journal clarifies the RCMP view on cyberbullying which they believe to be pointless as they cannot act on cyberbullying unless serious threats are made towards the victim, for example, death threats. This raises another question - whether the Canadian government gives the RCMP more money to deal with cybercrime if they are not taking cyberbullying seriously.

2.3 Equality legislation in the UK and Canada

2.3.1 UK

The Equality Act 2010 (UK) brings all previous separate UK legislation under one umbrella. It pays attention to groups of people whose differences are known as 'Protected Characteristics'. A list of these is shown in Appendix 1. It shows that these groups of people are protected under Equality law from discrimination, harassment, and victimisation in terms of cybercrime there are four groups of particularly vulnerable people who are those with disability (physical or mental health illness), race, age, and sex. For example, young children and teenagers will be vulnerable to harassment e.g., cyberbullying and grooming (NSPCC, 2020). People who suffer from a disability are vulnerable to cybercrime as they are unaware of being groomed or someone with mental health issues could find harmful material. An example of this can be the case of Molly Russell who killed herself after finding harmful material online, however, it is unclear if she suffered from mental health issues (BBC, 2019). As mentioned, people from different ethnic backgrounds will need to deal with a high volume of

online hate crimes. Regarding gender, many females are vulnerable to online cyberstalking as mentioned earlier in Davison (2019) report many females are likely to find themselves as victims of cyberstalking whilst males are likely to be the offender. Transgender people in cybercrime terms are likely to be cyber-bullied compared to other sexes, for example in cyberbullying research undertaken by Patchin, (2011) many victims of cyberbullying were transgender, the responders said they were easy targets for people to bull them as they are vulnerable.

2.3.2 Other legislation offering protection

The current legislation that protects vulnerable people in the UK include Communications Act 2003, The Crime and Disorder Act 1998, Anti-Social Behaviour Act 2003, Criminal Justice and Immigration Act 2008, Crime and Security Act 2010.

The strength of the Communications Act 2003 legislation is that if a person is trolling another vulnerable person, they may be arrested straightway under the 'Improper use of a public electronic communications network'. Anyone who feels vulnerable to online trolls may report it, possibly leading to arrest (Bishop, 2012). A weakness of the Act is that the maximum prison sentence for offenders is currently six months meaning the online troll would be able to re-offend if the penal system has not rehabilitated them properly (Bishop, 2012).

Victims of Cyberstalking in the UK are protected by section 2A of the Harassment Act 1997; this means that if stalking occurs over a period of time and if the police's repeated warnings to the stalker have been ignored, the police can arrest the stalker. However, in 2012 section 4A was added, which means that if the victim is fearful of violence by the stalker, then the police can arrest the stalker as the victim is already vulnerable (CPS, 2018).

2.3.3 Canadian Human Rights Act 1985

Like the UK Equality Act 2010, the Canadian Human Rights Act 1985 brings existing acts together under one section, however, the difference between the acts is that the Canadian government only includes discrimination rather than harassment or victimisation (Government of Canada, 2020). The protected characteristics in Canada are Race, their National or Ethnic origin, the colour of their skin, a religion they follow, age of the individual, the gender of the person, sexual orientation, gender identity or expression, marital status, family status, genetic characteristics if they have a disability or have a past criminal conviction (Government of Canada, 2020).

The extra differences between the Canadian Human Rights Act 1985 and the Equality Act 2010 is that the Minister of Justice in Canada is held responsible for updating the Canadian Human Rights Act 1985 whilst in the UK it is Parliament's responsibility to update the Equality Act 2010. The second difference between the two acts is that the UK Equality Act covers more areas such as harassment

and victimisation in public and the workplace. The Canadian Human Rights Act 1985 only talks about discrimination in the workplace and public areas. Both legislations point out what specific vulnerable groups will be exposed to this type of crime happening to them, however, neither the UK nor Canada equality legislation includes cybercrime or how both governments will protect those vulnerable groups accordingly. This raises the question whether there needs to be a revision of the legislation in each country.

2.4 New strategies to protect vulnerable people UK & Canada

The UK government is hoping to introduce new legislation which benefits vulnerable people & victims of cyberstalking through the 'Online Harms White Paper' which will cover a wide range of issues around harmful content, self-harm, online abuse and radicalisation (Home, Office, 2020). In one section of the paper, the government has indicated that it will hold social media companies responsible with penalties (for example, imposing fines) if they do not resolve issues or report incidents early on (Home Office, 2020). The only negative side to the Online Harms White paper is



that many MPs have argued against the impact upon freedom of expression online, causing a delay in the progress of the paper within the House of Lords (Home Office, 2020). Figure 5 illustrates an argument between online organisations and online individuals about whether the UK government should do more to protect children online.

Figure 5 Should the government be doing more to help people manage their own and their children's online safety and, if so, what? Note: Online portal respondents only.

Like the UK, Canada at this time does not have any legislation relating to cybercrime; however, Canada has added cyberstalking to an updated version of Code 264 of the Criminal Code Act (1985), last amended in September 2020. Within this, the Canadian Justice Department states that no individual should fear another person following them without their knowledge; the Canadian courts can imprison the offender for ten years maximum or issue a restraining order (Government of Canada, 2020).

2.5 Charities linking with Cybercrime

Many charities exist to help to protect vulnerable people to prevent and when affected by cybercrime in UK and Canada. All charities are important as they provide their services free of charge. This could be providing information about aspects of cybercrime.

The UK charity Victim Support aims to help vulnerable people by providing them with support throughout their cases. On the Victim Support website, the charity explains what cybercrime is and how it affects people, this is one of its main strengths as it provides clear information about a range of online crimes; secondly, it explains how a victim may feel during an incident, this is a strength especially for vulnerable people who may not be able to explain how they are feeling about something whereas another person can see the signs (Victim Support, 2021). The weakness of this website is the lack of further information about other services they provide for victims. Also, they do not provide leaflets which means people without internet access cannot be informed about Victim Support Services.

Another charity to discuss is the Child Exploitation and Online Protection Command (CEOP) which aims to ensure that children stay safe online and are not exploited by adults when using the internet. The charity operates on a global platform which means it seeks to protect all children which therefore includes children from the UK as well as Canada (CEOP, 2021). A strength of the website is that a person can report a case immediately if the child felt vulnerable. Another strength is that any person living with their abuser can press an escape button to quickly exit the page before the abuser has any idea what is happening (CEOP, 2021). The weakness of CEOP is that it does not offer any other services for example, reports relating to cybercrime like the NSPCC does; however, the CEOP does work alongside police services globally including the UK and Canadian police. A potential threat to the charity's future is its failure to protect children who were filmed as part of a paedophile ring that was exposed by Canadian police about 2,345 British paedophiles living in the UK. The UK IPCC felt disappointed in CEOP for their handling of the information and not informing about it sooner (BBC News, 2016). These types of cases do give the CEOP a poor reputation which could result in some people not using them to report cases.

2.6 Summary/emerging issues

Many emerging issues need to be addressed, the first is both governments need to have more policies in place to protect vulnerable people online. Both nations now need to think about what they are doing to aid vulnerable people instead of relying on other services, as the first two case studies have shown the UK government failing to help their most vulnerable people though Breck Bednar's death was in the early stages of cybercrime when the UK government had little understanding on how online grooming worked.

Secondly, UK & Canada now need to update their legislation on protecting vulnerable individuals in society. The UK for example will use 'Misuse of Communications Act 2003' and other related legislation depending on the crime, while Canada will use 'Criminal Code of Canada 1985' on cybercrime cases. Yet, the UK has the Online Harms White Paper which will hopefully protect vulnerable people once it becomes legislation.

Chapter 3 Methodology

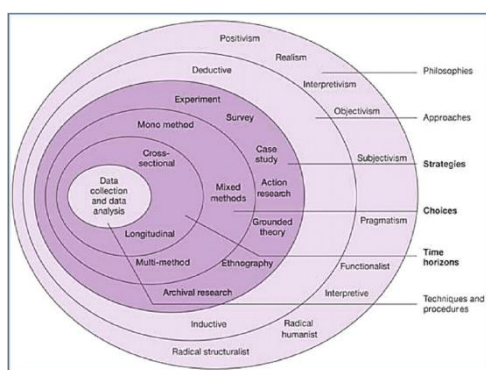
Introduction

It is important to have a good methodology as it allows the reader to understand how the researcher carried out the study, the investigator in turn needs to ensure that his methodology is to a high standard because it is the only section that is evidence on his findings. If the researcher does not use proper methodology, it can confuse readers as they will not be aware of how the investigator collected data for their study which could end up undermining his research leading to an unsuccessful study (Biggam, 2011).

This methodology will explain how the investigator collected the data, methodology for this paper followed the research onion layout (Snyder, 2019). A research onion is where the researcher describes each section of the methods employed, what philosophies were utilized, the approach used, what were strategies used to collect the data from the participants in the study, and the techniques used to analysis the data. The methodology section also explains the limitations the investigator faced during the research process over the course of nine months and the COVID-19 19 pandemic.

Research Onion

The Research Onion was published by Saunders and he believed when a researcher was undertaking their investigation, there would be layers to research like an onion; Saunders found that there are six



areas when conducting research. the six are Philosophies, Approaches, Strategies, Choices, time zones, and Techniques and procedures (Sahay, 2020). Figure 1 shows a diagram of the research onion.

Figure 6 Research Onion

Philosophies

Positivism was considered in this research as the study involves examining statistics and by approaching people in communities to carry out this investigation; the term was first used in the 19th century by Auguste Comte (Feigl, 2020). A positivism approach was needed to carry out the research, as it reviewed statistics, for example whether and how governments protect vulnerable people from cybercrime.

Interpretivism was employed as this study involved human participants in this investigation. Interpretivism is an important methodology tool to use during any research as it gains people's views on a subject area (O'Reilly, 2012; Williams, 2000). In this case, an online questionnaire was designed for the participants to answer. According to (Lin, 2005) the problem of interpretivism at the master's level is that it can become biased over the lifetime of the research which may affect the researcher study.

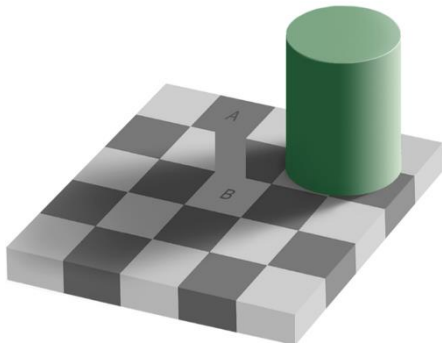


Figure 7 Illustration of direct realism and critical realism

Realism philosophy was used in this research which considers a person's point of view on a particular subject using a scientific method to help understanding and learning (Novikov & Novikov, 2013). There are two types of realism philosophy. The researcher used critical realism as opposed to direct realism as this research was to review government policies about protecting vulnerable people from cybercrime. The researcher must have prior knowledge of the topic area that is being investigated and when carrying out the primary research, it will allow participants to be

aware of the current situation of the policies that are set by their government as the researcher will inform them.

Approaches

A deductive approach involves gathering information that is from a specific area (Warwick, 2020). A deductive approach was employed in the dissertation because there is current data on the topic that was included then reviewed during the process of writing this dissertation. The deductive approach was the corrected one to use because the researcher had his theory which was his question about the UK & Canadian governments and are, they are doing anything to protect vulnerable people from cybercrime; the online questionnaire (hypothesis) was designed around the theory. Once all the data was collected from the online questionnaire and review it went back to answering the theory questions.

Strategies

Strategies used to undertake the research included an online questionnaire. These allow an online connection with communities of hard-to-reach people or groups (Andrews et al., 2010). An online questionnaire was a useful tool for this research as it collected a wide range of opinions from different people. Also, as it is online, the questionnaire can be circulated within different communities, for example, the researcher posted his online questionnaire on different community pages, such as Facebook and Twitter. The disadvantage of online questionnaires is that participants may not understand the question given to them or they may give a short answer (Nayak, et al,

2019). To overcome this the researcher ensured that all questions were carefully planned and the email address was given if participants had any questions, then the researcher would be able to respond accordingly.

