Cybercrime and Public Criminology

by

Jonah A. Savage

A thesis submitted to the
School of Graduate and Postdoctoral Studies in partial
fulfillment of the requirements for the degree of

Master of Arts in Criminology

Criminology/Ontario Tech University/Social Science and Humanities

University of Ontario Institute of Technology (Ontario Tech University)

Oshawa, Ontario, Canada

December, 2023

THESIS EXAMINATION INFORMATION

Submitted by: **Jonah Savage**

Master of Arts in **Criminology**

Thesis title: Cybercrime and Public Criminology

An oral defense of this thesis took place on December 11, 2023 in front of the following examining committee:

Examining Committee:

Chair of Examining Committee	Dr. James Walsh
Research Supervisor	Dr. Steven Downing
Examining Committee Member	Dr. Amir Mostaghim
Examining Committee Member	Dr. Jordan Harel
Thesis Examiner	Dr. Karla Dhungana Sainju,

The above committee determined that the thesis is acceptable in form and content and that a satisfactory knowledge of the field covered by the thesis was demonstrated by the candidate during an oral examination. A signed copy of the Certificate of Approval is available from the School of Graduate and Postdoctoral Studies.

Abstract

The enigmatic nature of cybercrime is an enduring theme across the criminology literature. As a result, a disconnect between stakeholders involved in digital crime seems to contribute to irresponsible discourse and ineffective policy. Further, this confusion has created a competition of interests in which narratives surrounding cybercrime inherit the ideology of the ‘winning’ sector (Habermas, 2015). It seems that private security is currently having undue influence over this discourse, and as such, narratives surrounding cybercrime remain marketized (Banks, 2015). Thus far, public criminologists have yet to adequately adapt to the merging of the technological and social realms, an adaptation that is a necessity in avoiding a continuation of punitive crime control trends (see Crepault, 2017; Garland and Sparks, 2000). The intersection of public criminology and digital criminology lies in discourse generation and the messaging the key cybercrime stakeholders provide to the public. This paper draws from eight semi-structured interviews with cybercrime experts in private security, financial institutions, academia, litigation, and law enforcement. The objective of this project is to spur a conversation between the different stakeholders explored below by merging the considerations of cybercrime and public criminology.

Keywords: cybercrime; cybersecurity; public criminology; discourse; stakeholders

AUTHOR'S DECLARATION

I hereby declare that this thesis consists of original work of which I have authored. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I authorize the University of Ontario Institute of Technology (Ontario Tech University) to lend this thesis to other institutions or individuals for the purpose of scholarly research. I further authorize University of Ontario Institute of Technology (Ontario Tech University) to reproduce this thesis by photocopying or by other means, in total or in part, at the request of other institutions or individuals for the purpose of scholarly research. I understand that my thesis will be made electronically available to the public.

The research work in this thesis that was performed in compliance with the regulations of Research Ethics Board under **#16848**

Jonah A. Savage

STATEMENT OF CONTRIBUTIONS

I hereby certify that I am the sole author of this thesis and that no part of this thesis has been published or submitted for publication. I have used standard referencing practices to acknowledge ideas, research techniques, or other materials that belong to others. Furthermore, I hereby certify that I am the sole source of the creative works and/or inventive knowledge described in this thesis.

ACKNOWLEDGEMENTS

I would like to acknowledge the contributions and assistance of my committee members including Dr. Steven Downing, Dr. Amir Mostaghim, and Dr. Jordan Harel.

TABLE OF CONTENTS

LIST OF TABLES

CHAPTER 2

LIST OF ABBREVIATIONS AND SYMBOLS

CIS	Center for Internet Security
UNODC	United Nations Office on Drugs and Crime
DoD	Department of Defense
DODIN	Department of Defense Information Network
DISA	Defense Information Systems Agency
FBI	Federal Bureau of Investigation
NIST	National Institute of Standards and Technology
CBA	Canadian Banker’s Association
PPP	Public-Private Partnerships
EFF	Electronic Frontier Foundation
IC3	Internet Crime Control Centre
OWASP	Open Web Application Security Project
PCI	Payment Card Industry
IT	Information Technology
CISO	Chief Information Security Officer
TA	Thematic Analysis
SSA	Safe Streets Act
LCBO	Liquor Control Board of Ontario

Chapter 1. Introduction

1.1 Introduction

Introduction

Many iterations of the concept of crime have impacted the way that criminologists, policy officials, police officers, and legislators have studied the term. Criminology has undergone a similar conceptual shift with the advent of *cybercrime.* Though a comprehensive definition of cybercrime does not currently exist (UNODC, 2013), many scholars tentatively agree on some definitional aspects that provide a foundational understanding of the concept. The use of technology to facilitate acts of deviance is a universal characteristic of competing definitions of crime in cyberspace (Holt and Bossler, 2014). However, whether or not crime in the online space warrants a unique lens of study from traditional crime is a contentious topic in the current literature.

Sheila Brown poses an interesting dilemma in the crime and technology literature as a false distinction between our 'real' and 'virtual' lives (2006). In a critique of both positivistic dichotomies and postmodern semiotics, Brown contends that criminologists must entertain a merging of the scientific and the social into the 'technosocial' or a 'criminology of hybrids.' This seemingly popular opinion is echoed in more recent literature, such as Floridi's (2013) notion of the 'onlife' and Stratton et al.'s (2017) critique of criminology's self-referential nature. The social and technical worlds *are* evidently intertwined in ways that trivialize positivist methodologies, such as routine activities theory, that are unfortunately still very common in cybercrime research (Herrero et al., 2021; Leukfeldt and Yar, 2016); however, Whitson and Haggerty's (2008) 'data double' is a more accurate description of the intersection between the technological and the social. The data double is a virtual abstraction of an individual from their physical location, which can be scrutinized, analyzed, and surveilled. The data double implies a sense of conscious and subconscious creation, whether by the individual or by companies who wish to build (and sell) consumer profiles off the virtual identities. The technosocial, as proposed by Brown and other proponents, just *is*, which does not bode well for measurement or analysis. Brown's theory may be tautological, typical of the postmodern logic that the author aims to transcend. According to Brown, "hybrid—technosocial—culture cannot be accounted for by linear paradigms or causal scientific explanations, nor indeed hierarchies of knowledge concepts. Neither can it be conceived of as merely a constellation of representations. Nor can the answer lie anywhere simply 'in nature' or 'in society' (p. 228)". This claim is reminiscent of a common dilemma in the social sciences that occurs when abstract social concepts are proven to be true by virtue of being impossible to refute.

However, some commonalities exist between Brown's (2006) theorizing and concepts emphasizing individual agency in the digital space. Specifically, Brown's technosociality is reminiscent of an article about the 'techno-security-capitalist complex' by Banks (2017). Banks argues that a "technocrime consciousness" has enveloped all spheres of society and is used as a tool by elite sectors to manufacture anxiety and generally dictate public opinion. From a more critical lens, Banks would agree with Brown about the possibly insidious merging of the technological and the social; however, Banks' notion better captures the creation and evolution of the two by drawing upon Habermas (1964) to highlight the potential ramifications of the technological conscious in the public sphere (as cited in Habermas, Lennox, and Lennox, 1974).

A framework for analyzing crime in the digital space that accounts for some of the semiotic issues with Brown's (2006) theorizing can be found in Powell, Stratton, and Cameron's (2018) aptly titled book *Digital Criminology.* Digital criminology entails surpassing the narrow study of crime in the digital space as indistinguishable from traditional crime in the real world. Powell, Stratton, and Cameron (2018) note that the dichotomy of on and offline contributes to perpetuating the status quo of criminology. That is, applying traditional criminological knowledge to *online crime* without any effort to acknowledge the "relational, cultural, affective, political and socio-structural dimensions of crime and justice" in the digital society unnecessarily narrows the developing field of study (p. 8).

The conceptual framework of digital criminology lends itself to acknowledging both unique and recurring social processes in the online space, reminiscent of public scholarship's attempts to coalesce different branches of the *public* in disseminating academic knowledge. A significant challenge for scholars in the politically charged environment of crime control in contemporary society is working outside academia and applying knowledge to real-world problems. Engagement with the public on academic matters concerning crime and crime control is essential. Punitive trends in incarceration, especially in the United States of America, highlight the need to challenge existing structures and the notion that ideas of crime are common sense (Crepault, 2017). As Uggen and Inderbitzin (2010) state, "nowhere is the gap between perception and evidence greater than in the study of crime and punishment" (p. 726).

Public criminology is a developing field of scholarship that aims to adapt the typically academic-exclusive nature of criminological scholarship to serve a broader range of publics (Loader and Sparks, 2011). The roots of public scholarship lie in Herbert Gans' conception of the public intellectual (Uggen and Inderbitzin, 2010). According to Gans, the public intellectual serves as a mediator between academics and the general polity, allowing for scholarly insight into relevant social phenomena. The heart of public scholarship, then, is intrinsically linked to social activism. With the punitive turn of punishment in North America spanning the last few decades, public criminology is more crucial than ever (Loader and Sparks, 2011). In their special edition of the 'key ideas in criminology' series, Loader and Sparks (2011) call for a democratic underlabourer in the public sphere of crime and justice. The democratic underlabourer refrains from providing radical ideas of either left or right political orientation that translate well into soundbites. In other words, the democratic underlabourer guides the civilian's navigation of complex ideas by unearthing the 'truth' from the web of competing ideas about crime provided to non-academics while at the same time bridging the gap between scholars and the public. Further, as noted by the UNODC, criminological and sociological theory may be useful for understanding cybercrime and, thus, help avoid a performative attempt at bridging the academic and public spheres (2013). However, as mentioned above, the comprehensive study on cybercrime conducted and organized by the UNODC may overestimate the utility of traditional criminological theories such as routine activities theory and general theory of crime (2013).

In my estimation, the intersection of public criminology and digital criminology lies in discourse generation and the messaging provided to the public by the key cybercrime stakeholders. As alluded to earlier, Jurgen Habermas’s (1964) conception of the public sphere helps ground the discussion of public scholarship in the interconnectedness afforded by the digital society (as cited in Habermas, Lennox, and Lennox, 1974). The public sphere "mediates between society and state, in which the public organizes itself as the bearer of public opinion, accords with the principle of the public sphere that principle of public information which once had to be fought for against the arcane policies of monarchies and which since that time has made possible the democratic control of state activities" (1974, p. 73-74). This quote and Habermas' framework, more generally, emphasize the agency of the public in discourse generation. In other words, according to Habermas, citizens are an integral part of the public opinion. This view contrasts with Gramsci's theorizing of hegemony in which the public is more of a passive consumer of information than an active discourse participant (Bezerra et al., 2021). Further, the concept of democratic participation found in Habermas' public sphere serves as a bridge between traditional notions of public criminology, such as Loader and Sparks (2011), and more contemporary understandings of the digital space as seen in Powell, Stratton, and Cameron (2018).

Early cybercrime scholars have suggested that deviance pertaining to networked technologies represents a manifestation of intense curiosity on the part of the 'hacker,' sometimes embodying an addiction to manipulating technology or the pursuit of knowledge more generally (Taylor, 1999). Further, hackers have also been associated with subversive, specifically anti-capitalist, ideologies in the extant literature, invoking a response to visions of either a *technodystopic* or *technoutopic* persuasion (Collier et al., 2021). As such, it is important to delineate (at least partially) the similarities and differences between traditional *hackers* who are characterized, however accurately, as having an insatiable hunger for knowledge regarding complex networks and tangible pieces of technology, such as early iterations of phone phreakers with contemporary cybercriminals who primarily operate from overseas via the Internet. This evolution may be likened to a shift in perspective from a romantic ideal of cybercrime and deviant hacker subcultures to a more realistic, routinized view of the contemporary cybercriminal (Collier et al., 2021). Collier et al. (2021) claim that the underground hacker subculture has become industrialized and, thus, has lost some of the novelty that perhaps characterized early cybercrime discourse. In much the same way, echoing the thesis of this project, narratives provided by different stakeholders in digital crime seem to have inherited the same marketized tendencies. In fact, as stated by Collier et al. (2021), the illicit hacker economy appears to mirror the "mainstream economy," whose bureaucratization and structure, ironically, may be seen as a precursor to the politically libertarian underground hacker culture.

The findings of Collier et al. (2021) may be partially explained by the motives of current cybercriminals becoming largely financial in nature. Pogrebna and Skilton (2019) claim that while digital criminals of the past were intrinsically motivated, the advent of the Dark Web and networked social forums in the early 21st century catalyzed a change in both the methods and goals of contemporary *hackers*. Initially the *pioneers* of the digital counterculture, aided by the globalization of the digital criminal economy, hackers now enjoy the ability to sell their services anywhere across the globe (Castells, 2010). However, it would be naïve to state that the romanticism associated with the hacker culture has completely vanished and that digital criminals are solely financially motivated. In a relatively small study examining the self-professed reasons for offending in the digital space, Payne et al. (2020) found that among the most popular justifications was the enjoyment of the challenge and thrill provided by the opportunity to offend, suggesting that the spirit of early hackers reverberates in the subsequent generations.

Similarly, Pogrebna and Skilton (2019), in an analysis of interviews with hackers, suggest that many of these individuals cite subversive reasons for breaking the law. For instance, some hackers seem to display illusions of grandeur in their reasoning for their crimes, stating that they hope to ‘change the world’ and resist the proliferation of government surveillance. These findings may suggest that further merging of the digital and physical realms will reinforce the romanticized ideals associated with early hacker culture as technology continues to encroach on the *real* world.

Interestingly, differences in motivation may appear based on the nature of cybercrime being discussed. For instance, Holt, Freilich, and Chermak (2017) find that cybercrimes committed with ideological motivations, perhaps evidently, differ from traditional cybercrimes. Importantly, interviews with ideologically motivated offenders prove that the conception of a typical cybercriminal is someone who is interested in financial benefits, whereas those with patriotic motivations are enticed by their “flags, language, and nation” (Holt, Freilich, and Chermak, 2017, p. 224). The researchers attribute this difference to one of objective rather than motivation; that is, both ideological and non-political cyber offenders are motivated by the same factors discussed above, such as curiosity and technological mastery. The difference lies in the outcome of the actors, political offenders targeting resources that will further their agendas, while typical cybercriminals are mostly interested in attaining monetary assets (Holt, Freilich, and Chermak, 2017).

As already noted, many scholars feel that increasing education among targets of online crime may lead to increased safety and awareness (Birthriya and Jain, 2022; Wall, 2008; Yar, 2013). Similarly, Payne et al. (2020) find that perpetrators cited a lack of understanding of consequences and the seriousness of their behaviour as reasons for offending. As such, addressing discrepancies in understanding may simultaneously increase the resiliency of victims and deter future offenders. Many cybercrime scholars have theorized that Habermas' public sphere may apply to the digital space. For instance, as mentioned above, Banks (2017) asserts that some scholars feel that the democratic participation of the Internet and other networked technologies can revive the public sphere.

Similarly, Castells (2008) believes that the globalized civil society, aided by networked technologies, allows for shifting public opinion. According to Castells, the digital society has exponentially increased opportunities for activism and social solidarity worldwide. Powell, Stratton, and Cameron echo this sentiment in stating that "the democratizing effect of digital technologies has enabled state agencies to engage with the public in ways that were unavailable before" (2018, p. 9).

Scholars who are proponents of the benefits associated with the coupling of the terrestrial and online worlds, such as Castells (2008) and Powell, Stratton, and Cameron (2018), are sometimes criticized as 'sociotechnical imaginaries' (Lavorgna and Ugwudike, 2021). According to Lavorgna and Ugwudike, the sociotechnical imaginaries are uncritical of the historic partnering of the criminal justice system, public, and academia and naively exalt the potentials of networked technologies in shifting power imbalances (for those skeptical of sociotechnical imaginaries, see Banks, 2017; Min, 2010; Nam, 2012). Interestingly, Habermas himself stated that the public sphere was unrealized and remained subservient to capitalist relations (as cited in Habermas, 2005). However, as Castells (2008) said, “the global civil society now has the technological means to exist independently from political institutions and from the mass media. However, the capacity of social movements to change the public mind still depends, to a large extent, on their ability to shape the debate in the public sphere” (p. 86-87).

As such, I believe that practical public criminology is possible with the aid of what Powell, Stratton, and Cameron (2018) refer to as ‘open-source intelligence’ and the aforementioned democratizing ability of the internet. However, as demonstrated historically, the public sphere poses many obstacles to knowledge dissemination, which can result in discrepancies in communication and understanding between the branches of the public sphere (Carrier, 2014). For instance, Cross, Holt, Powell, and Wilson (2021) find that police believe that the public is unaware of the severity of victimization in digital spaces, while citizens feel they have an adequate understanding of the danger. Perhaps they lack knowledge of the resources available to them upon victimization (for underreporting of cybercrime, see Wall, 2008; Cross, 2018; Reynolds, 2022; Holt and Bossler, 2014). The comprehensive study on cybercrime conducted by the United Nations Office on Drugs and Crime in 2013 states that “underreporting derives from a lack of awareness of victimization and of reporting mechanisms, victim shame and embarrassment, and perceived reputation risks for corporations” (UNODC, 2013, p. 21). Similarly, Banks (2015) claims that government officials and CJS practitioners are ineffective in public discourse surrounding digital crime. The main contributor to this discourse is private security, which has a financial interest in specific messaging provided to the public. What exists then is a competition of interests diluting the potential for precise and consistent discourse in the public sphere (Habermas, 1974).

Nevertheless, this needs to be revised to communicate effectively. Keeping with Habermas, the news media's role in this counterproductive discourse cannot be understated. Mesko and Bernik (2011) state that the news media does a poor job of informing the public of the dangers surrounding cybercrime and how to remain safe in cyberspace. Instead, news media often opts to run sensationalized media reports of hackers and national security threats. Considering that media and public attention on cybercrime is increasing with the ubiquity of technological communication, both academics and media institutions should assess their role in the growing discourse with sincerity and urgency (UNODC, 2013).

The increasing marginality of criminologists in the political and media spheres accentuates the problems surrounding cybercrime messaging (Tidmarsh, 2022). No clearer is this seen than in contemporary academic discussions of digital crime. In criminal justice policy discussions, many stakeholders contribute their input to shape a dominant narrative provided to the public. Crepault (2017) claims that the public sphere in capitalist democracies is a contested space and a site of ideological struggle. In this space, policymakers, academics, police practitioners, government officials, and more compete to have their voices heard. Wall (2008) notes that cybersecurity is plagued by the same disarray that characterizes the public sphere, stating that several independent and conflicting discourses surround cybersecurity, generating a culture of fear surrounding cybercrime.

Evidently, there needs to be a more concentrated effort on utilizing the benefits of technological advances to create cohesion between the many branches of the public sphere and their interactions with the digital space. This effort begins with analyzing the consistency of narratives between said branches. To accomplish this, I will conduct interviews with various stakeholders to determine what the prevalent narratives provided to the public are regarding cybercrime and whether these narratives paint an accurate picture of current digital crime discourse. The literature discussed in the following review will supplement the interview findings to assess the shortcomings of discourse generation and outline some possible avenues toward more responsible messaging.

I contend that narratives surrounding digital crime have inherited market values and are inconsistent due to the variety of discourse participants (public, corporate actors, private security, government officials, police, etc.) contributing to ineffectual or contradictory messaging in the public sphere. With this in mind, how can these actors facilitate a more responsible discourse with the enigmatic concept of digital crime? In this paper, I will examine the existing gaps in the literature surrounding digital crime and public criminology - the most important being that there is scarcely an intersection between the two fields. To highlight these gaps, I will analyze what I deem to be the prevalent trends in the literature to date. I will conclude the literature review by listing criticisms of the existing scholarship that inform my rationale for my project. The method section will detail the inspiration for the interview guide as well as the approach to interviews while also highlighting the analytical approach utilized in examining the thought-leaders' perspectives. Further, the findings garnered in the interview process will be presented and dissected, followed by a discussion of the implications of the results of this project, along with suggestions for future avenues of research.

1.2 Literature Review

Private Actors

As noted above, the marketization of cybersecurity narratives contributes to the apparent ineffectiveness (Banks, 2015; Yar, 2008). The market values inherited by these crime control narratives are a product of neoliberalism and its tendency to manifest through governance and social control (Jordan, 2001). Considering the discussion of Floridi’s (2013) conception of the ‘onlife’ and the apparent certainty of interaction with the online sphere, questions of how individuals who are not technologically savvy or perhaps unaware of developing trends in digital harm are expected to navigate this limitless environment of the ‘technological’ are inevitable. One of the most apparent ways in which neoliberal attitudes seem to manifest in crime control is through the concept of responsibilization. According to David Garland (1996), the responsibilization strategy “involves the central government seeking to act upon crime not in a direct fashion through state agencies (police, courts, prisons, social work, etc.) but instead by acting indirectly, seeking to activate action on the part of non-state agencies and organizations” (p. 452). Though Garland does not explicitly mention cybercrime, one may infer that the responsibilization strategy applies directly to the current state of crime control as well. Specifically, Jewkes and Yar (2012) note that corporations prefer to seek assistance from private organizations (security) to formal or traditional institutions (police). Garland (1996) would explain these revelations by arguing that the acceptance of crime as an inevitable aspect of late modernity justifies both the extension of the private sector in criminal justice and allows the state to disperse the responsibility of safety to many different entities.

Many authors have explored responsibilization in the digital world, often concerning specific cybercrimes such as identity theft and fraud (Wall, 2008; Whitson and Haggerty, 2008; Yar, 2013). However, as Gordon, McGovern, Thompson, and Wood (2022) mention, discussions of crime in the digital sphere should include the critical distinction between online harm and those activities against the law. Neoliberal attitudes, as noted above, play a prominent role in the responsibilization of technology users due to the ideology's effect on the discourse surrounding regulation and online behaviour. For example, Jordan (2001) claims that informational libertarianism or anarchy can classify cyberpolitics. Similarly, in a study of online discourses surrounding cyberspace, Dunn-Cavelty (2013) finds that one of the key conceptions is that of a lawless frontier. Like in economic or social policy in the physical world, neoliberalism prioritizes the rights and freedoms of the individual at the expense of state regulation. These trends are mirrored in cyberspace. For instance, Jordan (2001) compares cyberspace to a free market of ideas and goods; as a result, regulation is unnecessary as individuals are capable of self-governance. Unfortunately, this type of discourse has implications outside the communication of ideas. Specifically, Kremer (2014) finds that libertarian language also affects cybersecurity mindsets. This mindset can manifest through prioritizing cost-effective security measures that inherit the market ideology of capitalism and thus place individuals and their information at risk or perhaps ironically justify more intrusive measures of cyber-protection.

Banks (2015) finds that a consumerist orientation has enveloped cybersecurity in keeping with the marketized tendencies of the discourse surrounding cyberspace. Other scholars have noted that the marketization of cybersecurity is alarming and seemingly more prevalent than ever (Yar, 2008). For example, the Canadian Banker's Association's (CBA) website, instead of providing strategies and best practices for individuals in managing their money online, the CBA points to individual banks for cybersecurity information. Examining some of the prominent Canadian banks' websites proves that each financial institution partners with external agencies to sell antivirus software or a service that helps individuals protect their information online.

Corporations and other private actors that profit from the computer crime control industry encompass private security literature (Banks, 2015; Yar, 2008). As mentioned earlier, partnerships with financial institutions and anti-virus software companies highlight a cooperative attempt to profit off of the insecurity of members of the public regarding cybersecurity (Banks, 2015). A similar trend is witnessed in the punitive turn of traditional crime control in the public criminology literature. Garland and Sparks (2000) note that the extension of the private sector in crime control directly results from victim-oriented shifts in discourse and the politicization of crime fears. The fear generated through discourse results in themes of uncertainty defining cybersecurity (Christensen and Petersen, 2017). To address this uncertainty, Christensen and Petersen (2017) view public-private partnerships (PPP) as a viable solution. PPPs allow necessary flexibility in a domain with as many interested parties as cybersecurity has. As the United Nations Office on Drugs and Crime states, PPPs are often used for fostering communication regarding threats and patterns in cybercrime (UNODC, 2013). However, Carr (2016) believes PPP leads to a market-oriented cybersecurity approach.