The researcher has already identified three target groups for this study who are people who suffer from disabilities, mental health issues, and people who are undergoing or have changed their birth sex e.g. transgender people. The reason these groups have been selected is that they are deemed

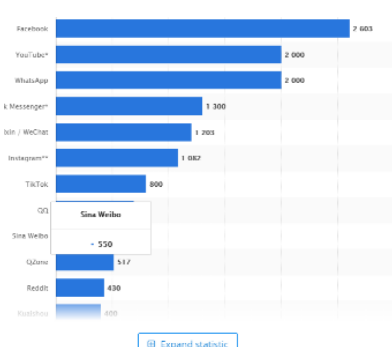


Figure 8 Bar chart Most popular social networks worldwide as of July 2020, ranked by number of active users.

vulnerable to cybercrime (Martellozzo & Jane, 2017). To access the groups, the researcher used social media websites such as Facebook, Reddit, Twitter, and Instagram as these are popular platforms (Clement, 2020). As seen by figure 3 shows what the current popular social media sites that were popular at the time. The researcher also had the help of family and friends who circulated online questionnaire forms to their friends and work partners.

Case studies

To enhance the secondary research, numerous case studies were used which can be defined as a record of a group or person within a situation (Ebneyamini et al., 2018). It included three case studies to highlight examples of situations involving vulnerable people. However, a weakness of case studies is that it becomes time-consuming for the researcher (Vannoni, 2014). The reason that these case studies were chosen was because they are useful to point out where the government have failed to protect vulnerable people from harm via online. Yin believes that studies cases are best used for qualitative research (Yin, 1984). There are three types of case studies according to Yin which are exploratory, Descriptive, and explanatory (Noor, 2008). As the research question involves a political paradigm this means, case studies were needed to point out where the two nations' governments have failed and the value of the three case studies points to where the UK & Canada can improve on their protection of vulnerable people. The strength of using case studies is that it allows the researcher the opportunity for future research to be carried out (McLeod, 2019).

Online Questionnaire

The researcher selected to use the descriptive approach when applying to Online Questionnaires this means an Online questionnaire was used because it could researcher was able to reach a wider range of groups from different places, though he had to specific groups which the online

questionnaire aimed towards. Another reason online questionnaire was picked was due to Covid 19, which means online questionnaire was a safer option instead of handing out questionnaires to people on the streets as the researcher and the participants would be breaking government guidelines that were placed at the time. For this study, the primary research consisted of Online questionnaire the researcher aimed to have 50 people take in the online questionnaire minimum and the maximum will 200 people take part in the online questionnaire, there were multiple reasons why online questionnaire was used during this paper, one of the main reason being; there is a fast response time with online questionnaire as they only take a couple of minutes to be done, another point was the investigator was not there in person this meant that participants can open more freely without feeling their being judge by the researcher himself (Wright, 2005).

Data collection was used during the case studies as the researcher was collecting the case studies from online resources such as BBC news articles, Newspapers, and university website about the three cases that are in the literature review.

Choices

The study consisted of mixed methods research (MMR) as there was primary and secondary research during the dissertation. MMR is identified when researchers use both qualitative and quantitative enquiry (Clark, et al, 2008). The advantages of this allow the researcher to use two choices at the same time during the study (Johnson, et al, 2007). However, the disadvantage of MMR can become complex overtime for the researcher as they will need to understand multiple methods to use MMR effectively (Mary, et al, 2011).

Secondary Research

Secondary research was applied when writing the paper on the subject matter, the meaning of secondary research is defined as examining existing studies and analysing the findings from each investigation to answer the researcher's question. When the researcher examine another individual's piece of work, the investigator can offer new opinions on the subject area (Heaton, 2008). For example, when analysing the research regarding UK & Canada cybercrime policies to protect vulnerable people, this could be a new area that both governments could review.

Data Collection

Primary research is described as an independent study during the dissertation; it may include questionnaires, interviews, or focus groups (Lowe, et al, 2011). online questionnaires were used as this will offer a wider range of views. The advantage of primary research is that new data was collected by the researcher, and the researcher gained specific results for his dissertation on the subject area. The only disadvantage to primary research it did become time-consuming for the

researcher during the writing of the dissertation (Shidur, 2017). Data collection, when the findings came back to the researcher kept all the data on two USB sticks which both key pass software which means the person trying to get the information from the researcher will need the password. The reason key pass software has been used is to protect the data that has been collected by the researcher; the other reason why the findings were kept on two USBs was that if something was to happen to one of the USBs the researcher would have a backup one kept safe at all time when the research was taking place.

Time horizons

A cross-sectional approach was employed for the dissertation. A cross-sectional method is where the researcher asks the participants their opinions at a given time (Dermatol, 2016). The reason that this methodology was selected for the dissertation was because of the time frame of the dissertation as the research only had nine months to be finished by 12 March. The Gantt chart was also deployed because it was used as a time frame for the researcher to have set deadlines. The study will not employ a longitudinal method because such an approach would need to be used over a period as the researcher only had nine months to complete the study (Dis, 2015).

Techniques and procedures

An online tool that was used to collect the data was Google documents as it is a free trustworthy application for students to use when carrying out research (Suite, 2019). In addition, Microsoft Excel was deployed to analyse the collected data. The reason why Microsoft Excel was used was to make pie charts, line graphics, and bar charts which showed the findings from the online questionnaire. Microsoft Excel also benefited the researcher as he was able to place the data into organised groups and which made it easier for the researcher to place the data into graphics.

Microsoft Excel is software that can be used to analyse data, which is to make table and graphs (Microsoft,2021), learning researchers, marketing, surveys companies and many more services (Microsoft,2021). Excel was used to form different graphical analysis of the differences between the participants as part of the quantitative analysis e.g., their age range, disability, mental health issues, sex transformation and nationality from the online questionnaires

Resources and planning

This research includes a Gantt chart to manage the timetable for this dissertation. It shows a timeline of what targets are planned for each week/month (Wilson, 2003). Figure 4 shows the researcher Gantt Chart that was

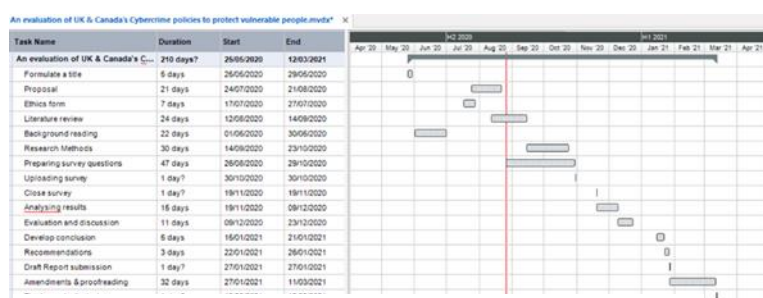


Figure 9 Elis Park (P149475) Gantt Chart

used during the dissertation period. The advantage of Gantt charts is that the researcher will be able to keep on schedule and it also avoids resource overload (Gerald, 2012). The disadvantage of the chart was that it constantly needs to be updated which becomes time-consuming for the researcher (Severina, 2019).

Data reliability

The data is reliable as 86 out of 87 participants took their time to answer all questions within the entire questionnaire. This should have taken respondents around 15 minutes to complete according to the test timing by the researcher. From this investment of time, it can be assumed that many of the participants answered the questions truthfully. However, one participant indicated that the research was pointless, did not answer the questions correctly and used aggressive behaviour towards the researcher. This respondent's answers were therefore discounted from the study.

Data validity

Data validity is important in terms of the design of the investigation; by following the research onion, time and effort were spent planning the questionnaire so that the responses would be both quantitative and qualitative in content. The questionnaire was administered in a way so that participants were able to give their views and opinions openly about the topics. The researcher was happy with the overall response to his questionnaire as many of the participants gave a good amount of detail within their answers.

Coding

There are three types of coding that the researcher used during the data analysis section of this research. The advantage of coding is that it allows the researcher to handle large amounts of qualitative data into themes (Cope, 2010). Coding will differ between each researcher according to varying epistemologies and objectives. In this case, it was used to test the research question in a deductive approach in contrast to coding for empirical data.

There are three types of coding that the researcher used during the data analysis section of this research.

Interpretation or analytical coding – this coding allowed the researcher to make sense of the data from the questionnaire responses that the researcher can reflect on afterward.

The second type of coding used is "Attribute coding" which enabled the researcher to examine participants age and gender explain through quantitative data; this was important for the researcher to know these details about the participants because some cybercrimes are linked by these factors (Mallette and Saldaña, 2019).

The third coding used was “Participant own words coding”. Throughout the data analysis, numerous quotes were used to compare with each other for each question. They were contrasted against each other to show differing views of the respondents then summarised as in grounded theory (Corbin and Strauss, as cited by Parameswaran, Ozawa-Kirk and Latendresse, 2019).

Triangulation

Triangulation involves using multiple methods or data sources for qualitative research; here, the researcher used three case studies within the literature review. All three studies highlight examples of when the UK and Canadian governments have failed to protect their vulnerable citizens from cybercrime.

Limitations of the Study

There were some limitations to the online questionnaire that needed to be acknowledged when researching the dissertation. The main drawback was the design of the online questionnaire's questions; the researcher needed to ensure that the questions were not biased for or against either country and also ensure that questions did not offend or discriminate against anyone participating in the online questionnaire.

Another limitation of using online questionnaire is that the researcher is not present to explain any of the process of the questions. This may result in some questions being avoided or where short answers may be given as the participants do not understand the question and the researcher was unable to explain the questions to them in person (Duffy, et al, 2005). To overcome this limitation, the researcher can place his email address at the start of the online questionnaire; participants can email the investigator about any issues of the questionnaire.

Covid 19 limitations

Due to the COVID-19 virus pandemic, many resources for the secondary research were not available, for example, the University of Wales Trinity Saint David (UWTSD) library was closed due to health and safety guidelines. Although the university library offered online services, there were library server issues due to the large number of other students trying to connect to services and the researcher did report it to the correct services. This was a COVID-19 limitation. As a consequence it was necessary to use Google Scholar to find research on the study question.

Secondly, there was a UWTSD statement preventing researchers from conducting face-to-face interviews because of Covid 19 (UWTSD, 2020). Also, there were government lockdown rules in place at the time when the research took place. However, interviews were still allowed but they had to be completed online using Microsoft Teams or Zoom.

All teaching elements for the dissertation had to be delivered online which was a further limitation to the research. The online workshops consisted of PowerPoint presentations which had a pre-recorded voice of the university lecturer, so this meant that no one was able to ask live questions and so it became necessary to send emails to resolve queries.

Regarding the remote dissertation meetings, the student was not able to direct any issues to his dissertation supervisor in person, however, the university did offer online support where guidance could be obtained from the dissertation supervisor about any issues. However, there was a number of delays as it took time to arrange these meetings with the supervisor. As a result of this, this was slower progress than in person, this being another Covid 19 limitation.

Ethics

Before participants took part in the online questionnaire, they signed a consent form declaring that they were happy to take part in the study during the study. It was important that participants stayed anonymous due to the sensitive nature of the information that was shared between researcher and participants, which included confidential information. Before the test was given there was an online test survey given to the researcher's friends and family before the actual model was realised to the public. This was done so that changes could be made to the online questionnaire if there were any faults in the test raised by friends or family during the test phase. At the end of the Online questionnaire, the participants were invited to receive a copy if they so wished once the dissertation had been completed.

The participants who wanted to have a copy of the finished paper had to provide their email address at the end of the Online questionnaire, the email address was then added to a word document before being placed in a key Pass protection.

Chapter 4 Data Analysis

4.1 Introduction

This research dissertation is evaluating the United Kingdom (UK) & Canada's Cybercrime Policies, whether they protect vulnerable people and whether they are relevant in today's society. The dissertation viewed many different papers and documents of authors who looked into this subject before the researcher itself. Currently, the UK & Canadian governments have been working towards ensuring that their citizens are safe from any sort of danger from the cyber world. For the primary research, the researcher developed a 20-question online questionnaire using the Google Documents platform instead of using online questionnaire Monkey due to its limitations, the researcher received 87 replies from people online. However, there was one respondent who took it upon themselves to insult the researcher and their work this respondent's answers will be ignored. The results are based on 86 responses. An analysis of all the primary research is shown below.

4.2 Findings

Q1. Are you the UK or Canadian Citizen? What nationality are you? UK Canada Other

As seen above, Fig. 1 shows a pie chart of the number of people that took part in the online questionnaire. Within this, 54.5% that took part in the survey are people from the UK, while the second-highest group is Canadians which was 32.2% and 10.2 % represents others from any other country. This means that the highest number of responses came from citizens from the UK; however, the researcher did a post on Canadian Facebook social media sites and asked family members and friends from UK and Canada. This shows that a fair balance of attempts was made to

obtain responses from both countries.

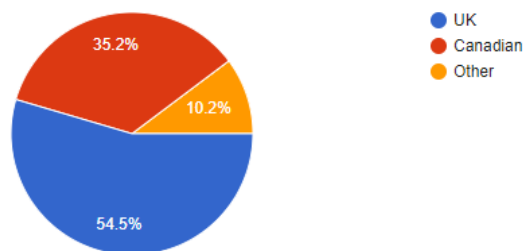


Figure 10 Obtain responses from both countries.