Further, Haggerty and Ericson (2000) claim that today’s information economy institutionalizes multiagency approaches to policing. Banks (2017) notes how the marketization of cybersecurity discourse in neoliberal societies can create a preventive logic that scares consumers into paying for cybersecurity and peace of mind. Similarly, Hall and Winlow (2005) comment on consumerist culture and how it sells insecurity. This insecurity may manifest through anti-virus software, as mentioned above or even through subscription-based services offered by financial institutions that take extra steps to safeguard information. Hope (2006) posits that the threat of crime predicates private security consumption and that citizens do not have the same resources to avoid the danger. As mentioned above, Jewkes and Yar (2012) claim that corporations are more reliant on private security than police in matters of online victimization; this has implications for underreporting of online crime and also the narratives provided to customers about a corporation's victimhood.

State Actors

A similar trend to the responsibilization of consumers in the messaging of private actors occurs in the cybersecurity narratives provided by state actors. State actors’ messaging surrounding crime in the digital space often relies on the terrifying possibility of invisible external threats. Primarily, there is a fatalistic narrative that typically accompanies rhetoric around national security and malevolent *hackers*. For instance, Powell, Stratton, and Cameron (2018) claim that governments conceptualize cybercrime through a militaristic lens and portray to the public that cyber-attacks are, first and foremost, a threat to nation-states (p. 44). Kremer (2014) also echoes this, stating that traditional militaries often see the threat as the other. This othering is mirrored in cyberspace as the militarization of the digital world consists of clustering threats using evocative language, such as hackers and terrorists and espousing narratives of danger to the public (Holt and Bossler, 2014).

Ball and Snider (2013) (as cited in Lyon, 2014) claim that national security is a business goal as much as a political one, which can justify intrusive surveillance from the state. For example, Haggerty and Ericson (2000) relate contemporary security approaches to Foucault's carceral state (1975), claiming that privacy is increasingly a commodity to be bargained for and negotiated. Further, Owen (2021) analyzes the implications of cyberattacks from foreign entities on critical infrastructures such as water treatment plants. Owen (2021) finds that the Department of Homeland Security may underreport cyberattacks on critical infrastructure due to fear of reputational damage and further victimization. Similar to Hall et al. (1978), who highlight the racially-based narratives surrounding an increase in reported muggings, one might argue that the omnipresent digital threats that characterize the onlife create a moral panic. Crepault (2017) similarly uses the Canadian Safe Streets Act (SSA) to highlight how government narratives tried to cause moral panic in backing their bill. The policymakers and government officials utilized the emotional appeal of a moral panic to garner support for the controversial safe streets and communities act. Some argued that the SSA legislated draconian penalties on a race and class basis.

Hill and Marion (2016) dissect tactics used by governments to frame cybercrime to the public, including vague links between terrorism and child pornography. In a testament to the communication issues between branches of the public sphere, Hill and Marion (2016) find that the effectiveness of creating insecurity surrounding risk begins by linking a familiar or straightforward national security issue, such as terrorism, with an enigmatic concept, such as cybercrime. The researchers also delineate how presidential speech changes contextually, as the topic of cybercrime discourse changed throughout different United States' presidencies. For instance, George Bush Jr. drew a theoretical connection between digital crime and children's safety, whereas Barack Obama emphasized the potential of hackers in terrorist acts. Levi (2009) also finds a strong relationship between presidential talks and moral panic. Similar claims are echoed in the public criminology literature.

Firstly, populist ideas espoused by the powerful institutions of society are often perceived as accurate by the public (Rock, 2014). The inherent truth in these claims is secondary to the influential capacity of populist ideals. As previously mentioned, Chancer and McLaughlin (2007) highlight that state entities utilize a victim-centered shift in politicizing crime control to support the privatization of security. Beck (1992) claims that the public is insecure about the risk of invisible external threats (as cited in Hill and Marion, 2016). The literature surrounding cybersecurity and the role of state actors seems to convey that this emotionality can advance political agendas, a trend also witnessed in the public criminology literature on punitivity and moral panic (for punitivity and moral panic, see Chancer and McLaughlin, 2007; Currie 2007; Carrier, 2014; Bell, 2014; Piche, 2016; Lumsden and Goode, 2018).

Media

As mentioned in the context of Habermas' public sphere, the media plays a crucial role in discourse production and knowledge dissemination regarding cybersecurity. Public criminologists face several barriers when attempting to provide insight in the media. For instance, Stanko (2007) claims that public criminologists may be labelled biased when entering the public sphere. Similarly, Elliot Currie (2007) attributes public criminology's lack of effectiveness historically to the notion that academics will lose their status as objective researchers upon participating in the public discourse.

Chancer and McLaughlin (2007) state that public engagement with academic knowledge is declining, so criminologists cannot influence policy. Further, Rock (2014) claims that criminologists need to learn how to enter the public arena and disseminate knowledge effectively through the media. These accounts misrepresent the reality of effective knowledge dissemination in the punitive state of contemporary crime control. It is difficult to ignore the seemingly unending list of obstacles that the contemporary public criminologist must effectively navigate to influence a less punitive criminal justice system. The state-funded media, which has been an environment of 'trial and error' in recent memory, best represents this claim (Barak, 2007). Currie (2007) finds that one of the criticisms surrounding traditional public criminologists, specifically that they are no more than simple popularizers of complex information, is unwarranted. Again, according to Currie (2007), popularizing information is a complicated task. Accessibly disseminating knowledge that has historically been the exclusive domain of academics requires strategic insight and a keen understanding of the intricacies associated with privately funded media outlets in the neoliberal market. As such, public criminologists often speak in an echo chamber while engaging with the public through the media. This lack of targeted messaging can manifest in the perpetuation of ineffective messaging surrounding digital crime.

One of the reasons for this 'failure' of public criminologists in navigating the media is the misappropriation of what Barak (2007) refers to as 'newsmaking criminologists.' According to Barak (2007), soundbites often misrepresent newsmaking criminologists in popular media forums. Small tidbits of information are usually provided without the intended context and, more importantly, contribute to a sensationalized idea of crime. According to Barak (2007), these soundbites are ineffective in changing policy and actively work against a more academically informed criminal justice system. The media can utilize claims legitimized by or directly provided by public criminologists to *other* specific groups in society through the media, as seen in the aforementioned state rhetoric. Wacquant (2009) notes how contradictory ideas in the media reinforce ignorant discourse that is wholly disconnected from reality regarding the ‘others’ in society and mirrors a self-fulfilling prophecy amongst 'offenders.' That is, messages surrounding where the danger lies in society become internalized by the public and the 'others,' leading to a cycle of misinformation regarding the true nature of threats.

Moreover, concerning newsmaking criminologists, Rowe (2013) states that the neoliberal market's impact on popular media in 24-hour rolling news cycles has significant consequences for the public criminologist. Specifically, this method of news again promotes sensationalized ideas of crime while also neglecting the vital process of reflection in consuming information. Ideas from academics provided through the rolling news cycles are thus represented without context, sanitized, and portrayed in sensational soundbites that do not translate well into consistent and responsible messaging. Instead, the public criminologist exposes individuals to sensational ideas of crime that can serve ineffective narratives through the media.

In the digital society, social media has mitigated some of the antiquated aspects of traditional news media (Powell, Stratton, and Cameron, 2018). Social media represents the bridge from conventional media to the digital space. Powell, Stratton, and Cameron (2018) note that the lack of hierarchical knowledge production that social media affords can be useful for providing responsible narratives to the public and demarketing the messaging the state offers by giving the public power in communicating ideas of crime. Powell, Stratton, and Cameron’s (2018) optimism contrasts with scholars such as Dodge (2016), who view social media as exacerbating important issues like racism and sexual harassment. Lavorgna and Ugwudike (2021), in an analysis of abstracts, mention that only one article highlighted the role of social media in cybercrime knowledge production. In dissecting the narratives surrounding the datafication of the criminal justice system, Lavorgna and Ugwudike (2021) highlight the increasingly algorithmic nature of crime control. One wonders whether algorithms popular amongst social media services may contribute to the ineffective discourse surrounding crime by portraying specific narratives. Lyon (2014) also captures the importance of digital technology in matters of crime by noting that social media is on the scene before first responders. Lyon’s findings emphasize the ability of social media to shape and share narratives, a point also discussed by Powell, Stratton, and Cameron (2018).

Milivojevic and McGovern (2014) find social media shifting a news-mediated narrative of victim-blaming to a more responsible discourse about violence against women in the aftermath of an Australian woman's murder. Milivojevic and McGovern testify to the ability of public scholarship and digital crime to intersect effectively. Combining this concept with the democratic possibilities of social media noted by Powell, Stratton, and Cameron (2018) demonstrates that open-source intelligence and the democratizing potential of the internet can generate an effective and responsible discourse surrounding cybercrime. Milivojevic and McGovern (2014) also prove that social media can mitigate some of the negative implications of the traditional news media mentioned earlier and even the playing field with respect to generating practical messaging and aiding knowledge production vis-a-vis public criminology.

Police

As the primary institution of crime control, the police serve an essential role in facilitating discourse surrounding threats to the public. As such, in the traditional sense of the discipline, public criminologists are expected to navigate the public sphere and provide informed knowledge through partnering with the criminal justice system in hopes of "getting it right" (Petersilia, 2008, p. 336). Unfortunately, despite a long history of collaboration (Rock, 2014), the police-academic relationship is often strained, and public criminologists are deemed to not contribute much to the discourse surrounding crime and harm (Chancer and McLaughlin, 2007). In a familiar sentiment, a former academic criminologist who transitioned into the public sector notes that "scientific knowledge does not drive crime policy and probably never will" (Petersilia, 2008, p. 353). Further, Stanko (2007) finds that the traditional methods of policing are so entrenched and resistant to change that theory-based evidence, typically provided by criminologists, is devalued. This claim speaks to the lack of cohesion between academia and the public sector; perhaps a more open forum for the democratic production of knowledge surrounding digital crime can aid in generating a more productive discourse.

Cross, Holt, Powell, and Wilson (2021) mention in an analysis of victim experiences that police are the primary point of contact, and civilians are dissatisfied with this. As attributed to the "CSI effect," the authors mention that victims feel that the police should jump into action and are disappointed when their experiences are ultimately translated into consumer education rather than apprehending criminals. Some of the discrepancies between police and community expectations mentioned in this article involve cross-jurisdictional issues and inadequate knowledge of technology to effectively address these communication issues between the police and the public. This disconnect results in police advocating for civilians to use protective measures. As highlighted by Reynolds (2022) and Johnson and Wetmore (2021), the certainty of cybervictimization is one of the main reasons for protective measures. De Paoli et al. (2021) provide one of the few studies to analyze police perceptions of cybercrime through interviews. The researchers interview police cybercrime specialists about their experiences *policing* cybercrime. The findings generated by De Paoli et al. (2021) largely echo the extant literature. Namely, the police report issues with taxonomies that manifest through different branches within the same police force, essentially dedicating resources to the same phenomenon with a different title. For instance, an "IT crime" division and a "high-tech crime" division. Further, issues of underreporting instances of online victimization plague police forces across the globe, according to the participants. Though De Paoli et al. (2021) provide a useful, in-depth examination of one branch of the public sphere surrounding digital crime, my study aims to survey different sectors to create a more comprehensive picture of cybercrime and public engagement.

One of the benefits of the previously mentioned merging entailed in the *technosocial* is the democratizing effects of networked technologies on social control. Formal methods of social control relevant to digital crime policing include the use of law enforcement agencies, such as the FBI or Interpol, to investigate and prosecute cybercriminals from a transnational perspective (UNODC, 2013). In recent years, there has also been an increase in the use of technological solutions, such as firewalls and encryption, to prevent cyberattacks and protect against data breaches (UNODC, 2013). However, as some scholars have noted, there are significant challenges associated with formal social control in cybercrime. Jurisdictional issues, for example, can make it difficult to investigate and prosecute cybercriminals who operate across multiple geographical areas (Cross, Holt, Powell, and Wilson, 2021).

Informally, social control through networked technologies manifests as a more flexible response to the ever-changing nature of digital threats. Importantly, mediums such as open-source and community-driven technologies may allow for a more proactive approach to digital safety. Technologies and institutions such as the Open Web Application Security Project (OWASP) and the Electronic Frontier Foundation (EFF) promote a collaborative orientation to social control similar to the democratic capabilities of internet in digital advocacy detailed by Powell, Stratton, and Cameron (2018).