Q2. Age of Respondents

The age range of the people taking part in the survey varies in different ages, the highest age group

being 18 -25-year-olds, this means that age range will likely know more about the cybercrime compared to second which is the group range of 51 plus and over, which is deemed to be one of the groups who are

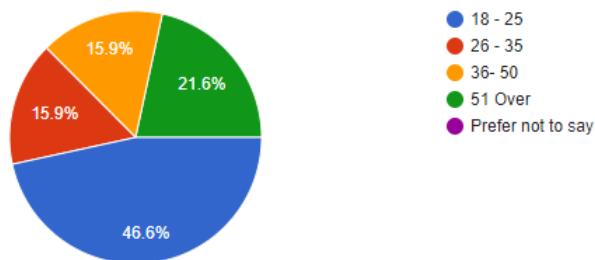


Figure 11 Age Groups

unaware of cybercrime and what it is. The third group being joint third are people aged of 26-35 & 36-50 which both resulted with 15.9%; both age groups should be aware of what cybercrime is and some may know what they are dealing with e.g., it could be someone in that field of work.

Q3. Respondents by Gender

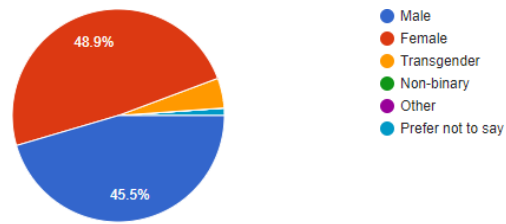


Figure 12 Genders Groups

The largest gender group who responded to this online questionnaire is females with 43 females replying to the online questionnaire, while the second

largest group were 40 who identified as male. Only three people declared themselves as transgender; this was a disappointing result as the researcher believes that transgender people are also one of the highest groups to be vulnerable to cybercrime especially cyberbullying - there has been some research from America that implies this link (Hinduja & Patchin, 2011).

Q4. Diversity of respondents

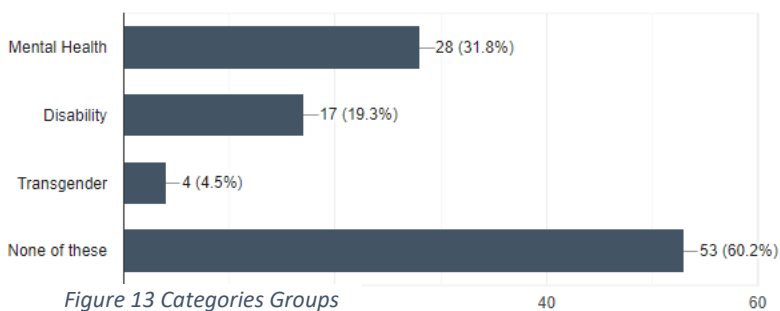


Figure 13 Categories Groups

Apart from children and older people, there are also diversities which include mental health, disability, and transgender, who are vulnerable to cybercrime. Fig. 4 shows how the

respondents are made up of these groups when responding to this questionnaire. It shows that 53 people that took part in the online questionnaire fall outside these categories; the second highest being mental health 28, then disability 17 and transgender 4.

Q 5 Understanding of the term vulnerable individual

When given this question 72 out of 86 the respondents gave the same answers on what they define the term vulnerable person or individual.

R41 stated, "Those who are at risk, like cancer survivors or people with really bad mental health or disabilities."

R50 said, "An individual who, through lack of education, mental or physical capacity, or access to information, is unable to make good decisions on issues affecting their well-being."

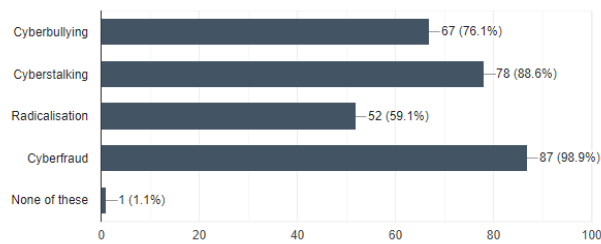
R51 "A person who, because of age or physical/mental disability, cannot protect their interests".

R80 believes that the term vulnerable individual is "An individual who is at risk mentally or physically."

R87 "A person how doesn't have the capacity even mental, physically or socially to take care of themselves and/or other people may take advantage of easy."

The reason why these five respondents' answers were picked was that they all are similar to each other and are the ones closest to Chesnay & Anderson (2008) who define a vulnerable person as someone likely to be influenced or harmed by a particular individual or communities. From a public perspective, this means that the term vulnerable individual is someone who suffers from mental health and/or physical disabilities and is unable to have a normal daily life without having support put into place. which under the UK Government Equity act 2010 states that a person who has a disability has the following suffers from mental health or physical health issues (Home Office,2020). Another point to make as well is R87 who states that the vulnerable person is also easy to be taken advantage of as well. This links back to the theory that many terrorist groups will target as they know they do anything because their vulnerable, the theory comes from Torok's (2007) who stated that terrorist groups tend to target young males who are in university in the UK.

Q6 Types of Cybercrime



People were asked to explain what they believe cybercrime includes. Although some do not have any knowledge of the area, a lot of people believed that cybercrime only consists of cyberfraud as it is one of the most common types of

Figure 14 Types of Cybercrime

cybercrime around the world. However, most listed cyberfraud, but different forms of cybercrime exist, for example, cyberbullying is part of cybercrime but a different form of it. It is very unlikely that people have heard of it because it tends to be a crime committed by younger people who may still be in the education system.

Q7. Opinions on whether cybercrime is a current threat

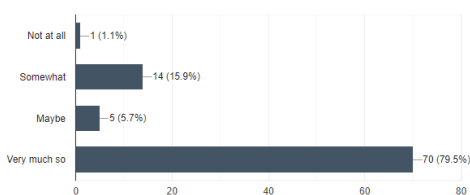


Figure 15 Cybercrime a Threat

Fig. 15 shows what the responders thought about cybercrime as a threat today, 70 (79.5%) believed it was a threat while some responders 14 (15.9%) of them believed it was a realistic threat in today's world. While one person thought it was nothing to worried about while another

person may be believed it was the art into worlds. This shows that the responders believe that cybercrime is a threat in our society today and action should be taken; while the other person believes that cybercrime may be a threat in today society and government should be relaxed about it and the final comment that cybercrime is no threat in today society and both governments should not worry about it. Currently, there is no cybercrime threat level chart for the UK or Canada, however, both nations have security threat levels for terrorism which informs the public. Currently, the UK is at a 'severe' level which means an attack is likely (MI5, 2021). In contrast, the Canada terrorism level is at 'Medium' meaning an attack could happen (Government of Canada, 2018).

Q 8. Impact of a personal cybercrime incident

Out of the 86 respondents, only 23 stated that they were involved in some sort of cybercrime incident; a small number of them gave details on what happened.

R48 “Yes, cyberstalking. Found out my address, where I lived etc, and followed me to my house. I was a lot younger than them as a young woman felt extremely vulnerable.”

R9 “Depends on your view of cyber harassment”.

R48 & R9 are both from the UK one is female and the other is male, both respondents had experienced cyber-harassment. This links with a government report by Davidson et al., (2019) which argues that females are likely to be harassed and cyber-stalked by other people e.g., males, however, R9 is a male who suffered a similar experience. This supports Davidson et al’s theory that females are more likely to be cyberstalked does have flaws as they did not acknowledge that males could also be victims of cyberstalking.

R16 “Yes. A fellow Etsy seller made up fake names and emails, purchased low-priced items from me, and then gave me bad reviews. Yes, I felt vulnerable.”

R19 “yes my father-in-law almost got caught with believing that he needed to send money to someone in another country to help them”

R33 “Online purchases. cyber fraud”.

R62 “Yes. My wife’s bank account information was skimmed. She did not feel vulnerable as the matter was discovered quickly and resolved by the bank.”

R74 “Credit card fraud. When I spoke to the bank I asked if there was anything, I could have done to be safer. They said no. I do not feel vulnerable. It is just a fact of life now that someone will steal your shit on the internet at some point. That’s why we have insurance.”

Many of the 23 respondents explained that they or a family member dealt with cyber fraud many times, R74, a female Canadian, made an interesting comment, saying that their money is “insurance” so that if cyber fraud does occur, the insurance company will be able to pay them compensation.

R16 & R74 reported that they both felt vulnerable at the time of the incidents as they also felt nothing could be done about their cases. This shows that the public’s confidence is affected by cyber fraud.

Q9. How many times have you been involved in a cybercrime incident?

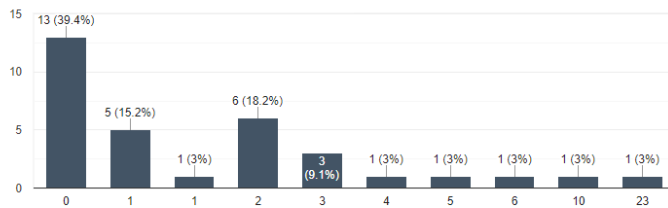


Figure 16 Involved in a cybercrime incident

Fig. 16 shows the responses that when asked how many times people were involved in cybercrime incidents, the responses varied. Whilst most of the respondents indicated no experience

(13), other answers ranged between once (6 respondents), to 23 times for the highest (1 person). Here the researcher has assumed that due to the high number of recurrences for those with 3 or more instances of cybercrime, the individuals must be doing something wrong as they have been targeted so many times by cybercriminals. However, the individuals have not stated what happened, only that they have been involved in cybercrime incidents so is difficult to acknowledge what has happened - it could be from cyberbullying to cyberfraud. In contrast, the people who experienced it once or twice have must have taken advice from the police or reported it to them to deal with it.

Q 10. Handling of cybercrime incidents by the police

When respondents were asked how the police services dealt with their case, only a handful gave answers about their experience.

R16 "The police will only investigate if they think it is a large-scale operation".

R21 "I haven't contacted the police".

R24 "phishing emails, I did not respond, to email and just deleted the emails, bit clicking on the link".

R33 "Didn't call".

R38 "Did not contact police".

R50 ", they barely understand the issue and if they do, you aren't going to be put high on their priority lists."

The above five respondents that were selected from the number of responses all explain how the police services did not understand how serious their cases were, for example, R50 explains how the police did not understand them and what they were going through at the time. This does link with the argument that many police forces still do not understand cybercrime; this also aligns with the case study of Breck (2015) when the police force did not understand Breck's parents' concerns.

R21, R33, and R38 all gave similar answers to this question which was not to bother calling the police at all about their case; this agrees with the Netherlands (2018) Government research that many of the victims do not call the police as they do not see it necessary to take legal action regarding their cases. Overall, the responses are negative about how the police services responded to these cases.

Q 11. Number of times police were contacted about cybercrime incidents

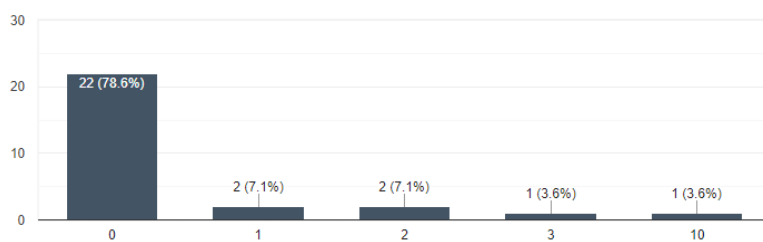


Figure 17 Number of times police were contacted about cybercrime incidents

The bar chart shown in Fig. X on the X-axis shows how many times people tried to contact the police about their cybercrime incidents. The Y-axis shows that 22 people did not contact the police at all following their incident; while only 2 people contacted them

once. Two victims called the police twice, 1 one-person called three times, and one person ten times. The highest amount relates to the 22 respondents who did not contact the police at all about their cybercrime incident. This links with the CBS (2019) research in which the Dutch police argued that many people did not contact them; they believe it is to do with victims' banks can sort out the fraud issue before legal action is taken as many of the cybercrime incidents in the Netherlands are related to financial fraud.

Q 12. Charities approached for support

Of the respondents who replied to this question, they explained that many of the charities like Victim Support did not contact them after the incident was reported to the police, neither did the police service give advice or contact details about the charities themselves.

R88 stated due to their behaviour, they do not want to share information with others:

“No, I got a stubborn nature, I don't like letting people know my issue as I scared they would laugh and shrug it off or look down on me ... effectively my conditions make me scared and give me anxiety around in social and people I don't know”.

For this person, contacting the police is a challenge as they suffer from anxiety, so describing their situation would be hard for them to explain; unfortunately, due to their reluctance to come forward,

the person would not be able to get the support they needed unless the police provide some sort of support.

Q 13. Effectiveness of the police in combatting cybercrime

People were asked how they think the police are currently dealing with cybercrime:

R2. "No, because cybercrime teams are very small."

R3 "No, more can be done to make others aware of what to look out for in cybercrime."

R4 "I believe so, the police are beginning to adapt to the changing environment of social media platforms and other issues on the Internet".

R6 "No. Lack of resource / finance. The pace at which cybercrime is developing and moving, and the sheer volume of organised criminal groups now involved in perpetrating these crimes means local and national forces like NCA cybercrime division have little resource to trave down all such incidence. Also, banks/financial institutions have also taken an historical lax attitude to wanting to investigate or support prosecution. Many hides behind the veil of AML tick box policies and raising SARS. This had led to exponential growth in financial cybercrime/scams, and now lack of controls on many social media platforms continue to perpetuate the problem."

R21 "Yes they are always playing catch up with criminals".

R48 "No I do not think they are doing enough. They do put effort and resources into investigating cybercrime, but it is definitely a problem which is much bigger than anyone realises. The many types of cybercrime and the vast number of different ways these crimes can be committed means it must be difficult for the police to investigate these matters and keep on top of it. There also doesn't seem to be many police officers trained specifically to deal with cybercrimes."

R85 "Yes. I don't think there's much more that they can do. Cybercrime is difficult to regulate/monitor".

R2,R3 & R4 all believe that that the police services are doing the best they can during this time for example R4 explains that is not the police service's fault due to austerity and lack of resources to deal with growing cases of cybercrime; R4 is British - this links with the ten years of public sector budget cuts. Although there is nothing in the literature review to back up this comment, there is a recent article from the CIPFA that backs R4's comments about the police services having a lack of resources and money to deal with cybercrime (CIPFA, 2019).

While R21 & R85 believe that police services should be doing more to combat cybercrime, R21 stated that the police are always playing "catch up", whilst R85 said it is challenging for them to

catch the criminals at all due to the nature of the crimes. R85 backs up a comment made by the media in 2018 stating that the police in the UK are having to catch up with the offenders, the main argument again being that police resources and budgets are insufficient to deal with cybercrime (Dodd,2018). This means UK police and Canadian police are always playing catch up with the offenders because of the lack of resources; however, the Canadian government will give RCMP more resources to the police force.

Q 14. UK Government strategies to protect vulnerable people from cybercrime

UK respondents given this question indicated that many citizens believe that the UK government should make people more aware of cybercrime policies and how they are protecting its residents.

R6 “1. Provide more resources to local forces to not only investigate but also to work with other partners on education (initiatives like friends against scams etc); 2. Make telecoms companies, ISPs, and financial institutions and payment providers more accountable through legislative changes.”

R9 “Work together with individuals and organisations to help ensure a safe and secure cyberspace for all”.

R20 “Provide more training courses for vulnerable people to identify if they are a victim of cybercrime and also ways in which they can protect themselves online.”

R86 “Protecting, amending, or adding rights and protection to vulnerable individuals/group in society”.

These four answers stand out because R6 & R9 believe that the government should be working with other services such as the UK police forces and other services in the cybercrime industry, such as GCHQ. R6 makes it clear that there should be new legal work that allows the telecom companies, financial institutions, and payment providers more accountable. R9 and R6 both agree that all the services in the cyber world should work together to ensure a safer place is made for UK citizens. R20 & R86 make very good points about what should be done which is to provide a training course for people who are vulnerable to ensure that the groups will be aware of the signs of cybercrime. This means that vulnerable groups like children, the elderly, and other groups should be educated about the signs of cybercrime, for example, young children should be taught about cybercrime and the risks of online grooming.

Q 15. Opinions on what the Canadian government should be doing to protect vulnerable people adequately from cybercrime

As for Q14, this question asks Canadian citizens what their government could do to improve to combat cybercrime and protect vulnerable people.

R2 "Take more action against cybercriminals by targeting them individually"

R16 "Hire more cybercrimes investigators."

R28 "television information clips on phishing emails, malware, and phone calls asking for private information, Scenarios to warn the general public. maybe same for school students as well in the school system."

R50 "Beat it at its source. Use regulations to punish or enforce companies that allow these crimes to happen using their networks or infrastructure."

R62 "Education. Helping to prevent it from happening."

Like the UK citizens, the Canadian people also believe more resources are needed for the police forces to combat cybercrime; for example, R2 & R16 both stated that action is needed to address cybercrime, and to do so the Canadian police force needs more resources to combat it. Recently, the Canadian government announced that as part of the cybercrime policy, it will increase the number of cybercrime officers (Government of Canada, 2019). In contrast, R28, R50 & R62 suggest that the government of Canada should ensure that people are educated about cybercrime and the warning signs of this. R28 commented that by using TV, posters, and through education, it would be an innovative idea to be taught in schools as children are one of the groups to be vulnerable to cybercrime. Therefore, this shows that people should be made more aware of the risks of cybercrime.

Q 16. How UK & Canadian governments can inform the public of measures to protect vulnerable people from cybercrime

Respondents were asked should the UK & Canadian governments explain what they are doing to protect their people from cybercrime especially vulnerable people.

R3 "Yes because this could reduce the amount of crime that happens."

R4 "Yes, because the government need to explain what the measures will do and how they will reduce cybercrime".

R30 “No to keep ahead of the perpetrators”

R36 “Yes, and how they'll protect the more vulnerable.”

R 38 “Yes. Data transparency should be a basic right, and a government should be able to demonstrate a basic level of respect for an individual's privacy. Cybercrime laws are naturally going to infringe on that right to privacy, so the government needs to be open and honest about how data is handled and by whom. It's no different from offering to check a vulnerable person's locks to make sure they're safe and secure but having the common decency and professionalism not to judge.”

R61 “No. Don't want fraudsters to see the tactics that are being applied.”

Many of the respondents agreed that both governments should be explaining how they are protecting the citizens within each nation,

For example, R3, R4, R36 & R38 believe that governments should explain what is happening about the policies and how they should be protected.

However, the Home Office (2019) has updated its strategy which is the Online Harms White Paper which will progress through Parliament in 2021. Similarly, the Canadian government has developed a policy for the next four years. However, some of the people who took part believe that governments should not share what each is doing about cybercrime and protecting vulnerable people. A reason for this could be that people may not want the government to release information about their secret policies. So, this infers that both governments should release only a limited amount of information e.g., how they will protect vulnerable people while retaining sensitive information that should be kept a secret within both governments and associated security services.

Q 17. Parental responsibility for their children's online activities (up to the age of 15)

The reason why people were given this question linked with a case study in the literature review which was about Shamima Begum. It is a debatable topic whether her parents should be held responsible for her actions. There is evidence in the Online Harms White Paper that many of the social media companies in the UK believe that parents should be held responsible for their children's actions.

R16 “Yes. If parents are held responsible, some of these crimes can be averted.”

R19 “Yes, they are responsible for that child and should be aware of what they do online. The internet can be very dangerous and young children should be monitored for their safety”.

R33 "Yes I think so, but at 15 that might be too old."

R35 "No. They can't be held criminally responsible for the actions of another person."

R45 "No. It is impossible to expect that parents can control their children's online activities at all times. Kids have access to the internet in all aspects of their lives and couldn't be controlled by their parents."

Many people agree that parents should be held responsible for their children's actions as they are still under their care, however in the UK the criminal age of responsibility is 10 which makes it challenging for the parents, whilst in Canada, it is 21. Some people disagree that parents should be held responsible for their children's actions at the age of 15 years old, with R35 & R45 saying it would be too difficult for the parents to police their children as the children will have more understanding about technology than their parents. This means that responders agree with the Online Harm White Paper about parents taking responsibility for their children's action while online.

Q. 18. Opinions on whether Shamima Begum should be allowed to re-enter the UK following her involvement with ISIS

In the UK, there is a fierce debate by the government and Law enforcement about whether Shamima Begum should be allowed to come back to the UK. Currently, the UK Government has denied her re-entry, but there has been a ruling from the Court of Appeal (BBC News,2020). However, in cybercrime terms, Shamima Begum was groomed by ISIS members as a recruit to support their cause as she was promised numerous possessions and a better life in Syria. Many of the respondents agreed with the UK government's decision to deny her return. Here, a handful believes she should be permitted to return to the UK with an appropriate penalty and rehabilitation support.

R2 "Definitely no, she gave up her citizenship to join an enemy of the UK".

R8 "Yes, after undergoing rehabilitation and a full psychological assessment."

R10 "No, willingly joins an extremist group that have been responsible for the deaths of innocents".

R11 "No, she poses risk to carry out the same crime again."

R31 "Yes she should be allowed to return. The girl was radicalised and ran away at 15 believing rubbish being spouted by that hate organisation. She should be put on trial in the UK and after any judgment / prison time has happened rehabilitated. She has been treated worse than Michael Adebolajo who should never leave prison in my opinion for his actions."

R2, R10 & R11 all believe that she is a threat to the UK which she stated during an interview in 2019 where she agreed with some of the ISIS views on bombing innocent people. She admitted that she views it as revenge for other Western governments have done to ISIS (BBC, 2019). This supports people's comments about Shamima Begum being a threat to the UK. Yet, R8 & R31 disagree and would support Shamima Begum's return to the UK as long she had an appropriate rehabilitation treatment, was dealt with by the UK justice system to spend time in prison. Again, in her BBC interview, she agreed to action by the UK justice system and rehabilitation if allowed back.

Q 19. Views on the UK Online Harm White paper and the Canadian National Cyber Security Action Plan (2019-2024)

The majority of the respondents were not aware of the Online Harms White Paper for the UK and The National Cyber Security Action Plan. A very small number (2) knew what they were to be able to comment:

R9 "The U.K. online harm white paper is quite informative but very long which may turn people against wanting to read it all and learn about cybersecurity"

R15 "Nothing."

R17 "Nothing"

R20 "I don't know anything"

R25 "I believe it is a new action plan to providing a safer internet. Primarily aimed at children."

It is concerning that people are unaware what the UK & Canadian governments are doing to protect their citizens, while some people do, for example R9 knew what it was about and believed that the Online Harm White Paper is too lengthy which will put off readers. This could be one of the reasons that people do not know what it is about.

Q20. Opinions on what the UK & Canadian governments should be doing about the current Cybercrime legislation

The final question was asking what the UK & Canadian governments should be doing about their current cybercrime legislation. Many of the respondents believe that the legislation should be updated.

R9 "I think there needs to be a lot of change for example: The 1990 freedom of information act currently exposes cyber professionals to prosecution if they carry out certain research against cyber criminals, it also doesn't have any proper law enforcement as there is still need for a warrant to prosecute."

R13 “Making harsher laws”

R20 “Many people don’t know anything about the legislation, so I believe that they should inform and educate individuals about it first. Some young people do not know what is legal and what is not.”

R24 “reinforcing this to better protect individuals from becoming prey to cyber criminals.”

R88 “Giving police powers and resources that they need to combat cybercrime more better”

The respondents argue that the UK & Canadian governments should educate people about cybercrime especially young people which R20 said many of the children in this day and age are unaware of what is legal in their view.

4.3 Summary of findings

summary -to do link to your objectives and lit reviews.

The findings section explains every questionnaire in detail about the research that was carried out by the researcher, the findings show interesting comments on what people think about the current policies of both governments & what both governments are doing to combat this issue. The findings section also compare the comments stated by the participant with each other and then evaluated by the researcher; the findings sections also show how many people are unaware of what government policies are out there to protect themselves from harm while they are online. the questionnaire.

Chapter 5 Discussion, Conclusion, and Recommendations

5.1 Introduction

This section of the dissertation will discuss the results of the finding and further information from the literature review; also in this section, there will be a part which talks about the Online Harm White Paper and what stage it is at this time. This section will also be looking into the conclusion of the findings itself from the questionnaire. At the end of the conclusion, there will be recommendations on what the government could do in the future to protect its citizens from a cybercrime attack.

5.2 Discussion

The main research question for the study was to determine whether the current UK & Canada cybercrime policies protect vulnerable people. Whilst the current legislation in the UK which is the strategy 2016-2021 does not specifically protect these diverse groups; the Online Harms White Paper (2019) certainly does seek to protect those people who are vulnerable. Currently this is at the stage where it will transform into law (Home Office, 2019). Recently, the bill returned to the House of Commons with amendments made to it prior to royal assent (BBC News, 2020). In contrast, whilst Canada has expanded the powers of the RCMP to include cybercrime training and teams being established, there is no policy to protect vulnerable people (RCMP, 2020).