OWASP is a community-driven project that aims to improve software security by providing free and open-source tools and resources to developers (Kellezi, Boegelund, and Meng, 2021). OWASP has listed the ten most critical web application safety risks as one of their many contributions to the collaborative approach to networked technology navigation. These include but are not limited to, using components with known vulnerabilities, security misconfigurations, and sensitive data exposure. Providing these risks in an open-source forum allows software developers to map vulnerabilities without necessarily needing to search for recorded data (that may be confidential) on breaches and other cyber incidents.

Similarly, the EFF is a non-profit digital rights group primarily concerned with online privacy founded in 1990 (EFF, n.d.). The EFF has also undertaken an essential initiative in hopes of spreading awareness and protecting consumers in the digital space. In 2014, the EFF launched the Secure Messaging Scorecard, which attempts to provide users with the tools to assess the safety of utilizing a particular end-to-end encrypted messaging system (Musiani and Ermoshina, 2017). Further, the discourse surrounding the Secure Messaging Scorecard, aided by the ensuing Edward Snowden leaks, is a microcosm of many of the prominent debates in cybercrime literature, such as ease of use versus integrity (Toma, Décary-Hétu, and Dupont, 2023) and privacy versus security (Lavorgna and Ugwudike, 2021). While formal social control can provide a strong deterrent against cybercrime, informal social control approaches can be more flexible and responsive to changing threats and community needs. Community-driven projects and open-source software, such as OWASP and the EFF, are examples of informal mediums that may serve as viable alternatives to formal approaches in some contexts.

Returning to the formal methods of social control regarding networked technologies, a reciprocal nature seems to constitute this disconnect between citizens and police. Powell, Stratton, and Cameron (2018) mention that police can use citizen information posted on social media as evidence. Though, this may also have adverse effects (Powell, Stratton, and Cameron, 2018). Namely, an overeager public force can contribute to potentially dangerous instances of vigilantism and false accusations. Further, Powell, Stratton, and Cameron (2018) highlight how citizens participate *directly* in matters of criminal justice, especially investigation through social media, which, as mentioned previously, can lead to internet sleuthing, vigilantism, and armchair detective work that has proved dangerous. I argue that we should instead embrace the piecemeal roles of a collection of actors in the navigation of digital space with regard to public criminology and participatory politics.

Public

Finally, the public's role in shaping the narrative is controversial. Powell, Stratton, and Cameron (2018) do an excellent job of highlighting the agency of the public in interacting with and shaping discourse surrounding online crime, which was mentioned above. The agency underscored by Powell, Stratton, and Cameron contrasts previous views of individuals as passive consumers in the public sphere (Johnson and Wetmore, 2021). Reiner (1988) recalls the post-WWII welfare state as a particularly potent space for academics informing policy effectively. Perhaps the relative social cohesion after the atrocities of a World War contributed to a socially conscious outlook amongst scholars and the public conducive to considering diverse perspectives in matters of crime. Further, Amanda Nelund (2014) claims that feminist scholars also have a rich history of informing policy, specifically regarding violence against women and mobilizing around social issues. Currie (2007) says more collaborative arenas are needed for scholars and the public. I believe that social media is aiding this already.

As mentioned above, Cross, Holt, Powell, and Wilson (2021) outline the experiences of victims of online identity theft and their perceptions of cybercrime. The researchers find that an individual’s level of awareness correlates with their perceived risk of victimization. This finding supports the claim that education is key to bridging the gap between branches of the public sphere regarding cybercrime messaging (Birthriya and Jain, 2022; Wall, 2008; Yar, 2013). Further, Wall (2008) claims that the public is severely impacted by the threats portrayed in news media and are more aware of these depictions than other sources of information. Perhaps encouraging public participation in the discourse surrounding major events will change the perception of civilians from passive consumers to active participants (Castells, 2008; Powell, Stratton, and Cameron, 2018).

The most apparent critique of the literature is the lack of interviews with the discourse participants introduced above (see Cross, 2021; De Paoli et al., 2021; Zhang, 2018, for examples of interviews with certain cybersecurity stakeholders). Many of the existing studies based on interview data pertaining to cybercrime do so in the context of victimization. A plethora of studies exist detailing victim experiences (see Cross, 2018; Millman, Winder, and Griffiths, 2017; Reynolds, 2022), but very few, if any, analyze the discourse generated by the thought leaders that are the focus of this paper. The second critique is the lack of an intersection between public criminology and digital criminology. Critics of public criminology argue that a 'better politics of crime' is needed to nurture a truly public criminology. Loader and Sparks (2014) note that this manifests through democratic legitimacy as opposed to Gramscian hegemony. According to Loader and Sparks (2011), a better politics of crime is nurtured through the humility of the public criminologist in their navigation of the politicized environment that characterizes crime control. Specifically, the public criminologist must be tolerant of the 'messy' business of politics and accept that "there is no alternative to a sober engagement with the realities of contemporary politics" (Swift and White, 2008, as cited in Loader and Sparks, 2011, p. 121). Democratic legitimacy in Loader and Sparks' conception is reminiscent of measures of due process and accountability employed to counter abuses of power in contemporary society. Perhaps there is room for the open-source intelligence generated through social media to contribute to a more democratic discourse.

Powell, Stratton, and Cameron (2018) hint at the possibility of a participatory approach to knowledge generation afforded by the democratic potential of social media in narrative formulation. However, they fail to recognize the potential of including PPPs in the revival of an effective public scholarship, which I believe to be possible. The hesitancy of researchers to use the term public criminology is buttressed by the dearth of literature highlighting how public academics have failed in the past (Rock, 2014; Carrier, 2014; Currie, 2007). I believe the participatory political approach outlined by Powell, Stratton, and Cameron (2018) and Ruggiero (2012) pairs well with Loader and Sparks' (2011) original conception of the public criminologist as a democratic underlabourer who calls attention to and challenges the status quo regarding matters of crime control. One of the ways to achieve this is by coordinating different stakeholders and disciplines to create a more effective discourse surrounding digital crime. By bridging the gap between digital criminology and other sectors of society, aided by the non-hierarchical approach to knowledge generation that social media can offer, I believe that a public digital criminology can play an important role in the evolving cyber landscape.

Justifications and rationale for my project are abundant. First, many scholars feel that education and open-source intelligence are the keys to remedying the confusion that surrounds digital crime (Birthriya and Jain, 2022; Wall, 2008). Education, as mentioned earlier, is aided by the participatory approach to knowledge generation. Dunn-Cavelty (2013) finds that cybersecurity discourse analyses of the past have focused solely on the claims of elite members of society (politicians and governments); my project allows for a more holistic examination of the narratives surrounding digital crime. Similarly, Holt and Bossler (2014) claim that the evolving landscape of cybercrime necessitates research "exploring the awareness, perceptions, and preparation for dealing with cybercrimes from the vantage point of front-line officers and managers at all levels. These studies are pivotal to guide policy development to improve the resources available for law enforcement to increase their overall capabilities" (p.34). Further, with respect to the *datification* of the criminal justice system, Lavorgna and Ugwudike (2021) call for "close scholarly scrutiny of how the technologies are framed and presented to the state and the general public, both of whom may be considered the core stakeholders" (p. 1-2).

Chapter 2. Body of thesis

2.1 Data

The data utilized in this project consists of eight semi-structured interviews conducted via virtual meeting software (Google Meet). The participants selected for interviews all had extensive experience in various sectors of cybersecurity; these include lawyers, IT professionals, academics, private sector employees such as those employed by cybersecurity firms, chief security officers at notable companies, and law enforcement officers. As the objective of this project was to primarily uncover the narratives provided to consumers/citizens by different stakeholders in cybersecurity, each participant was able to contribute unique perspectives as to their views regarding the thesis statement.

2.2 Methodology

The methodology of this project is informed by a variety of existing qualitative studies that prioritize exploratory, multimethod typologies. The interview structure utilized in data gathering for this project is reminiscent of De Paoli et al.'s (2021) framework and can most aptly be characterized as semi-structured in nature. As mentioned above, much of the previous literature assesses cybercrime from a micro-perspective, often employing positivistic methodologies and traditional theories of criminality, such as routine activities theory leading to a call for alternative epistemologies from various scholars (Holt and Bossler, 2014; Lavorgna and Ugwudike, 2021; Powell, Stratton, and Cameron, 2018).

Thematic Analysis

De Paoli et al. (2021) employ Braun and Clarke's (2006) thematic analysis (TA) in one of the recent studies based on interviewing cybersecurity stakeholders. The thematic analysis methodology entails approaching data with specific questions in mind that the investigator aims to code around. For instance, Braun and Clarke's (2006) step-by-step outline of the thematic analysis methodology encourages researchers to be rigorous and precise in relating vivid themes gathered from data collection back to the existing literature and current research question. Saunders et al. (2017) detail the concept of saturation in qualitative research, loosely defined as the point at which a researcher repeatedly witnesses the same phenomena in their data. The concept, though ubiquitous, is ill-defined, according to Saunders et al. (2017). The researchers illuminate different conceptions of saturation in hopes of contributing to the term's practicality. One of the theoretical conceptions of saturation outlined by Saunders et al. (2017) is 'a priori' thematic saturation' (as cited in De Paoli et al., 2021). A priori thematic saturation occurs when preidentified themes are identified deductively from the data gathered after the initial literature review. In the deductive approach, saturation occurs when a researcher feels that the data adequately reflect the preidentified themes or codes. As such, the data gathered during interviews or surveys enriches the themes present in existing literature (De Paoli et al., 2021). Another important advantage of thematic analysis, as illuminated by Braun and Clarke (2006), is the fact that researchers will generate results that are generally accessible to the public and valuable in informing policy development. One key objective of the current study is to foster a more efficient dissemination of information from the academic and private spheres to the public. As mentioned in the justification for this project, a lack of understanding characterizes the discourse surrounding online security and social control or policing (Cross, Holt, Powell, and Wilson, 2021). Finally, the flexibility inherent in thematic analysis allows the researcher to be an active participant in the research process; this includes designating codes and themes but also translates well to the data-gathering process or interviews, in this case.

Active Interviewing

Reynolds (2022) utilized an active interviewing approach informed by Holstein and Gubrium (as cited in Silverman, 1997) to interview identity theft victims. Reynolds (2022) states that the active interviewing approach is most suitable because it allows the interviewer to understand the interviewee’s underlying assumptions surrounding their victimization. A critical convergence of active interviewing from alternative methodologies is the primacy placed on suggesting connections between ideas provided by the interviewee. The active interviewing approach allows for reciprocal dialogue, as if the interviewer and interviewee are *both* learning from the interview. According to Holstein and Gubrium (as cited in Silverman, 1997), the interviewer must avoid dictating the interviewee’s interpretation of events; one of the ways the interviewer can accomplish this is through ‘playing dumb’ or being the ‘devil’s advocate.’ Assuming the position of inexperienced in the subject matter allows the interviewer to encourage participants to make their ideas and meanings explicitly clear, unburdened by jargon that may be used in conversation with a fellow expert in the field. Similarly, the role of the devil’s advocate aids in producing the alternative linkages mentioned above. For instance, if an interviewee suggests that victims of online crime are incautious, the interviewer may deem it appropriate to indicate that other institutional factors may also contribute to the victim’s circumstances.

Sampling

Purposive and snowball sampling was utilized in attaining the interviewees for this project. The researcher's existing connections provided an initial pool from which cybersecurity experts could be identified and contacted. The first interviewee contacted was participant one, who was a cybersecurity professional known to the researcher. Participant five was also an initial contact of the researcher. Participants two, six, and eight were suggested to the researcher as possible candidates by an acquaintance in law enforcement. Participant three was contacted through mutual colleagues within academia and participant four was suggested as a potential participant thereafter. Participant seven's interview also resulted from snowball sampling, specifically, they were suggested as a candidate by participant eight (see Table 1).

As a percentage of the sampling pool could be considered a hard-to-reach population, scheduling was the most difficult aspect of conducting interviews. Often, interviews were rescheduled, cancelled, or seemingly forgotten due to the busy schedule of some of the participants. The desired sample size for this project was approximately eight participants. When the researcher conducted eight interviews, further sampling or data collection was deemed unnecessary as many of the participants echoed similar sentiments and reiterated themes consistent with the literature.

Table 1

Participant Characteristics

Participant Number	**Sector of Employment**	**Location**
1	Private (Financial Institution)	Canada

Participant Number	**Sector of Employment**	**Location**
2	Litigation	Canada
3	Academia	Canada
4	Academia	Canada
5	Private (Information Security)	U.S.A
6	Private (Technology Corporation)	Canada
7	Public (Federal Agent) / Academia	U.S.A
8	Public (Federal Agent)	U.S.A

Material: Interview Guide

The interview guide utilized for this study was semi-structured and consisted of broad questions distinguished by their relevance to themes gathered from the initial literature review. That is, what are the prevailing cybersecurity issues that the public should be concerned about, according to different thought leaders, as well as who the actors are, their role in cybersecurity messaging to the public, and how these actors can facilitate a more effective engagement with the public surrounding these issues. Another key theme prevalent in both the extant literature and the interview data gathered for this project was the responsibilization of victims of online crime (Banks, 2015), as such, this was also represented as a potential probing concept in the interview guide. The interview guide, along with the interviewing style mentioned above, facilitated a flexible approach to research generation. For instance, the amount of depth with which prevalent themes were explored depended on a variety of factors that were fluid both across and within interviews. As such, probing questions were integral in guiding the respective interviews. In this sense, the interviewer benefitted from the loose structuring of the interview guide and the ability to adapt to each interview's contextual nuances. This manifested actively often through the concepts of playing dumb and devil's advocate mentioned above. Still, also, in a latent sense, the research-gathering process lent itself to prioritizing certain themes over others depending on the situation. For instance, some interviewees were less familiar with the policy arena or legal aspects of online crime, and thus, those interviews were tailored more toward general cyber-safety education and messaging. Other interviewees possessed a greater understanding of the logistical and technical aspects of cybersecurity, specifically in online banking software. They were more inclined to speak to the nature of bureaucratic considerations in creating and maintaining online environments for customers with significant financial risks.

As such, the interview guide possessed three main sets of questions, one general question for each prevalent theme, along with sub-questions intended for probing queries based on the response to the initial topic. The three main themes explored in the interview guide were: the pressing cybersecurity issues facing the public, the narratives or messaging provided to the public by different actors or stakeholders in cybersecurity, and the responsibility of consumers or citizens in their own security while navigating the digital space. Each of these themes benefits from the unique perspective of the interviewees, who, by definition, exist within distinct (though not exhaustive) sectors of cybersecurity. Again, these research areas may have been explored in the extant literature; however, no projects of this scope have addressed the specific perspectives analyzed in this project.

Coding

The coding process was conducted with the assistance of the “Google Meet” transcription feature. Each interview was recorded in an audio and visual format, along with an auto-generated transcription of the conversation. In listening to the audio recordings of the interviews, the respective transcripts were found to be very accurate in all instances. This accuracy allowed for confidence in the feature in subsequent interviews, providing the opportunity to stay very present in the conversation without worrying about keeping diligent notes so as to not miss anything important during the coding process.

Braun et al. (2014) provide an invaluable guide to utilizing thematic analysis with interview data. The authors outline a step-by-step approach to thematically analyzing interviews. As mentioned earlier, thematic analysis is a flexible and relatively straightforward methodology often utilized by amateur qualitative researchers. Thus, Braun et al. (2014) propose a framework for conducting TA while emphasizing the flexibility inherent in the method. Pertaining to coding, Braun et al. (2014) highlight two critical steps in the thematic analysis. They are, namely, rereading and familiarizing, and generating labels. Rereading transcripts of interviews allows the researcher to depersonalize the data. Often throughout the data-gathering process, the researchers would state that the sentiments reflected in a given interview completely echo the extant literature. Only after a few scans through the transcripts would the researcher realize that each interview was completely unique in its contributions to the project. This speaks to the quality of the research question and the addressing of a gap in the literature. However, this also speaks to the merits of thematic analysis as a qualitative method and its ability to uncover sometimes complex patterns of meaning across a dataset or transcript.

Braun et al. (2014) also provide some measures of scientific validity in designating a feature of a transcript or dataset as a code. The researchers mention that though qualitative methods can be flexible and straightforward, there are still mechanisms to implement different degrees of rigour into the method. One of the strategies proposed by Braun et al. (2014) is to ask a series of questions upon gathering an adequate number of codes and themes across the dataset. The questions are intended to verify whether the initial codes selected from the dataset are suitable for addressing the research question and are internally consistent to avoid redundancy.

2.3 Findings

The methods described above were utilized to analyze interview data in hopes of uncovering the common themes alluded to by participants in this study. The findings presented in this section allow for the examination of a hitherto underexplored intersection between two important branches of criminological study: public criminology and digital criminology. Five main themes were derived from the perspectives of the subject matter experts queried in this study. Those being: the disconnect between stakeholders, uncertainty regarding the main threats in the digital space, responsibilization, the impact of capitalistic ideologies on cybercrime and cybersecurity, and education.

Table 2

Summary of Main Findings

Theme	**Description of Findings**
Disconnect Between Stakeholders	• Jurisdictional Issues • Competition of Interest • Effectiveness of Public-Private Partnerships
Uncertainty Regarding Threats	• Sensational and Mundane Accounts of Cyber Crime • Media Impact on Threat Perception • Paternalism
Responsibilization	• Neoliberalism and Regulation • Victims are Apathetic Due to a Lack of Consequences • Public Displays of Victimization in Garnering Awareness
Capitalistic Lens	• Commodification of Security • Lack of Funding for Cybersecurity • Profit Maximization Versus Security

Education	• Importance of Educational PPPs • A Lack of Awareness from Citizens • Larger Entities Adequately Inform Employees

Disconnect Between Stakeholders

As mentioned in the abstract, one of the primary areas of interest for this study was the apparent disconnect between cybercrime stakeholders as to the prevalent or most important issues in digital crime. In particular, narrowing the scope of threats in the digital space, agreeing on practical outreach strategies, and achieving more consistent narratives can be beneficial for a host of reasons. Achieving a semblance of foundational understanding when it comes to the digital space could yield new potentials for outreach and education as well as general individual safety (De Kimpe et al., 2022). The interviewees' opinions mirrored the academic literature in having difficulty agreeing on the main issues. This disorientation across the interviews could be due to the unique qualities of digital crime and safety as compared to traditional forms of crime. As mentioned above (and buttressed by the interview data), jurisdictional issues plague the field of cybercrime and can lead to a competition of interests while vying for digital safety. Some have argued that a cooperative approach to justice in the digital space is useful (Milivojevic and Radulski, 2020). However, the sample of participants in this project seems to believe that some forms of collaboration regarding cybervictimization yield unfavourable outcomes for individuals hoping to have their situation addressed and rectified.

Jurisdictional issues in the digital crime landscape manifest in many different ways, according to the sample. For example, participant two, a lawyer who heads the cybersecurity and data privacy practice at their firm, believes that the disconnect between stakeholders is especially prevalent in Canada, where victims, in this case, corporations, do not know whether to call the RCMP, OPP, or local law enforcement when faced with cybercrime. The interviewee feels that the Internet Crime Complaint Centre (IC3) operated by the FBI mitigates some of this confusion for victims in the United States of America. It seems that the IC3 has merit regarding the reporting of digital crimes; however, participant seven was reluctant to claim that the IC3 has made strides in assisting victims with reparation or apprehending criminals. Instead, the participant, a federal investigator in the US, feels that the IC3 acts as more of a repository than a tool for criminal justice. These claims may be consistent with important findings from Cross, Holt, Powell, and Wilson's (2021) exploration of police perceptions regarding cybercrime. The researchers find that one of the contributing factors to a disconnect between law enforcement and citizens concerning online crime is the unrealistic expectations of victims. Specifically, victims expect police practitioners to promptly attempt to apprehend criminals when in reality, the police officers represented in the study feel that reporting is more important as a contribution to cybercrime education and awareness. Further mirroring these findings, two interviewees felt that the local levels of law enforcement are generally under-skilled, under-resourced, and underfunded for addressing cybercrime in a more effective manner.

Another contributing factor to the apparent disconnect between cybercrime stakeholders prevalent in the interviews is the competition of interests and priorities associated with criminal incidents. Perhaps aided by the project's sampling of a variety of different stakeholders interested in cybersecurity, an adequate cross-section of prioritized concerns was deciphered in the interviews. For example, one subtheme under the umbrella of *disconnect between stakeholders* was the perspective of many of the interviewed ‘corporate’ stakeholders signalling that the security considerations when addressing clients or customers are unique to other types of crime and distinct from the priorities of law enforcement addressing cybercrime. Participant two said:

> “Remember, law enforcement has a very different mandate [compared to corporations], which is a criminal mandate, to find bad guys and arrest them if they can. But this is a borderless crime in some cases, and as a result of it, it doesn't always work very well.”

This interviewee felt that customers should be aware that cybercrime can be quite different from traditional crimes in terms of seeking justice; again, one could assume that difference is partially due to the variety of stakeholders at play. For instance, a corporation as a custodian of consumer data and information is much more concerned with the public response to any breach or incident (Toma, Décary-Hétu, and Dupont, 2023), whereas the customer may be eager to seek justice and see the perpetrator apprehended, as noted above and corroborated by Cross, Holt, Powell, and Wilson (2021).

Another interviewee further delineates the differences in priorities of stakeholders by involving public or governmental entities as a contrast to private companies. When asked if the disconnect between cybersecurity stakeholders was apparent in their employment as a federal agent, participant seven made clear that “everyone’s got their own thing.” According to this thought leader, when faced with a breach, private companies will look to keep things under wraps and out of the public’s mind. There is a dearth of literature on the interests of private companies when faced with cybervictimization, and this subtheme will be discussed in more detail as it pertains to the data gathered in this study (see Holt and Bossler, 2014; Toma, Décary-Hétu, and Dupont, 2023; Whitson and Haggerty, 2008). Interestingly, this participant claimed that public entities tend to be proactive about informing citizens or clients about data breaches speculating that one of the reasons for this difference between private and public entities may be legislative obligations imposed on the public entity. Whitson and Haggerty (2008) also note that in contrast to public entities, internal policies in private corporations may prohibit (or perhaps complicate the process of) informing their customers of breaches.

The disconnect in priorities amongst cybersecurity stakeholders can be classified as competition due to the respective actors’ ability to control narratives surrounding their entity and cybercrime more generally, upon *winning* the competition. For example, Banks (2015) discusses how winning this competition can result in skewed narratives surrounding cybersecurity. Specifically, as participant five stated, savvy customers (in this case, corporations) offload the responsibility of cybersecurity for their customers onto private security firms. This claim is supported by a variety of sources in the criminology literature. Namely, Banks (2015) states that private security often prevails over federal actors or law enforcement in the competition of interest outlined above, implying that private security may disproportionately control the general discourse surrounding cybersecurity. This implication could prove dangerous for various reasons; according to Charles Perrow (1984), “private firms have the incentive and, often, the political and economic power to resist effective regulation” (as cited in Johnson and Wetmore, 2021). There is also the reality of the increased financial incentives of private security firms to dictate cybersecurity narratives captured by other critical scholars (see Joh, 2017; Lyon, 2014; Whitson and Haggerty, 2008; Wood, 2021). Further, the capitalistic nature of cybersecurity noted in the thesis statement of this project and explored in the literature review was extracted as a theme prevalent in the data collected and will be explored in more detail below.

The competition of priority and interest made clear through the interview data gathered for this project is reminiscent of the notion of a competition of expertise commonly found in public scholarship literature (Crepault, 2017). As mentioned above, Habermas (1964) stated that a competition of interest surrounds the public sphere (as cited in Habermas, Lennox, and Lennox, 1974), Crepault (2017) applied this concept to the criminological literature by stating that criminal justice discourse in the public sphere is ideologically contested and occupied by various competing parties. As such, we can draw parallels between the public scholarship literature and data provided by cybercrime stakeholders. Though the variety of interested parties in cybercrime can have negative implications, cooperation can also prove beneficial, according to the interview data. It seems, as hinted at by Powell, Stratton, and Cameron (2018), that “a two-way communication strategy that encourages ‘information exchange’ between officials and the community” (p. 78) may describe some of the strategies that cybersecurity stakeholders interviewed for this study envision as practical means of generating awareness. The two-way information exchange is reminiscent of the non-hierarchical knowledge transfer that many proponents of public scholarship view as necessary for creating a more socially-just society. In the interview data, participant six, who acts as the chief information security officer (CISO) at their technologically-inclined corporation details a reverse-mentoring project at their firm which emphasizes the importance of communication in matters of cybersecurity. In this program, young, creatively-minded employees meet with the middle-aged interviewee and share hot-button issues in the realm of digital safety. During the interview, participant six seemed to have a healthy amount of humility regarding a generation gap prevalent in their employment sector, specifically mentioning that some current digital threats are beyond their understanding as someone belonging to ‘generation x.’ As such, this participant advocated for a constant and well-oriented dialogue surrounding cybersecurity at their company, mentioning that being a teacher as a high-ranking official at a company of their size is important in fostering the two-way communication strategy noted above because:

> “If senior management makes a decision that says we don't value security as part of our organization, then that message from the top will trickle down. So no amount of security awareness training will be effective if the tone from the top is security doesn't matter.”