The strength of this dissertation is it is the first of its kind, there have been no other research papers written on this subject before this has allowed the dissertation to provide different points of views on the subject area from the public's view to how the government can improve their policy in protecting vulnerable people from cybercrime. A second strength of the study is its comparison of how the governments of the UK & Canada and their security services protect people from harm. The dissertation also makes a comparison between the policies of the two countries being examined and also indicates where the two countries can learn from each other.

There have been however some weakness of the dissertation, the pandemic (COVID-19) many lockdowns have made it difficult for the researcher to do physical face to face research for example going into a police station to ask about cybercrime figures; however, while the researcher could have emailed the police, it would have taken time and need to approval from the university and police force due to safety measures which would have taken more time and waiting. The second problem with the dissertation is the lack of information on Canadian law about cybercrime due to the researcher coming from the UK, even though the government website of Canada does Possess useful information. During gathering questionnaires, there was a lack of transgender participation

which diluted the finding meaning that there was no way of the researcher being able to reach an answer with regards to their vulnerability to cybercrime.

There are several improvements that could have been made to the dissertation such as a greater volume of participants answering the online questionnaire, an increased volume of answers would have resulted in a wider range of views from contributors such as greater clarity on how local police force work in preventing cybercrime.

The advertisement of the questionnaire could have been more inclusive of the transgender community, the views of the transgender community were lacking which meant that the researcher was unable to conclude if a transgender person were at an increased risk of being bullied online compare to other groups due to their lifestyle. Had there been greater transgender participation it would have been possible to compare with other research papers and discover if they are supported by current finding.

Difficulties faced during research, during the investigation there was a tight time frame in which to conduct the research in however with good planning this risk was minimised and presented only small risk overtime. The timeframe of the dissertation was altered however due to COVID-19, the pandemic required many alterations to be made to not only the timetable but how the research was conducted as most common research practices such as face to face interview could not be conducted so other methods had to be used which could be both time consuming and laborious.

5.3 Data reliability

The data is reliable as 86 out of 87 participants took their time to answer all questions within the entire questionnaire. This should have taken respondents around 15 minutes to complete according to the test timing by the researcher. From this investment of time, it can be assumed that many of the participants answered the questions truthfully. However, one participant indicated that the research was pointless, did not answer the questions correctly, and used aggressive behaviour towards the researcher. This respondent's answers were therefore discounted from the study.

5.4 Data validity

Data validity is important in terms of the design of the investigation; by following the research onion, time and effort were spent planning the questionnaire so that the responses would be both quantitative and qualitative in content. The questionnaire was administered in a way so that participants were able to give their views and opinions openly about the topics. The researcher was happy with the overall response to his questionnaire as many of the participants gave a good amount of detail within their answers.

5.5 Deductive approach

A deductive approach is normally linked with a hypothesis, this approach will always relate to qualitative research (Hyde,2000). The researcher will first develop a hypothesis linked to academic theory; the second step to the research is to analysis the data for their findings section. The final step to the deductive approach is to analyse the findings, evaluate and interpret what this means to form a conclusion of their findings.

5.6 Conclusion

The research question examined the cybercrime policies for the UK and Canada and whether these protect specific groups of vulnerable people. It was found that whilst the UK and Canada are providing strategies and resources, these are not sufficient for vulnerable people including children. There continue to be reported cases relating to cyber fraud, online grooming.

From the primary research, the case studies and literature review allowed the overall aim and all objectives for the study to be met.

The data was valid and reliable for use as the qualitative answers were written in detail and the participants took their time. These responses can be seen as truthful and therefore reliable.

In conclusion, the results of the findings suggest that people who suffer from mental health and disability are more likely to be vulnerable to cybercrime alongside children and the elderly. However, many of the respondents to the online questionnaire without mental health issues or disabilities have also fallen victim to cybercrime as well.

From the number of occasions that respondents fell victim to cybercrime and from the views of those who responded to the survey, it shows that respondents believe that cybercrime is a significant threat today and should be taken seriously by both the UK and Canadian governments.

What was expected was participants strongly supported the UK & Canadian police being given more resources and funding to tackle cybercrime, alongside harsher punishments for offenders; the lack of resources can be attributed to cuts that both governments made during the global financial crisis.

A common issue raised by the contributors that were affected by cybercrime was the lack of police sympathy over the cause of the incident which resulted in some of them not contacting the police, this often has a knock-on effect, the lack of crime reports can lead to a dearth of knowledge on cybercrime resulting in the department of cybercrime being targeted for budget cuts. This lack of sympathy extends to the charitable sector where there has been a lack of support for the victims of cybercrime by charities.

Many of the respondents believe that both governments should clarify to the public what they are doing to protect them though not without jeopardising police procedures on combatting cybercrime e.g., “how to combat cyber terrorism”.

One of the questions, (Q 17) asked if parents should be held responsible for their child’s actions when online, for example, the Online Harms white paper report discusses who should be held responsible for their children; many people believe that parents should be held responsible for their children’s actions instead of placing the blame on social media companies.

What stood out was many of the participants from the UK & Canada were not aware of the Online Harms White Paper or Canadian National Cyber Security Action Plan (2019-2024) as both documents are important pieces, especially the Online Harm White Paper has been in the news for the past couple of years because of its debates in the House of common and in the Houses of Lords. The researcher could understand about the Canadian participants maybe not being unaware of the Canadian National Cyber Security Action Plan (2019-2024) as it is a document that some people would probably not search online. another piece that stood out for the researcher was the amount of some of the participants did not state the type of cybercrime they were involved in, this is understandable some people would like to keep it private; however it would have been useful if the researcher could have known the issue.

From the responses, there were only 4 respondents who regarded themselves as transgender. Worryingly, two of these had personal experience of cyberbullying. There were 17 who declared a disability and 28 with mental health problems. Of these, 5 reported the same experience for disability and 9 for mental health, respectively. Six respondents declared two or more factors relating to disability, transgender, or mental health. When compared with 53 neuro-typical individuals (no difference), there were 16 who reported the same experience.

Hopefully, this research will make people more aware of the types of cybercrime that exist in the digital world and will give more people an understanding of the signs of cybercrime for example cyber- stickering and online grooming. This research will also give the public an understanding of how the police & the government are trying to protect them from cybercrime along with how governments' strategies work to protect business and people.

This research could be beneficial to the educational sector. Importantly, the UK & Canadian government strategy plans are to protect businesses, however, this research is focused on protecting the vulnerable public within the UK & Canada. Both government and police will benefit from this dissertation, first, the police will be able to review areas where they can improve on e.g.,

someone people from the finding section thought the police were not approachable when talking about their incident. While for the government they can evaluate how they can improve in areas of weakness e. g., give the police more resources & bring in new cyber legislation to combat evolving cybercrime.

5.7 Recommendations

1. That both the UK & Canada should update their cybercrime legislation in line with the Online Harms White Paper.
2. Both the UK and Canadian governments should provide more funding to their police services and especially the UK police to combat cybercrime, this would mean that the police services would have more resources to combat cybercrime hopefully reducing it.
3. That the UK & Canadian police services need to train their police to understand cybercrime as many of the victims in the online questionnaire stated how they felt scared of talking to the police officers about the incident as they have felt guilty themselves. Such training would lead to more people reporting cybercrime to the police without feeling very uncomfortable reporting it.
4. Both nations to run awareness/information to the public about the dangers of cybercrime to vulnerable groups e.g., young people and the elderly, they could accomplish this through television (TV) adverts or anti-cyberbullying classes that can be done in the school system, free prevention classes for elderly or online. This could mean that many crimes such as online grooming, online child pornography, phone, and email scams could be reported easily and dealt with quickly.
5. Although charities offer excellent support to victims of cybercrime incidents and also provide information for the public about cybercrime topics. However, charities & police need to improve working together and sharing information, possibly within an automatic opt-in scheme.

6. UK Banks & police services need to work together when cyberfraud occurs to victims' accounts; this means the police would have a better understanding of how cybercrime works and how they could combat it in the future.

References

- Arkkelin, D (2014) Using SPSS to Understand Research and Data Analysis, Valparaiso, Indiana: Valparaiso University.
- Andrews, D , Nonnecke, B , Preece J (2010) Electronic Survey Methodology: A Case Study in Reaching Hard-to-Involve Internet Users, International Journal of Human–Computer Interaction, 16(3),pp 185-210 . Available at: <https://psycnet.apa.org/record/2003-09369-004> (Accessed: 21 July 2020).
- BBC News (2016) Breck Bednar murder: Killer 'contacts victim's mother', Available at: <https://www.bbc.co.uk/news/uk-england-essex-35413240> (Accessed: 24 August 2020).
- BBC News (2019) Shamima Begum: 'I didn't want to be IS poster girl', Available at: <https://www.bbc.co.uk/news/uk-47276572> (Accessed: 24 August 2020).
- BBC News (2019) Hate crimes recorded by police up 10% , Available at: <https://www.bbc.co.uk/news/uk-50054915> (Accessed: 21 September 2020).
- BBC News (2019) Mental health: UK could ban social media over suicide images, minister warns Available at: <https://www.bbc.co.uk/news/uk-47019912> (Accessed: 21 September 2020).
- BBC News (2020) Shamima Begum can return to UK to fight for citizenship, Court of Appeal rules Available at: <https://www.bbc.co.uk/news/uk-53427197> (Accessed: 19 December 2020).
- BBC News (2020) Online harms law to let regulator block apps in UK Available at: <https://www.bbc.co.uk/news/technology-55302431> (Accessed: 28 February 2021).
- BBC News (2016) Child protection body failed over paedophile reports Available at: <https://www.bbc.co.uk/news/uk-37616825> (Accessed: 28 January 2021).
- Breck Foundation (2020) Our Work, Available at: <https://www.breckfoundation.org/> (Accessed: 24 August 2020).
- Bishop,J (2012) 'The art of trolling law enforcement: a review and model for implementing 'flame trolling' legislation enacted in Great Britain (1981– 2012)', International Review of Law, Computers & Technology, 2013, 27(3), pp. 301-318 [Online]. Available at: <https://www.tandfonline.com/doi/abs/10.1080/13600869.2013.796706> (Accessed: 12 September 2020).

Broll,R Huey,L (2015) 'Just being mean to somebody isnt a police matter:Police perspectives on Policing Cyberbullying ', Journal of School Violence , 14(2), pp. 155-176 [Online]. Available https://www.researchgate.net/publication/271992514_Just_Being_Mean_to_Somebody_Isn't_a_Police_Matter_Police_Perspectives_on_Policing_Cyberbullying (Accessed: 12 September 2020).

Biggam,J (2011) Succeeding with your master's dissertation: a step-by-step handbook, 2nd edn., Maidenhead, Berkshire: Open University Press.

Chesney, M. Anderson,B (2008) Caring for the Vulnerable: Perspectives in Nursing Theory, Practice, and Research, Burlington : World Headquarters .

CIPFA (2019) “Achieving finance” Available at: <https://www.cipfa.org/services/achieving-finance-excellence-in-policing> (Accessed: 16 December 2020).

excellence in policing

CBC (2020) Students, experts call for explanation after York University suffers 'extremely serious' cyber-attack, Available at: <https://www.cbc.ca/news/canada/toronto/york-university-cyber-attack-1.5555106> (Accessed: 24 August 2020).

CBS (2019) 1.2 million cybercrime victims, Available at: <https://www.cbs.nl/en-gb/news/2019/29/1-2-million-cybercrime-victims> (Accessed: 09 July 2020).

Chesney,M Anderson,B (2008) Caring for the Vulnerable: Perspectives in Nursing Theory, Practice, and Research, Burlington : World Headquarters.

The Children’s Commissioner (2018) Who Know What About Me? Available at: <https://www.childrenscommissioner.gov.uk/digital/who-knows-what-about-me/> (Accessed:21 September 2020).

CPS (2018) Stalking and Harassment, Available at: <https://www.cps.gov.uk/legal-guidance/stalking-and-harassment> (Accessed: 18 September 2020).

CPS (2020) Cyber / online crime, Available at: <https://www.cps.gov.uk/cyber-online-crime> (Accessed: 10 July 2020).

CPS (2020) Cybercrime - prosecution guidance, Available at: <https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance#:~:text=a%20cybercrime%20case.-> (Accessed: 09 July 2020).

CPS (2017) Terrorism Available at: <https://www.cps.gov.uk/crime-info/terrorism> (Accessed: 14 February 2021).

Citizen advice, (2020) Pregnancy and maternity discrimination, Available at: <https://www.citizensadvice.org.uk/law-and-courts/discrimination/what-are-the-different-types-of-discrimination/pregnancy-and-maternity-discrimination/#:~:text=The%20law%20which%20says%20you,the%20Equality%20Act%20is%20unlawful.&text=Pregnancy%20and%20maternity%20discrimination%20is,you've%20recently%20given%20birth.> (Accessed: 20 September 2020).

Citizen advice, (2020) Race discrimination Available at: <https://www.citizensadvice.org.uk/law-and-courts/discrimination/protected-characteristics/race-discrimination/> (Accessed: 20 September 2020).

Citizen advice, (2020) Sexual orientation and transgender identity hate crime Available at: <https://www.citizensadvice.org.uk/law-and-courts/discrimination/hate-crime/sexual-orientation-and-transgender-identity-hate-crime/> (Accessed: 20 September 2020).

Clark, V (2008) The Mixed Methods Reader, London : Sage Publications

Clement, J (2020) Most popular social networks worldwide as of July 2020, ranked by number of active users(in millions), Available at: <https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/> (Accessed: 9 October 2020).

CEOP (2021) Are you worried about online sexual abuse or the way someone has been communicating with you online? Available at: <https://www.ceop.police.uk/safety-centre/> (Accessed: 20 January 2021).

Davidson, J Livingstone, S , Jenkins,S , Gekoski, A, Choak,C,Ike, T, Phillips,K (2019) 'Adult Online Hate, Harassment and Abuse: A rapid evidence assessment', Home Office , 1(1), pp. 40-45 [Online]. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811450/Adult_Online_Harms_Report_2019.pdf (Accessed: 14 September 2020).

Dilipraj, E (2016) 'YAHOO!' FIASCO – A SINKING VESSEL NEEDS NO NAVIGATION', CAPS In Focus ,
(), pp. 1-4 [Online]. Available at:

https://d1wqtxts1xzle7.cloudfront.net/49833843/CAPS_Infocus_DR_22.pdf?1477317860=&response-content-disposition=inline%3B+filename%3DYAHOO_FIASCO_A_SINKING_VESSEL_NEEDS_NO_N.pdf&Expires=1600697990&Signature=R2pvlg-qJVKGeKL5PbbvQz3ZwOrvhfnM0wefsCoWi66pGXGZulgpolyTcZONult888SWoar5xC3ML3MyEFDpoY76y-h1ucCnIWxkYhq4gh9Ktlj1k7jLhw0JMOsKRhTrPqveAFfsDxVTljRZS1RXRkLGqEd7ImJQYxgl4YMgL4EBLVacicGiHFYbZUiAGNfUDvcmbmOjxvYrYOTzhFRkBfUIUvXGUn3Wpl~D6-987x8fxEmvHf3qR~xINz6zUEqubRb2AGXnBVm91RNVWCHDHrFong~sx-A5~p84INwYDwBLX6Z1Hwlir-6lcn30rxYkwfcZ8dR2nFL6qMzY19w_&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA (Accessed: 15 September 2020).

Dermatol, I (2016) Methodology Series Module 3: Cross-sectional Studies Available at:
<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4885177/> (Accessed: 30 July 2020).

Dis, J (2015) Longitudinal studies, Journal of Thoracic Disease, 7 (11), pp 338 - 339 Available at:
<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4669300/> (Accessed: 30 July 2020).

Duffy, B, Smith, K, Terhanian, G, Bremer, J (2005) 'Comparing Data from Online and Face-to-face Surveys', International Journal of Market Research, 47(6), pp. 615-639 [Online]. Available at:
<https://journals.sagepub.com/doi/abs/10.1177/147078530504700602?journalCode=mrea>
(Accessed: 11 October 2020).

Ebneyamini, S, Moghadam, R (2018) 'Toward Developing a Framework for Conducting Case Study Research', International Journal of Qualitative Methods 17 (1), Available at:
<https://journals.sagepub.com/doi/full/10.1177/1609406918817954#:~:text=Case%20Study%20as%20a%20Method,-Despite%20being%20one&text=%E2%80%9CA%20case%20study%20is%20an,1989%2C%201994%2C%202009> (Accessed: 30 July 2020).

Esteves, J Ramalho, E Haro, G (2017) 'To Improve Cybersecurity, Think Like a Hacker', Technology Innovation Management Review; Ottawa, 58(3), pp. 71 - 77 [Online]. Available at: <https://search.proquest.com/docview/1885859523?pq-origsite=gscholar&fromopenview=true> (Accessed: 15 September 2020).

Equality and Human Rights Commission, (2020) Gender reassignment discrimination Available at: <https://www.equalityhumanrights.com/en/advice-and-guidance/gender-reassignmentdiscrimination#:~:text=In%20the%20Equality%20Act%20it,sex%20to%20your%20pREFERRED%20gender> . (Accessed: 20 September 2020).

Equality and Human Rights Commission, (2020) Religion or belief discrimination Available at: <https://www.equalityhumanrights.com/en/advice-and-guidance/religion-or-belief-discrimination> (Accessed: 20 September 2020).

Equality and Human Rights Commission, (2020) Age discrimination Available at: <https://www.equalityhumanrights.com/en/advice-and-guidance/age-discrimination> (Accessed: 20 September 2020).

Feigl, H (2020) Positivism Available at: <https://www.britannica.com/topic/positivism> (Accessed: 30 July 2020).

Fell, J (2017) Hacking through the years: a brief history of cyber crime Available at: <https://eandt.theiet.org/content/articles/2017/03/hacking-through-the-years-a-brief-history-of-cyber-crime/> (Accessed: 20 December 2020).

Geraldi, J (2012) Gantt charts revisited: A critical analysis of its roots and implications to the management of projects today. Available at: <https://www.emerald.com/insight/content/doi/10.1108/17538371211268889/full/html#:~:text=Gantt%20chart%20enables%20a%20clear,move%20to%20a%20next%20task>. (Accessed: 31th July 2020).

Government of Canada (2020) Criminal harassment, Available at: <https://laws-lois.justice.gc.ca/eng/acts/c-46/section-264.html> (Accessed: 15 September 2020).

Government of Canada (2019) National Cyber Security Strategy, Available at: <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf> (Accessed: 21 September 2020).

Government of Canada (2020) Canadian Human Rights Act (R.S.C., 1985, c. H-6) Available at: <https://laws-lois.justice.gc.ca/eng/acts/h-6/> (Accessed: 11 September 2020).

Government of Canada (2020) Cybercrime, Available at:

<https://cyber.gc.ca/en/guidance/cybercrime-0> (Accessed: 09 July 2020).

Government of Canada (2020) National Cyber Security Action Plan (2019-2024) , Available at:

<https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/ntnl-cbr-scrt-strtg-2019/index-en.aspx>

(Accessed: 09 September 2020).

Government of Canada (2018) Canada's National Terrorism Threat Levels Available at:

<https://www.canada.ca/en/services/defence/nationalsecurity/terrorism-threat-level.html>

(Accessed: 21 February 2021).

Government of Canada (2015) Memorializing the Victims of Terrorism Available at:

https://www.justice.gc.ca/eng/rp-pr/cj-jp/victim/rr09_6/p3.html (Accessed: 14 February 2021).

Home Office (2020) Online Harms White Paper - Initial consultation response, Available at:

<https://www.gov.uk/government/consultations/online-harms-white-paper/public-feedback/online-harms-white-paper-initial-consultation-response> (Accessed: 14 September 2020).

Home Office (2016) NATIONAL CYBER SECURITY STRATEGY 2016-2021, Available at:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf (Accessed: 3 September 2020).

Home Office, (2020) "Equality and diversity" Available at:

<https://www.gov.uk/government/organisations/home-office/about/equality-and-diversity>

(Accessed: 14 December 2020).

Heaton, J. (2008) 'Secondary Analysis of Qualitative Data: An Overview', Historical Social

Research / Historische Sozialforschung, 33(3), pp. 33-45 [Online]. Available at:

<https://www.jstor.org/stable/20762299?seq=1> (Accessed: 11 July 2020).

Heaton, J. (2008) 'Secondary Analysis of Qualitative Data: An Overview', Historical Social

Research / Historische Sozialforschung, 33(3), pp. 33-45 [Online]. Available at:

<https://www.jstor.org/stable/20762299?seq=1> (Accessed: 11 July 2020).

Hern, A (2017) CloudPets stuffed toys leak details of half a million users. Available at:

<https://www.theguardian.com/technology/2017/feb/28/cloudpets-data-breach-leaks-details-of-500000-children-and-adults> (Accessed: 11 February 2021).

Hyd,K (2000) 'Recognising deductive processes in qualitative research', Qualitative Market

Research, 3(2), pp. 82-90 [Online]. Available at:

<https://www.emerald.com/insight/content/doi/10.1108/13522750010322089/full/html>

(Accessed: 03 March 2021).

IBM (2020) IBM SPSS software, Available at: <https://www.ibm.com/uk-en/analytics/spss-statistics-software> (Accessed: 11 October 2020).

Internet Matters (2020) Understanding the risks for children , Available at: <https://www.internetmatters.org/wp-content/uploads/2019/04/Internet-Matters-Infographic-Digital-piracy.pdf> (Accessed: 14th September 2020).

Internet Matters (2019) Look Both Ways, Available at: <https://www.internetmatters.org/wp-content/uploads/2019/04/Internet-Matters-Report-Look-both-ways-screen-time.pdf> (Accessed: 14th September 2020).

Internet Matters (2020), Online grooming facts & advice Available at: https://www.internetmatters.org/issues/online-grooming/?gclid=Cj0KCQjw7Nj5BRCZARIsABwxDKLIwXX7rieTfctZR7DKYJV0UK6-zO2IZi_W4MMm33OzGiz19gbaN78aAq2cEALw_wcB (14th August 2020).

Johnson, R, Onwuegbuzie, A, Turner, L , (2007) Toward a Definition of Mixed Methods Research Journal of Mixed Methods Research Available at: <https://journals.sagepub.com/doi/abs/10.1177/1558689806298224> Volume: 1 issue: 2, page(s): 112-133 (Accessed: 31th July 2020).

Jr,E, Chandrasekaran, A , Blake, A, Parker, G (2017) 'Managing Distributed Product Development Projects: Integration Strategies for Time-Zone and Language Barriers', Information Systems Research , 29(1), pp. 3-6 [Online]. Available at: <https://pubsonline.informs.org/doi/10.1287/isre.2017.0733> (Accessed: 12 October 2020).

Johnson, J (2019) How concerned are you about experiencing being asked for a payment in return for getting back control of your device?, Available at: <https://www.statista.com/statistics/1090096/level-of-concern-over-device-hacking-related-extortion-uk/> (Accessed: 22 August 2020).

Legislations (2010) Equality Act 2010, Available at: https://www.legislation.gov.uk/ukpga/2010/15/pdfs/ukpga_20100015_en.pdf (Accessed: 10 September 2020).

Legislation (2010) Equality Act 2010 (Sex) , Available at: <https://www.legislation.gov.uk/ukpga/2010/15/section/11> (Accessed: 20 September 2020).

Loyd,A (2019) Shamima Begum: Bring me home, says Bethnal Green girl who left to join Isis, Available at: <https://www.thetimes.co.uk/article/shamima-begum-bring-me-home-says-bethnal-green-girl-who-fled-to-join-isis-hgvqw765d> (Accessed: 24 August 2020).

Livingstone,D (2007) Terrorism in the Twenty First Centaury , Kansas: Distribution unlimited at: <https://web.b.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=2&sid=3091060e-1064-428c-9226-e094be39ae4f%40pdc-v-sessmgr01> (Accessed: 11 September 2020).

Lin, A (2005) Bridging Positivist and Interpretivist Approaches to Qualitative Methods. Available at: <https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1541-0072.1998.tb01931.x> (Accessed: 31th July 2020).

Lowe, C, Zemliansky,P (2011) Writing Spaces: Readings on Writings 2nd Parlor Press.

Lakomy, M (2017) Let's Play a Video Game: Jihadi Propaganda in the World of Electronic Entertainment, Studies in Conflict & Terrorism, 42 (4), pp 383-406 Available at: <https://www.tandfonline.com/doi/abs/10.1080/1057610X.2017.1385903> (14th August 2020).

Mary, M , Hanne, N , Frank, H (2011) Lessons learned: advantages and disadvantages of mixed method research, Qualitative Research in Accounting & Management, 8 (1), pp. 59-71 Available at: <https://www.ingentaconnect.com/content/mcb/qram/2011/00000008/00000001/art00004> (Accessed: 30 July 2020).