However, this democratized approach to information sharing does not have to exist in strictly demarcated confines such as those of a particular company or office building. As mentioned earlier, Christensen and Petersen (2017) believe that public-private partnerships can serve as an alternative to top-down information sharing that perhaps characterizes traditional criminal justice policy discourse. The interview data also seems to support the claims of Christensen and Petersen. For instance, participant one, who works as a business analyst at a reputable financial institution in Canada speaks to the importance of community-driven non-profit organizations that allow for increased collaborations between federally-funded and private entities. Specifically, the Center for Internet Security (CIS), which accomplishes many of the same functions as the EFF and OWASP detailed in the literature review, may signal a potential example of PPPs' effectiveness in a practical context. According to this participant, the CIS has implemented its critical security controls into the National Institute of Standards and Technology (NIST). The NIST allows for financial institutions, such as the bank this participant is employed at, to achieve a state where the company can have its cybersecurity protocols audited. The NIST is a federally-funded agency that maintains a comprehensive and evolving cybersecurity framework that is mandatorily adhered to by various agencies, especially those that are publicly funded (National Institute of Standards and Technology, n.d.). The interviewee claims that the CIS control outcomes within the NIST serve as an accessible tool for inter-agency communication. The CIS provides critical security controls and how they might reasonably be measured in adherence to the NIST cybersecurity framework. According to the participant, this detail allows information security experts to communicate with management or fellow employees who may be less technologically inclined while remaining goal-oriented and mitigating confusion. Generally, this symbiosis between CIS and NIST, a private and public entity respectfully, may serve as an illustration of larger-scale democratic participation that can alleviate some of the disconnect and uncertainty between cybersecurity stakeholders and the public.

Though PPPs are useful in sustaining discourse and generating participation, the public (citizens) are also key stakeholders in cybersecurity. Thus, a 'cyber, public criminology' must consider the public's role in these issues as well. The interview data gathered for this project highlights many different aspects of the public's place (or lack thereof) in this conversation. University professors and cybercrime researchers were queried for this study, and the sample seems to agree with the need for greater engagement with the public in matters of cybercrime through PPPs. Participant four detailed their research interest originating in the lack of representation for female students in cybersecurity courses. In an effort to generate a more inclusive discourse surrounding cybersecurity, the interviewee began analyzing some of the reasons for the lack of female participation. Ultimately, the researcher has spearheaded a PPP, which includes cooperating with banks and other financial institutions to conduct cyber-safety seminars in secondary and elementary schools.

Participant eight spoke to the apparent effectiveness of PPPs in public engagement regarding cybercrime as a former US federal agent with years of experience dealing with cyber investigations and first-hand encounters with various sectors of online crime. This participant was most familiar with the Federal Bureau of Investigations' (FBI) awareness efforts, citing the 'InfraGard' program as a valuable tool for promoting collaboration between the FBI and private entities. According to the interviewee, the InfraGard program has representatives go across the country and meet with corporate actors to run workshops and seminars pertaining to the eminent threats in the digital space. The participant does, however, concede that the InfraGard program is largely for executives and does little to benefit the individual beyond the incidental sense of the companies they may work for (or consume from) being more informed.

Powell, Stratton, and Cameron (2018) may be overly critical of the stifling nature of the state and its institutions, leading to a failure to recognize the necessity of PPPs in their call for “a new kind of public criminology” (p. 198). Though both viewpoints are represented, the researchers seem to focus more on the subversive power of networked and digital technologies than the collaborative implications of a more democratized public arena. For instance, corporatization in the contemporary state, monikered the ‘digital sovereign’ “can be understood explicitly as a mode of regulating human activity to gain profit, as opposed to freeing markets to make them more efficient” (p. 52) according to Powell, Stratton, and Cameron. As such, there is a fatalistic framing of the digital public sphere as a site of potential “networked authoritarianism” where the increased capabilities for public discourse provided by these technologies have the adverse effect of allowing states to further control and manipulate activist movements. This possibility, according to Powell, Stratton, and Cameron (2018), is currently aided by the PPPs in the democratic nations of the West and is not to be discounted as a phenomenon of traditionally authoritarian states.

In contrast, the majority of participants in this study who were familiar with state entities and their cybersecurity practices were largely eager to applaud their efforts (specifically pertaining to the partnerships detailed above). For instance, participant seven, a federal agent, mentions that:

> "in the government, we're pretty good; I mean, they throw a ton of money at cybersecurity, they really do, not enough still, but they do. Private sector, they don't. If you look at any charts about cybersecurity spending, it's not pretty".

From a different perspective, participant four, who works in academia feels that the Canadian government "has been doing some stuff. I mean, the government has been developing programs and putting material out there." Again, the interview data seems to suggest that there is some attention and investment being directed towards cybersecurity from the public sector (especially when compared to the private sphere), yet, these investments, financial or otherwise, are deemed inadequate by many of the participants for reasons that will be explored further in a separate theme.

The notion of public-private partnerships representing a strategy for creating more cohesion between cybersecurity stakeholders leads to questions of centralization. Both the data gathered for this project, along with the extant literature, have pointed to the utility of partnerships between entities; however, one must also consider the borderless nature of cybercrime and how public-private partnerships may be overly exclusive, especially when a citizen hopes to file a complaint with a large corporation that utilizes the services of third-party vendors that may be located overseas. As such, international cooperation may yield future research or policy applications. The literature surrounding international cooperation in the fight against cybercrime is somewhat scarce, though efforts are ramping up (Cherniavskyi et al., 2021). Some of the interviewees provided their opinions on whether centralization is possible in relation to PPPs and cybercrime. Participant two demonstrated their lack of confidence in centralization at the global level occurring with respect to cybercrime by noting that some states would be hesitant to expose (or cease) their cyber espionage practices as a consequence of signing a global treaty regulating digital activity at the governmental level. Participant seven, a federal agent, mentions that even at the national level, centralization akin to the IC3 creates more confusion for citizens, giving the example of a small business losing five thousand dollars as a cybercrime victim. The IC3 is a large, federally-funded initiative, and according to this participant, the IC3 may not be the correct avenue for reporting smaller-scale losses. As such, the victim may find themselves in the merry-go-round described by Cross (2018), where they find it difficult to determine what agency should be informed of their situation.

Some interviewees were more skeptical of the viability of public-private partnerships. A prevalent trend in cybercrime literature to this point is the classification of types of cybercrimes, cybercriminals, and whether cybercrime can be included in discussions of traditional crimes or if the phenomenon deserves its own discipline (see Holt and Bossler, 2014; Notte, Leukfeldt, and Malsch, 2021; Wall, 2001). According to participant three who is employed at an academic institution, one of the reasons for hesitancy to commend PPPs was a lack of a standardized framework for communication between stakeholders. This interviewee contrasted the communication issues surrounding cybersecurity with the experience of obtaining a driver’s license; that is, standard rules and regulations exist when operating a motor vehicle that need to be practiced if one wishes to be a legally recognized driver in a certain jurisdiction. The participant noted that practices regarding cybersecurity are usually implemented on an ad hoc basis, and perhaps there should be more regulated training or licensing for people dealing with digital privacy. From a different perspective, participant one, who works in the financial sector notes that financial institutions in Canada adhere to a select few organizations that provide a common taxonomy of vulnerabilities. However, these services are utilized by private corporations, and the interviewee admits that “their customers are just consumers [financial institutions], so the government may want to coach their strong regulatory frameworks that protect the little guy [citizens].” Again, it seems the consensus among the cybersecurity stakeholders interviewed for this project is that state entities invest money and provide informational resources, yet this disconnect between parties persists, and there still exists significant dissonance in the public sphere regarding cybercrime. As participant one notes regarding the awareness and training measures often exclusively shared by private entities and public or federal actors, “out to the public; yeah, I think there's still an opportunity.”

As mentioned at the beginning of this section, narrowing the scope of threats is a critical aspect of addressing this disconnect between stakeholders. The discourse generated surrounding threats has been demonstrated to be misleading in the cybercrime literature (Mesko and Bernik, 2011). This is especially true when one group of stakeholders possesses an inordinate amount of influence over discourse generation or public opinion (see Dunn-Cavelty, 2013; Hill and Marion, 2016; Kremer, 2014; Wall, 2008). As such, with the disconnect between stakeholders substantiated by the participants of this study, another theme made apparent in the interview data was a general uncertainty regarding the threats that warrant the most attention in the digital space.

Uncertainty Regarding Threats

The cross-section of stakeholders interviewed for this study provides an interesting opportunity to survey the different perspectives on threats in the digital space. According to Neufeld (2023), “academic, legal and practitioner responses to cyber threats have been predominantly reactive, punitive, and deterrence-based” (p. 1). In conjunction with the public criminology literature explored above, punitive crime control measures are often accompanied by emotionality and can lead not only to misleading discourse (Carrier, 2014), but ineffective justice practices as well (Neufeld, 2023). One of the ways that this punitive narrative manifests in both the existing literature and the interview data is through sensationalized accounts of crime. Especially when examining a rather contemporary discipline of criminology, such as digital crime, it is easy to allow enigmatic qualities to shadow our understanding of the reality of this phenomenon. One of the justifications for this project is that it provides an opportunity to hear from experts across various sectors of cybercrime unencumbered by popular media portrayals or policy-making applications (that is not to say that the respondents’ offerings to this project are completely unbiased).

The sensational versus mundane accounts of digital threats subtheme that emerged in the interview data yielded many interesting findings pertaining to awareness. Before gathering this data, it could be reasonably assumed that the sample of stakeholders queried for this project would display a general consensus as to the primary threats despite the fact that the participants are stratified in their expertise and experiences. Considering that these individuals spend much of their time speculating about digital crime, if not directly applying their knowledge to active investigations or research projects, it was surprising to peruse the interview data and have difficulty deducing an overarching threat that the majority of actors put forth. The criminological literature provides an interesting context for the phenomenon of uncertainty regarding threats, some of which were explored above. For example, much has been written about media portrayals impacting the public perception of cybercrime, specifically malevolent or omnipotent 'hackers' (Wall, 2008). As information sharing has become less hierarchical and the criminal justice system becomes increasingly quantified, Lavorgna and Ugwudike (2021), employing a postmodern epistemology, note that scrutiny of the framing of the technologies central to digital criminology is imperative as it is these frames that shape and organize the public's understanding. Therefore, examining how these stakeholders frame the threats to be most concerned about can accomplish the manifest feat of understanding how experts frame these issues to the public as well as the more latent implications of how these threats have been framed to aid the experts' understanding prior to participating in this study.

Firstly, many participants who provided context or examples for their responses when asked what the main threats the public should be concerned about in the digital space are, seemed more grounded in their perception of threats. Specifically, participants who worked directly in information security or worked closely with IT departments seemed to provide an account of danger that was distinct from what may be considered *popular* notions of cyberthreats, in other words, sensational accounts of cybercrime. These responses were usually accompanied by a technical understanding of the issues and how they are dealt with on a practical level. It is worth noting here that the *playing dumb* interview strategy mentioned above was most prominent when the discussion would shift to descriptions of security measures or practical accounts of attacks. This may have had an impact on how intricate a participant’s response to this cluster of questions was.