MacFarlane,K Holmes,V (2017) Multi-agent System for Safeguarding Children Online, Cham: Springer International Publishing AG.

McCarthy (2015) ISIS Is Expanding Its Reach On Twitter, Available at: <https://www.statista.com/chart/3308/isis-is-expanding-its-reach-on-twitter/> (Accessed: 14 September 2020).

Mori,S Goto,A (2018) 'Reveiw of National Cybersecurity Strategy Case Study UK ', AIS eLibrary, (), pp. [Online]. Available at: <https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1334&context=pacis2018> (Accessed: 14 September 2020).

Moore, R. (2005) Cybercrime: Investigating High-Technology Computer Crime, 2nd ed., Oxford : Elsevier.

McLeod,S (2019) Case Study Method, Available at: <https://www.simplypsychology.org/case-study.html> (Accessed: 9 October 2020).

Martellozzo, E & Jane, E (2017) *Cybercrime and its victims*, New York: Routledge.

Microsoft Excel (2021) *Analyze your data instantly* Available at:

<https://support.microsoft.com/en-us/office/analyze-your-data-instantly-9e382e73-7f5e-495a-a8dc> (Accessed: 21 January 2021).

MI5 (2021) *THREAT LEVELS* Available at: <https://www.mi5.gov.uk/threat-levels> (Accessed: 21 February 2021).

Mallette, L,J, Saldaña (2019) 'Teaching Qualitative Data Analysis Through Gaming', *SAGE Journals* , 25(9-10), pp. 1085-1090 [Online]. Available at: <https://journals-sagepub-com.ezproxy.uwtsd.ac.uk/doi/pdf/10.1177/1077800418789458> (Accessed: 28 February 2021).

Nayak, S, Narayan, K (2019) *Strengths and Weakness of Online Surveys* Available at:

<http://www.iosrjournals.org/iosr-jhss/papers/Vol.%2024%20Issue5/Series-5/E2405053138.pdf> (Accessed: 30 July 2020).

Novikov, A.M. & Novikov, D.A. (2013) "Research Methodology: From Philosophy of Science to Research Design" , Florida: CRC Press.

Noor,M (2008) 'Case Study: A Strategic Research Methodology', *American Journal of Applied Sciences*, 5(11), pp. 1602 - 1604 [Online]. Available at:

https://www.researchgate.net/profile/Khairul_Baharein_Mohd_Noor/publication/26517241_Case_Study_A_Strategic_Research_Methodology/links/5462bd80cf2c0c6aec1b83e/Case-Study-A-Strategic-Research-Methodology.pdf (Accessed: 9 October 2020).

Norton (2020) *Cyberstalking: Help protect yourself against cyberstalking*, Available at:

<https://us.norton.com/internetsecurity-how-to-how-to-protect-yourself-from-cyberstalkers.html> (Accessed: 19 September 2020).

NCA (2020) *Cyber crime*, Available at: <https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime> (Accessed: 16 September 2020).

NSPCC (2020) *Online grooming facts & advice* Available at:

https://www.internetmatters.org/issues/online-grooming/?gclid=Cj0KCQjwk8b7BRCaARIsAARRTL5HGVAUYI9QFpDfAM1JjF-PjPTFF9NXuymFBPu1YJxeQYAMUZ3U590aAi8MEALw_wcB (Accessed: 21 September 2020).

Oath,S (2017) *Yahoo provides notice to additional users affected by previously disclosed 2013 data theft*, Available at: <https://www.verizonmedia.com/press/yahoo-provides-notice-to-additional-users-affected-by-previously/?guccounter=1> (Accessed: 14th September 2020).

Oppenheim,M (2020) 'Scammers carrying out sextortion cybercrimes during coronavirus crisis', Independent , 23rd April, p. .

O'Reilly, K. (2012) *Ethnographic Methods*, 2nd ed., London and New York: Routledge.

Paulk,M, Curtis,B Chrissis, M (1993) 'Capability maturity model, version 1.1', IEEE, 10(4), pp. 18-27 [Online]. Available at: <https://ieeexplore.ieee.org/abstract/document/219617> (Accessed: 2nd September 2020).

Patchin, J (2011) *Cyberbullying Research Summary Bullying, Cyberbullying, and Sexual Orientation* Available at: https://cyberbullying.org/cyberbullying_sexual_orientation_fact_sheet.pdf (Accessed: 21 September 2020).

Parameswaran, U, Ozawa-Kirk.J & Latendresse,G (2019) 'To live (code) or to not: A new method for coding in qualitative research', *SAGE Journals* , 19(4), pp. 630-644 [Online]. Available at: <https://journals-sagepub-com.ezproxy.uwtsd.ac.uk/doi/full/10.1177/1473325019840394> (Accessed: 28 February 2021).

Reeves, J Soutar, E Green, S Crowther, T (2017) *Children and young people's vulnerabilities to being groomed; what can be done?* , Kent : University of Kent .

Robbetts, K (2015) *Preventing Terrorism - Duties in the Higher Education Sector*, Available at: <https://www.vwv.co.uk/news-and-events/blog/higher-education-law/preventing-terrorism-in-he> (Accessed: 24 August 2020).

Rethink mental illness, (2020) Overview Available at: https://www.rethink.org/advice-and-information/rights-restrictions/mental-health-laws/discrimination-and-mental-health/?gclid=Cj0KCQjwk8b7BRCaARIsAARRTL5ZLkAMk3jV5Vg3LbsNVYU1YVXYOGsJzDVCv_xYXH6RiqFWPIXU5ZEaAiCCEALw_wcB (Accessed: 20th September 2020).

Royal Canadian Mounted Police (2020) *The National Cybercrime Coordination Unit (NC3)* Available at: <https://www.rcmp-grc.gc.ca/en/nc3> (Accessed: 28th September 2020).

Short, E, Et al (2015) *A practical guide to coping with cyberstalking*, Bedfordshire : Andrews UK Limited.

Smart, W (2018) *Lessons learned review of the WannaCry Ransomware Cyber Attack*, Available at: <https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf> (Accessed: 15 September).

Smith, J (2015) Breck Bednar murder: How Lewis Daynes manipulated his victim, Available at: <https://www.bbc.co.uk/news/uk-england-essex-30730807> (Accessed: 24 August 2020).

Surrey Police (2020) Breck's Last Game film, Available at: <https://www.surrey.police.uk/police-forces/surrey-police/areas/campaigns/campaigns/2018/brecks-last-game-film/> (Accessed: 24 August 2020).

Sahay, A. (2020) Peeling Saunders's Research Onion, Available at: https://www.researchgate.net/profile/Arunaditya_Sahay2/publication/309488459_Peeling_Saunders's_Research_Onion/links/5813283508aedc7d89609ea8/Peeling-Saunders-Research-Onion.pdf (Accessed: 10 July 2020).

Shidur, R (2017) The Advantages and Disadvantages of Using Qualitative and Quantitative Approaches and Methods in Language 'Testing and Assessment' Research: A Literature Review , Available at: <https://eric.ed.gov/?id=EJ1120221> (Accessed: 31th July 2020).

Severina, S (2019) Morden Projects Management Methods: Their Advantages and Disadvantages Available at: <http://journalsofznu.zp.ua/index.php/economics/article/view/121> (Accessed: 31 July 2020).

Suite,G (2019) 7 steps to create surveys using Google Forms Questionnaire Available at: <https://digital-transformation.media/en/g-suite/google-forms/questionnaire/> (Accessed: 21 January 2021).

Snyder,H (2019) 'Literature review as a research methodology: An overview and guidelines', Journal of Business Research , 104(), pp. 333-339 [Online]. Available at: <https://www.sciencedirect.com/science/article/pii/S0148296319304564> (Accessed: 20 September 2020).

Torok,R (2010) "'Make A Bomb In Your Mums Kitchen": Cyber Recruiting And Socialisation of 'White Moors' and Home Grown Jihadists', AUSTRALIAN COUNTER TERRORISM CONFERENCE, (), pp. [Online]. Available at: <https://ro.ecu.edu.au/cgi/viewcontent.cgi?referer=https://scholar.google.co.uk/&httpsredir=1&article=1005&context=act> (Accessed: 12 September 2020).

University of Trinity Saint David (2020) Covid-19-Letter-Postgraduate-Research-Partner, Available at: <https://www.uwtsd.ac.uk/media/uwtsd-website/content-assets/documents/collaborative-partnerships-office/Covid-19-Letter-Postgraduate-Research-Partner.pdf> (Accessed: 23 July 2020).

Vannoni, M (2014) 'What Are Case Studies Good for? Nesting Comparative Case Study Research Into the Lakatosian Research Program', SAGE Journals, 49(4), pp. 331-357 [Online]. Available at: <https://journals.sagepub.com/doi/abs/10.1177/1069397114555844> (Accessed: 09 October 2020).

Warwick, (2020) Inductive or Deductive approaches, Available at: <https://warwick.ac.uk/fac/soc/ces/research/current/socialtheory/maps/when/> (Accessed: 20th July 2020).

Wilson, J (2003) Gantt charts: A centenary appreciation , Available at: <https://www-public.imtbs-tsp.eu/~gibson/Teaching/Teaching-ReadingMaterial/Wilson03.pdf> (Accessed: 31th July 2020).

Wright, K (2005) 'Researching Internet-Based Populations: Advantages and Disadvantages of Online Survey Research, Online Questionnaire Authoring Software Packages, and Web Survey Services ', Journal of Computer-Mediated Communication, 10(3), pp. [Online]. Available at: <https://academic.oup.com/jcmc/article/10/3/JCMC1034/4614509> (Accessed: 10 October 2020).

Worlds Standards (2020) Internet country domains list, Available at: <https://www.worldstandards.eu/other/tlds/> (Accessed: 11 October 2020)

Warwick, (2020) Protected Characteristic Factsheets Available at: https://warwick.ac.uk/services/equalops/learnmore/training_guidance_resources/protectedcharacteristicfactsheets/protected_characteristic_factsheet_-_marriage_and_civil_partnership.pdf (Accessed: 20 September 2020).

West Yorkshire Police (2018) "A Guide to Cyber Crime and Online Safety" Available at: https://www.westyorkshire.police.uk/sites/default/files/a_guide_to_cyber_crime_and_online_safety_0.pdf (Accessed: 24 August 2020).

York University (2020) Community Update #3 - Cyber Attack Recovery Continues | Poursuite de la récupération à la suite de la cyberattaque, Available at: <https://safety.yorku.ca/2020/05/update-information-technology-system-disruption-may-4-2020/> (Accessed: 24 August 2020).

Appendix 1 Protected characteristic

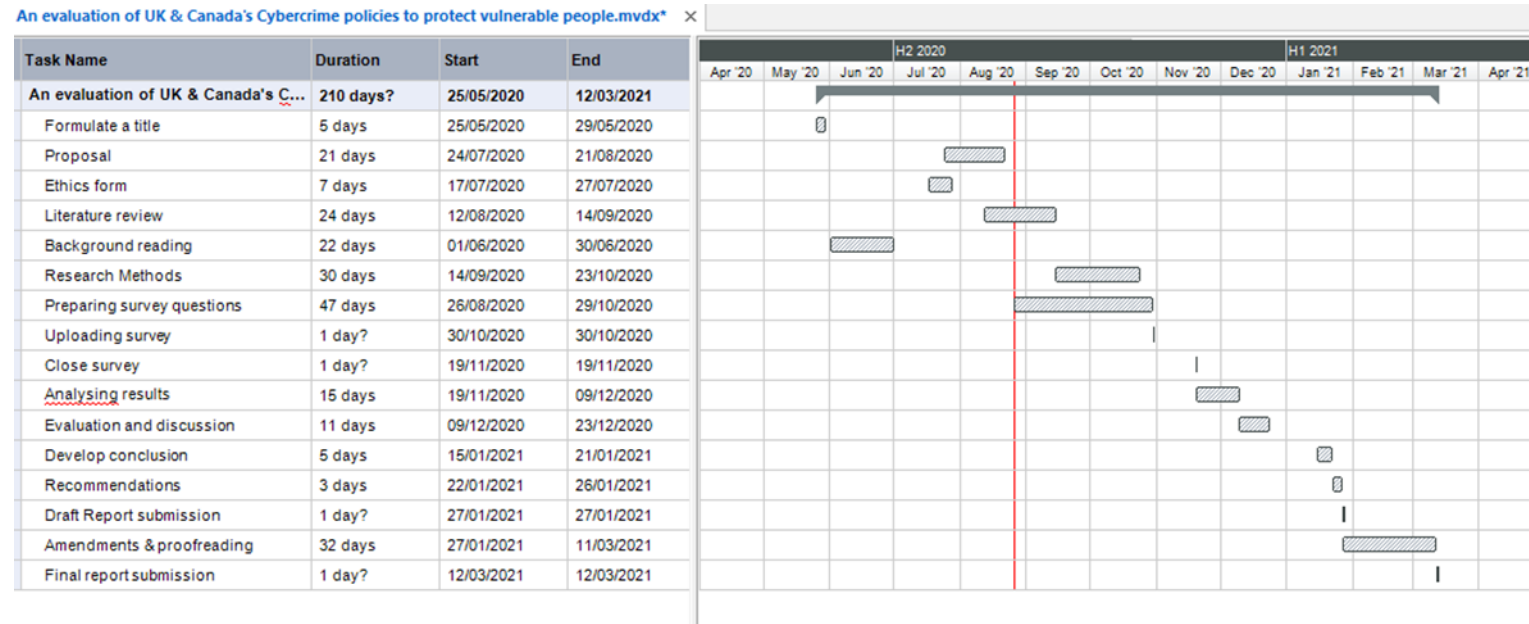
Protected characteristic	Explanation/Example	Citation
Disability	The Equality Act 2010 covers both physical disability and mental health - the act says that an individual must have affected the person's everyday life for more than 12 months to become classed as a disability	(Rethink mental illness, 2020).

Age	Age mainly concerns discrimination in work placements or public places and how employers or other persons cannot discriminate against a person because of their age, for example it is wrong to discriminate against a person because of their lack of knowledge about technology due to their age.	(Equality and Human Rights Commission, 2020)
Marital status	No one can discriminate against a person being married or in a civil partnership.	(Warwick, 2018)
PREGNANCY	It is against the law to discriminate against another individual who is pregnant or breastfeeding their child in a public or work area	(Citizen Advice, 2020).

Sexuality	A person cannot discriminate against another because they are gay, straight, or bisexual	(Citizen Advice, 2020).
Gender	An employer cannot discriminate against a person because they are male or female	(Legislation, 2010).
Gender Reassignment	Gender Reassignment is when a person becomes transgender; discrimination of a transgender person is by treating them differently because of their current gender.	(Equality and Human Rights Commission, 2020)

Race	This when someone discriminates against another because of their colour, nationality, ethnic background or national origin. In cybercrime terms many individuals who come from different backgrounds are vulnerable to online hate crime, for example BBC reported that hate crime increased by 10% according to UK police, whilst the Home Office said that race hate crime increased by 11%	(citizen advice, 2020). (BBC News, 2019).
Religion	The legislation states that someone cannot discriminate against another person due to their religion beliefs or philosophical belief	(Equality and Human Rights Commission, 2020)

Appendix 2 – Gantt Chart



Appendix 3 - Online Questionnaire

1. Are you a UK or Canadian Citizen? What nationality are you? UK Canada Other *

- ☐ UK
- ☐ Canadian
- ☐ Other

2. What is your age? *

- ☐ 18 - 25
- ☐ 26 - 35
- ☐ 36- 50
- ☐ 51 Over
- ☐ Prefer not to say

3. What gender do you identify as currently? * ::

- ☐ Male
- ☐ Female
- ☐ Transgender
- ☐ Non-binary
- ☐ Other
- ☐ Prefer not to say

4. Do you consider yourself to belong to one of these categories? Tick all that apply to you *

- ☐ Mental Health
- ☐ Disability
- ☐ Transgender
- ☐ None of these

5. What is your understanding of the term 'vulnerable individual'? Please explain.

Long-answer text

6. Do you think cybercrime is any of the following (tick all that apply)? *

- ☐ Cyberbullying
- ☐ Cyberstalking
- ☐ Radicalisation
- ☐ Cyberfraud
- ☐ None of these

...

7. To what extent do you believe that cybercrime is a threat in today's society? *

- ☐ Not at all
- ☐ Somewhat
- ☐ Maybe
- ☐ Very much so

8. Have you or a family member been involved in cybercrime activity (if yes, please name the type of crime and explain whether you/they feel/felt vulnerable) check if Yes go to Q9 if no go to Q13

Long-answer text

9. How many times have you been involved in a cybercrime incident?

Short-answer text

10. If you contacted the police, on a scale of 1-10 (where 1 is awful and 10 is excellent), how did you think the police handled it? [number] Please explain the reason for your answer?

Long-answer text

11. How many times did you contact the police about this/this incident / s?

Short-answer text

12. What charities did you approach for support, if any, and why?

Long-answer text

13. Do you think the police are doing enough to combat cybercrime? (yes or no and why)

Long-answer text

14. In your opinion, what should the UK government be doing to protect vulnerable people adequately from cybercrime (UK citizens answer only)?

Long-answer text

15. In your opinion, what should the Canadian government be doing to protect vulnerable people adequately from cybercrime (Canadian citizens only)?

Long-answer text

16. Should both governments explain how they are going to apply the measures to protect the vulnerable people from cybercrime (yes or no and why)

Long-answer text

17. Should parents be held responsible for their children's online activities up to the age of 15? (yes or no and why)

Long-answer text

18. Should Shamima Begum be allowed to re-enter the UK following her involvement with ISIS? (yes or no and why)

Long-answer text

...

19. What do you know about the UK Online Harm White paper or the Canadian National Cyber Security Action Plan (2019-2024)?

Long-answer text

20. In your opinion, what should the UK & Canadian governments be doing about the current Cybercrime legislation?

Long-answer text

Thank you for taking part in this research.

Description (optional)

Appendix 4 – Milestone Table (Government of Canada)

Goal 1: Milestone Table				
Initiative	Department	Action/Milestone	Target End Date	Status
Goal 1: Secure and Resilient Systems				
Supporting Canadian Critical Infrastructure Owners and Operators	Public Safety Canada (PS)	Acquire/develop a technical cyber assessment tool	2019	Planned
		Establish an Industrial Control System (ICS) Advisory Committee	2019	Planned
		Increase the number of cyber security exercises delivered to critical infrastructure stakeholders	2020	Planned
		Develop technical ICS security training and awareness solution	2020	Planned
Improved Integrated Threat Assessments	Communications Security Establishment (CSE)	Increase capacity to enable CSE to better meet increasing demands for cyber threat assessments	2024	In Progress
		Increase capacity to enable CSE to assess a wider array of cyber threats reflecting the Cyber Centre's growing client base	2024	In Progress
Preparing Government of Canada Communications for Advances in Quantum	Communications Security Establishment (CSE)	Protect Government of Canada's classified information against anticipated advancements in quantum computing	2024	In Progress
Expanding Advice and Guidance to the Finance and Energy Sectors	Communications Security Establishment (CSE)	Finance and energy sectors work cooperatively with the Cyber Centre and within their sectors to improve their cyber security posture	2024	In Progress
		Improve cyber security posture of the finance and energy sectors	2024	In Progress
Cyber Intelligence Collection and Cyber Threat Assessments	Canadian Security Intelligence Service (CSIS)	Augment CSIS collection of national security cyber intelligence and cyber threat assessments	2023	Planned
National Cybercrime Coordination Unit (NC3 Unit)	Royal Canadian Mounted Police (RCMP)	Reach initial operating capability	2020	In Progress
		Establish NC3 Unit Advisory Group	2021	In Progress
		Launch the National Cybercrime and Fraud Public Reporting System	2022	In Progress
		Reach full operating capability	2023	In Progress
Federal Policing Cybercrime	Royal Canadian	Deploy cyber specialists abroad	2020	In

Appendix 5 - Vulnerable people Case study (UK & Canada)

Case Study One - Breck Bednar

The first example of where a vulnerable child was at risk from online grooming was Breck Bednar from the UK, Breck regularly played video games with his friends after school and made online communities where he and his friends met other people using a telecom software called Teamspeak (BBC News, 2015). Breck met Lewis Daynes his groomer online in 2013, over time friends and family members started to feel concerned about Breck's actions towards them. Lorin LaFave (Bednar Mum) said he stopped attending church gatherings on Sunday with family whilst his friends from school told were told no longer intended to game with them as much (BBC News, 2015). It was noted by Surrey Police that in December Lorin LaFave contacted them with concerns about her son's behavior since she believed her child was being groomed by Lewis. Later when police entered the scene of the incident, they discovered Lewis had destroyed multiply USBs and hard drives; when the suspect was taken into custody, he would not give officers passwords to any of his devices. With the lead detective saying Lewis wanted to feel that he was in control of the confrontation (Reeves, et el, 2017).

The results of this case study were numerous, Surrey police was made to compensate Breck parents for their handling of the case as the Independent Police Complaints Commission (IPCC) believed the call handler and their supervisor lack the knowledge of online grooming thus they were not sure where to direct Mrs Bednar for specialist help. The IPPC found Surrey police service guilty of inadequate checks of Lewis Daynes who was registered on the National Police Data Base due to similar case back in 2011 (BBC News, 2016). It should be noted that Surrey Police Force will review how they can improve their services to help protect children from online threats (MacFarlan, at el, 2017).

In 2018 Lorin LaFave designed a short film for parents, Teenagers, and young adults on the dangers of online grooming called 'Breck's Last Game' on her son murder , which will be shown in multiple schools along with being televised on the BBC (Surrey Police, 2020).

The Bednar family have also set up a foundation to help other families and friends who may feel someone is vulnerable online, the foundation campaigns to have the government review and update their policies (Breck Foundation, 2020).

Case Study Two - Shamima Begum

In 2015 Shamima Begum left the UK to join ISIS alongside two other girls Amira A base and Kadiza Sultana (Loyd, 2019). When interviewed by the BBC in 2019 on what made her join IS, her reply was “I started watching videos of British hostage being beheaded and the life style that ISIS offered for Muslim people around the world”, during the interview she commented that she would be happy to come back to UK live to be rehabilitated (BBC, 2019). Currently Shamima is allowed back to the UK to petition for the return of her UK citizenship which was revoked by the government in 2019 (Grierson, 2020). This case study is good example of how a young teenager can be vulnerable to cybercrime becoming a victim of radical terrorist organization that seeks to groom new members online.

The case of Shamima Begum shows the failures of government in protecting vulnerable people from online threats. In 2007 the UK government unveiled its Prevent strategy which aimed to prevent a terrorist attack from happening along with stopping having people become radicalised. In 2015 the Prevent Scheme was strengthened by section 26 (1) of the Counter Terrorism Act 2006 and Security Act 2015 , which obliges that all institutions of higher education have a duty of care to vulnerable students who are risk of becoming radicalised (Home Office, 2020). Universities boards alongside the Home Office have introduced Relevant Higher Education Bodies (RHEBs) with the aim of RHEBs to protected vulnerable students from becoming radicalised (Robbetts, 2015).

Even though RHEBs are for university students, in the case of Shamima Begum school should have picked up on the signs that she was becoming radicalised online and intervened to stop her but because Shamima Begum was not in a university environment she was not on their radar. The UK government could correct this vulnerability by bring in something like the RHEBs for all education faculties which would help schools combat the issue. The government had failed to protect Shamima Begum from becoming radicalised online due to focusing on older ages groups ignoring a large vulnerability within the system that could be exploited by radical groups.

Third Case Study - York University cyber attack

In March 2020 York University in Toronto Ontario was victim to a cyber-ransom attack, the hackers were able to gain access to critical servers stealing information on students and research from the university labs. The hackers wanted York university give them a sum of money in return for the hackers ceasing their activities against the university, It is believed that the university was hacked to find data on the Covid 19 vaccine research as York University is one of the main research facilities in Canada with a \$250,000 fund. Before the cyber-attack, the US & UK warned to other nations that they saw an increase of cyber-attacks against university and health boards. The cyber-attack on York university were able to gain access to 6,100 devices, 15 servers and a virtual private network (VPNS) of the human resources (HR) and financial departments during the ransom, the main concern of university of York was it students as they could become vulnerable due to financial information being stolen form them by the hackers in response the university sent an email warning of the extra steps to ensure their cyber safety (CBC, 2020).

The University of York Toronto released a statement on the 3rd of May apologising to student about cyber issues stating to their student that many of the university services would be down for a while because of the hack. Student were advised to update their office 365 passwords including their emails, Zoom accounts, campus Wi-Fi accounts and Moodle accounts (University of York, 2020).

York University was fortunate not to pay the ransom as they were able to combat the incident internally, they were also fortunate enough that none of their student financial details were taken thanks to the quick action from the university. However, the University of Saskatchewan was a victim to a DOS cyber-attack in February of 2020 year the university of York could have done more to prepare themselves for the cyber-attack.