Further, the response's intricacy may impact whether the researcher views the threat mentioned as supported by an expert opinion; conversely, a simple reply may lead the researcher to deem that the response constitutes a popular conception, regardless of the inherent truth in the participant’s answer. For instance, ransomware was a threat that was explicitly noted in five of the eight interviews conducted for this project. In four of those five interviews, ransomware was described as a primary threat that is both prominent and worthy of the ‘public’s’ consideration. When asked what the prominent cybercrime threats are currently, participant eight, a federal agent, unequivocally stated, “It’s ransomware. I mean, it’s just rampant”. Participant six, the CISO at a large tech-focused corporation, when posed the same question, responded, “I think the primary one has been ransomware; I mean, it's the most predominant and most reported on.” Here we can see that, though unprompted, by the interviewer, the participant seems to partially separate their expertise and experience by including an acknowledgement of the level of awareness that a threat appears to garner, a subtheme that will be explored in more detail below. Further, participant two, who mentioned ransomware as a threat that perhaps generates more attention than warranted had this to say:

> “I think it depends on the time of the year, right? Right now, I think everybody is super focused on ransomware for some reason; they think that's the biggest threat out there.… so that all changes depending on the tactic and what is the flavour of the month if you want to call it that.”

The inclusion of the disclaimer that people *think* ransomware is the biggest threat implies that the opinion of the participant is that this notion is untrue. Another interesting notion highlighted in this quote is the idea that the popular conception of *true* threats is constantly changing. It is not entirely clear whether the interviewee meant that the threats change with the "flavour of the month" in a practical sense or if the general consensus shifts while the threats remain constant (it is likely that both are true, in some sense).

Another threat that may fall into the less-sensational category of this subtheme is the theft of personally identifiable information. Though identity theft may be one of the more commonly reported cyberthreats (see Neufeld, 2023; Reynolds, 2022; Whitson and Haggerty, 2008), the researcher decided to include it with the practical threats due to the participants' ability to include anecdotal evidence with their claim that identity theft is a legitimate area of concern for the public. That is, the sensational threats that will be described in more detail below were partially distinguished by the vouching interviewees' inability to provide experiential accounts of the threat signifying that those threats may be more akin to what the general public may provide as a response to this question while lacking any specific expertise with digital crime. Participant eight, a federal agent, responded that for the individual, the theft of personal information such as credit card numbers and social insurance numbers "is really at the forefront of what cybercrime is today." Participant seven also emphasized the importance of risk mitigation in terms of incautiously utilizing credit cards and oversharing other personal information, implying that the individual is often at risk of identity theft during their everyday routine. The CISO, participant six, also noted the diligence required in protecting personal information by describing how the amount of confidential information, such as passwords and other digital access keys, has increased drastically and necessitated a more regimented approach to personal security online, an approach that may prove difficult for older or less tech-savvy generations according to the participant.

On the other hand, sensational threats, as mentioned above, were deemed by the interviewer to lack basis in real-life experience and are perhaps influenced by hearsay. It should be noted here that a participant providing an account of a threat deemed sensational by the researcher does not indicate that the interviewee is unaware of the *true* threats or that the sensational threats are not based in fact. The sensational label denotes that the threats provided by the participant may be seen as more romantic and explained with less anecdotal experience than the threats labelled mundane from the interview data. Further, the sensational threats derived from the interviews were sometimes accompanied by a fatalistic perspective contributing to the romantic ideals mentioned above. Participant one, when faced with the question of what cyber threats are the most prominent right now, responded that machine learning (which they described as “bad guys” creating very detailed profiles of individuals based on their technologies) was one of the threats that the public should be aware of. The same participant hypothesized that cybercrime generally is headed toward more “sophisticated attacks” as the way of the future. The exchange presented below provides context to the sensational nature of the threats described by this participant:

> **Interviewee**: if you think about – what's it called now? The virtual reality – like the hacker would be able to recreate my brother's face and have my brother send me a video and talk to me and stuff like that with all of the information about that… that would just make me convinced it's him, sort of thing – so that…

Interviewer: …Yeah, those deep fakes. Yeah.

Interviewee: Yeah, the deep fakes. Yeah. So there's that.

The interviewee in this instance, a business analyst for a financial institution, provided threats that seem partially removed from their experience working in information systems. This dissonance becomes more apparent when juxtaposed with the account of mundane threats provided above, in which case participants would detail their experiences with different cyber incidents in the context of their profession. The participants that cited sensational threats as most prominent seem somewhat speculative. This speculation may be a function of the participant’s expertise diverging from practical-level threats or active investigations as opposed to a lack of awareness. For example, participant three, a career academic, notes that the main threats the public should be concerned about have evolved considerably since they were studying these issues as an undergraduate student. This interviewee feels that the major cybersecurity issues were more practical in the past and revolved around the abilities and limits of the technology in question. For example, the professor cites a past concern about secure and encrypted storage with the caveat that if users did not actively store sensitive personal information on their computers, they were generally safe. The interviewee contrasts this with the machine learning threat mentioned above; that is, a social element now pervades the cybersecurity landscape. The participant notes that even if users are cautious about their technology use and display effective cyber-hygiene practices, machine learning via artificial intelligence is able to gather potentially sensitive information on a target. We can see a thread of humanism is imparted on the sensational branch of threats derived from this interview data, especially when compared with the mundane threats. Echoing participant six who championed the reverse-mentoring project, participant one noted:

> "So that's – I think that's an important dimension of cybersecurity as we move beyond. We've been so fixated on, just the technical stuff, that now it's – I think we're probably moving into a phase where those creatively minded people like… so this flows out of, you know, the agile framework and all that stuff the guys 20 years ago said… that creative responses to solving problems, right? I think we're moving to a phase…where cybersecurity is going to be able to be like this. Many of the things are going to like… the basics are going to be there, so now you're going to able to take the basics to the next level."

The sentiment expressed in this quote seems to be that contemporary cyber threats cannot be dealt with solely through technical means. The sensational threats especially require human mitigation as they exploit something other than technological infrastructure.

Participant three, a career academic, provided more threats that would fall under the sensational umbrella. Namely, they expressed concern over the recent proliferation of AI, specifically, ChatGPT. The decision to label this threat as sensational was based on the participant comparing ChatGPT to "Skynet" from the *Terminator* film saga. It seems that this interviewee views ChatGPT and other artificial intelligence as akin to sentient technologies often represented as malevolent in popular sci-fi films. Much has been written about the portrayal of cybercrime and cybercriminals in popular media (see Conway and Hadlington, 2021; Shires, 2020; Wall, 2008). This participant also alluded to the movie *Ex-Machina* in describing robots learning about hate and other human emotions. Films and popular media often purport a romantic or sensationalized ideal of digital crime. They can even be detrimental to public understanding of the phenomenon due to the emotionality inherent in inaccurate reports. Conway and Hadlington (2021), in an analysis of undergraduate students' perceptions of cybercrime claim that the empirical nature of academia and policy-making clash with the inflammatory essence of sensational accounts of digital crime. As such, "This discrepancy may impact on the successful communication of information from academic and legislative resources to the public, in turn explaining why there is a heavy reliance on other sources such as the mass media" (Conway and Hadlington, 2021, p. 120). Thus, these sensational accounts of threats informed by popular media and provided in the interview data for this project may be counterproductive to a public cyber-criminology.

Participant six also expressed concern over ChatGPT and other AI-based technologies. Though the participant did not explicitly list ChatGPT as a threat, they utilized the software to illustrate a broader conversation on the nature of digital threats and the public's understanding of them. They stated that the impact of ChatGPT over the last three months has been ubiquitous and represents the cybersecurity field's inability to keep up with threats. Specifically, the participant stated:

> "I think we were probably capable of a 10 percent change in digital transformation per year. Now we're seeing more like a 10 times change in the digital transformation. So our ability to not only comprehend but build laws… to build governance models, you know is one thing but also just the – if the average, everyday individual's ability to comprehend and understand how these technologies fit into. It's difficult. And then security becomes, you know, just another layer of part of that discussion, and it makes it even more difficult."

According to the participant, this comprehension difficulty also extends to our research capabilities. Threats that are evolving to become more complex (and thus, sensational), such as AI software, hinder the research process as the lines of how to operate according to ethical standards safely become blurred when dealing with technologies that are not fully understood. As a visualization, the interviewee stated that the human mind has a linear ability to absorb new information while technology and digital crime are advancing exponentially. Similarly, participant five, a program manager at a cybersecurity vendor who was interviewed for this project maintains that with “the hysteria around AI,” the threats that their teams are trying to defend against are growing exponentially while the availability of tools they have at their disposal (both technical and otherwise), follow a linear trajectory.

The above data are representative of a subtheme that emerged amongst the ‘uncertainty regarding threats’ main theme; that is, the media’s impact on each respective stakeholder’s understanding of threats. Participants would often include a discussion of how the media affects public understanding of issues regarding cybercrime, even if unprompted by the interview guide, signalling that the stakeholders queried for this project understand the inevitability of popular media acting as the main reservoir for a relatively complex field of criminal justice. Participant five, the project manager for a cybersecurity vendor, mentions that “log4j is the current vulnerability that’s in the media”. They continue to discuss how the “24-hour news cycle” impacts their company’s business dealings. Specifically, the interviewee mentions, after establishing that log4j is the current ‘hot topic’ in an otherwise revolving door of threats that garner media attention, that when a news story regarding cyber incidents breaks, their company sees a massive uptick in support cases with customers wondering whether or not they are "covered" with respect to the *new* threat. Participant two who works in litigation noted something similar. The interviewee provided a fresh perspective on why the media may play a large role in informing customer awareness, specifically for corporate entities. They note:

> "You have to realize – board of directors or client CEOs… They're not dealing just with cyber all day long. They're dealing with a lot of other things. So, they may have a cursory knowledge to go, 'Hey, I saw this company got hacked in the media. You know, is that… is that something that can happen?' They'll just focus on that particular type of attack. And so, the goal for us is when we speak to them is saying, 'Look sure that does exist. Ransomware is a thing, and it's a big thing, but there's so many other risks that are facing your organization right now which are probably more critical."

This response expands on the project manager's insight. Whereas the project manager seemed more dismissive of the media's effect on business dealings, the litigant implies that media coverage may steer decision-makers who, as mentioned, do not solely focus on cybersecurity away from the true threats as posited by experts. This could lead to resources being incorrectly allocated and, ultimately, perhaps, unnecessary vulnerabilities in a business' cybersecurity infrastructure. This example of misleading information affecting corporate suite decision-making harkens back to participant five, the project manager for a cybersecurity vendor participant. This interviewee gave the contemporary example of a current threat, log4j, a logging software that allows IT staff to keep track of application activity. As mentioned above, log4j was considered a main vulnerability in the tech world at the time of data collection, and the participant mentioned that people outside of the technology realm hear about the software due to the media coverage (in the participant's words; "the 24-hour news cycle") and yet do not know much about the issue. This leads to undue attention on the threat from c-suite clients when in reality, information security experts understand that a simple patch can rectify the vulnerability. The participant called this type of media reporting "a distraction" again illustrating that the media may have a detrimental impact on business proceedings regarding cybersecurity, at least from the corporate perspective. However, these two participants admitted that board members and other corporate actors are usually quick to "defer to experts" once their concerns are acknowledged.

Participant eight provided another unique perspective on the media's impact on digital threats. In discussing public awareness of digital threats, the interviewee noted that the news media is quick to publicize information surrounding incidents occurring within large corporations. Specifically on the subject of ransomware, the participant stated that when large companies experience a breach and are forced to pay a large sum of money as ransom, the media will often report that sum to the public, and this "catches the attention of the c-suite." This quote is supplementary to the notion of informing customers about breaches mentioned in the disconnect between stakeholders theme. Media attention seems to impact how private companies handle breaches and may affect their likelihood of paying ransoms.

Possibly due to the phrasing of the question in the interview guide in some cases, many participants distinguished between the real threats and what threats are most reported, implying that those two phenomena are mutually exclusive. As seen in participant six’s interview data and described above, sometimes that distinction was made without prompt indicating that the threat being reported the most and occurring the most are one and the same. This is evident in the log4j example provided above, where participant five felt that the threat receiving the most attention was more of a distraction than something the public should be legitimately concerned about. In total, four of the eight interview participants noted that a specific stakeholder was overly focused on a threat that, in their opinion, was not the most prominent. For example, participant six, the CISO, posited that identity theft and ransomware are both vying to be the most imminent threat though the latter is more often reported on than the former.

Further, according to participant seven who is employed by a federal agency in the U.S., the popular narratives espoused through the media and amongst the general public lead people to “fear the wrong thing.” Specifically, the participant pleaded that citizens are worried about being watched by the government when, in reality, “Apple and Amazon and everyone else along the path is buying your information and watching it.” The interviewee digressed to say that people who are *in the know* regarding cybercrime and cybersecurity are able to differentiate popular ideas from legitimate concerns, implying that those who are unwilling or unable to gather information and educate themselves about these issues will remain uncertain about digital threats. This subtheme will be explored in detail below. Another facet of the media’s possible misrepresentation of threats seen in both the digital crime literature and in the interview, data is that, as participant two states:

> “The other part of this… we don't talk about at all, I find, in the media… we should, is corporate espionage. There are bad actors out there that are stealing –

> they're conducting cyber-attacks, not because they want to make money, although that's a big portion of it, because they actually want intellectual property."

These claims relate to the abovementioned concerns regarding the theft of information by companies such as Apple and Amazon. It appears that the media is eager to display the digital threats that manifest most often at the individual level, such as ransomware and identity theft. As noted above, most participants detailed threats that affect citizens on a micro-scale. However, upon further examination of the interview data, it becomes apparent that many of the participants are also concerned about threats on a macro-scale. For instance, two participants spoke in detail about data integrity, which reflects the general public's willingness to trust the cybersecurity of institutions they interact with. A specific example of the compromising of health data through digitally stored hospital records was provided in two of the interviews. The data integrity conversation is an important illustration of how threats to institutions (state or corporate) can manifest for the individual citizen or consumer; in the case of health records, scrambling of blood types was discussed in one of the interviews as an infringement on data integrity that threatens the individual *and* the institution.

It also became apparent during the course of the interviews how crucial the acknowledgement of the intertwining of state and corporate institutions is, blurring the lines of distinction between threats against one or the other. This was alluded to during the discussion of PPPs above, as well as the difficulty that globalization causes when examining overseas third-party vulnerabilities from the corporate perspective. In this vein, corporate espionage being mentioned by participant two who works in private litigation manifested differently in interviews with federal investigators. Evidently, two federal agents who were interviewed for this study mentioned state threats as being a concern; however, both participants seemed more concerned with the micro-level threats of ransomware and identity theft mentioned in detail above. The state threats briefly described in the interview data were “advanced persistent threats” embodied by foreign actors. According to participant eight, these foreign threats stem from the governments and militaries of China, Russia, and North Korea, which will hire tech specialists who *moonlight* as hackers to steal intelligence from the United States and their allies. According to this participant, this threat could have catastrophic implications, but citizens are indifferent to these issues and, thus, unlikely to educate or protect themselves; this subtheme will be examined below.

Perhaps as a consequence of discussing sensational threats, a somewhat fatalistic narrative was detected amongst some of the interview transcripts. In an interesting contemporary analysis of cybersecurity discourse, James Shires (2020) compares the dystopian underworld of sci-fi and noir films with the moral ambiguity often associated with perceptions of cybersecurity. A vital element of the film genres analyzed by Shires, specifically film noir, is the theme of fatalism. Further, Shires claims that “a significant dystopian strand of science fiction–often labelled “cyber-punk”–is thus not easily distinguishable from noir” (p. 89). Shires and other similar research (see Banks, 2017; Wall, 2008; Yar, 2008; Yar, 2013) have established the tendency for deterministic attitudes to enshroud digital crime discourse, a phenomenon prevalent in the interview data. For instance, participant six was able to, either intentionally or otherwise, draw on common topics found in criminological literature to describe the fatalistic narrative that accompanies certain digital threats, stating that a trope that requires debunking is that “hackers are omnipotent. Hackers can fly. Hackers can stop bullets with their mind. There's nothing we can do to defeat them because they're superhuman, right? We see, you know, on TV how a hacker is represented”. Toma, Décary-Hétu, and Dupont (2023) label this threat the *superhacker*, a myth that allows corporations to absolve themselves of responsibility for victimization due to the notion that this villain cannot be thwarted. Evident parallels can be witnessed between Toma, Décary-Hétu, and Dupont’s (2023) research and Garland’s (1996) theorizing on responsibilization. The fatalism displayed in the interview data is a useful depiction of the difficulty in establishing certainty amongst stakeholders regarding threats in the digital space. The idea of omnipotent, malevolent hackers contributes to this mystery by invoking a sense of romanticism and determinism, especially with respect to the inevitability of victimization commented on by many of the interviewees as well as the extant literature (see De Kimpe et al., 2022; Reynolds, 2022).

A significant amount of attention was given to victims in the data contributing to the fatalistic subtheme. For instance, four participants implied that individuals do not care about their privacy when navigating the digital space, and thus, are complacent in this uncertainty regarding threats. Participant eight stated:

> "Part of it, I think is we've been conditioned at least, you know, North America and most of you know, Westernized Europe. That no one even cares about privacy anymore. Really comes down to the cyber side as…Where you’re sharing everything you're doing online? They don't even think twice about anything, they put online, or who they're giving it to. So, I think there's really no concern at all. I don't think they think about it [risk of personal data being weaponized], honestly."

The fatalism in this response is evident. Claiming that individuals are indifferent toward their personal liberties as evidenced by the fact that they are not secretive about their activities may be an example of victim-blaming. Participant one expressed a similar sentiment, saying that citizens are displaying blissful ignorance in their online activities. Specifically, the interviewee imagined that individuals think:

> "'Yeah, whatever, they have it all anyway [personal data].' Also, the… you know, 'my app will automatically… You know, my application already turns off my privacy. I'm fine not realizing you know… to go look at exactly what they're doing [what information corporations are gathering] because they're like -everything's off'. So yeah, there's kind of like a 'I'm too busy. I don't want to deal with it. It's too complicated, It's not easy to access'."

Both of these responses may seem paternalistic in their depiction of the citizens' awareness of and resistance to digital threats, a possible illustration of Millman, Winder, and Griffiths' (2017) *unhelpful victim*.

Another subtheme emerging from the data pertaining to uncertainty regarding threats was the *differences between the physical and digital worlds.* The emergence of Castell's (2010) network society has led to new forms of social organization and the development of global networks of communication and information exchange. However, these technological advancements have evidently created new opportunities for digital crime. Turkle (2011) argues that technology has led to a decrease in face-to-face interactions and thus, human connection, and has contributed to a sense of isolation amongst citizens. This disconnect holds negative implications for social cohesion and, as a result, education as well. However, among participants in this study, fatalistic narratives, and comparisons (or contrasts) between the digital and physical world seemed intertwined. Participant six, a parent, made the distinction between cyberbullying and traditional schoolyard bullying, admitting that they understood the latter from experiences in their youth, but they felt unable to protect their kids from the former because they did not grow up with cyberbullying. In this example, we can find traces of fatalism in the anecdotal contrast between two phenomena that manifest differently whether they are experienced face-to-face or through networked technologies. This interviewee also felt that people are too quick to apply assumptions about the physical world to their digital counterpart. Like participant three that mentioned the contrast between licensing requirements for activities such as driving a car and becoming employed in the information security sector, participant six stated that "we're drawing parallels to the physical world or what we're used to and we're applying it to the digital space, and they just don't translate." This example extends to the amount of regulation imposed upon goods or services in the physical world as opposed to online according to the interviewee. The participant gives the example of safety standards for appliances or cars, claiming that the diligence necessary in meeting those guidelines does not apply to many networked technologies that are even more ubiquitous. Another interviewee, participant three, echoed the above sentiment by stating that the government is able to legislate responsibility on various parties much easier in the physical world than in the digital world, possibly due to the jurisdictional issues mentioned above (amongst other factors). We can see that strictly demarcating these two realms can contribute to the air of mystery that enshrouds cybercrime, both in popular discourse and policy. The role of technology in the broader, social lived experience is multifaceted, and the implications of technological threat advancements require a deeper analysis of the human experience in relation to navigating the online space.

The final subtheme in *uncertainty regarding threats* is the human or social engineering aspect inherent in digital threats. As with the fatalism and paternalism examined in relation to sensational threats in the digital space, the individual consumer or citizen plays an interesting role in the uncertain dialogue surrounding these issues. As alluded to in discussing sensational threats and creative avenues to problem-solving, many of the participants cited social engineering as one of the prominent threat themes. There seemed to be some agreement amongst participants that many of the threats outlined above, in their inception, take advantage of human nature in some form. As participant seven stated, even when aiming to extort large institutions, “you [criminals] always have to start with the people.” In addressing the human engineering aspect of cybercrime, this participant gave an example of individuals digitally impersonating high-level staff at large corporations and requesting money transfers or sensitive information from other employees. This specific dilemma was mentioned by another participant as well. Participant eight, a federal agent, contextualized this threat by stating:

> “Now you have hackers… their only job is to… they go on LinkedIn, and people are saying ‘Oh I'm a… you know, an Oracle administrator for… you know, say IBM.’ They start watching that guy, targeting that guy, because if they can get *him*, he might infect the system for them because they figure, he's got admin rights. So, they might hack his home computer, his home system, his cell phone whatever they can get. And then eventually, they use him to get access inside of the business, and he doesn't even know it.”

Here we can see that human engineering, according to these participants, does not only apply to sensational threats, as posited above. Instead, even for a *mundane* threat such as ransomware, cybercriminals take advantage of creative techniques to perpetrate.

Part of the reason why this human engineering aspect to cyberthreats is prevalent right now according to many of the interviewees is that the *technical* facets of cybersecurity are bolstered so well that 'bad' actors are forced to adapt to these evolutions more creatively by exploiting people instead of technology. As participant four says, "Hackers, to say the least, are smart people, and you know, you close one hole, they'll find another way in." Similarly, participant eight claimed that:

> "The technical security has gotten so *good,* and they've done a great job of, you know, having great patch management. So new patches come out for the servers, production lines, they're getting them installed quickly. And so that vulnerability is not there so much as it is the human vulnerability…you know. You hear them say, we're [humans] always the weakest link. I mean, it's true.'

Here we can see another example of a participant implying that one of the true concerns for cybersecurity, in general, is not any one practical threat, but the inevitability of humans interacting with these technologies and eventually making mistakes. This dilemma holds interesting implications for awareness, outreach, and security, especially considering how many of the participants reported that often, an individual is exploited as a vector to high-priority targets. Participant one, who works for a financial institution wrestled with the consequences of this inevitability and theorized about how it might be communicated to the public. This interviewee thought that it may be prudent to admit to customers that a large majority of breaches and incidents are caused by human error (phishing or dupes, in their words); they suggested that “the big message needs to go that ‘we've gone as far [with respect to technical security] as we [financial institutions] can, and with all of our protection, still if you let them in, they're going to get in.’”

Participant five, as mentioned above, is employed by a cybersecurity vendor and as such, is well-versed in the technical aspects of information technology. Surprisingly, this participant also attested to the prominence of the human engineering ‘issue.’ In a detailed description of tangible threats, this participant noted how their firm’s approach to cybersecurity software has evolved in accordance with the shifting nature of cybercrime in general that most participants seemed to convey; that is, a change from bolstering the technical facets of security to ensuring the mitigation of human error. The interviewee notes that their firm’s approach is less about endpoint security than application behaviour. As the participant describes, the competitors’ approach involves detecting malware files more so than making sure that “the people in the building are doing what they’re supposed to.” This approach holds the advantage of being able to scrutinize those who have access to secured networks or sensitive data, legitimately or otherwise. By detecting application behaviour and flagging anomalies, the firm’s cybersecurity team can assess individuals’ interactions with digital assets beyond the black box of having access to these systems. The participant mentions that often times people who were once cleared to work with sensitive digital information may never have their clearance revoked even though they have shifted projects or are no longer employed at the same company. This can evidently lead to a host of issues, but this approach to cybersecurity can profile users based on histories of interactions and is thus, more holistic than a purely technical strategy.

The same participant gave an interesting anecdotal insight into the ways in which general cyber-hygiene training has attempted to account for human error. The interviewee says that an inside joke for infosec professionals revolves around ‘silly’ 20-minute seminars that corporations hold quarterly to educate employees on how to avoid infecting the technology that the company utilizes. According to the participant, these seminars include skits about not plugging in USB devices found around the office and not leaving customer information open on your desk during breaks. Further, the participant admits, upon describing another seminar trope of not holding the door for people trying to enter their building without security clearance or identification, “that's what bad actors are taking advantage of is just normal human nature.” Participant three also spoke about human error in matters of cybersecurity through an anecdote. This participant drew on the story of a doctor who accidentally left their notebook with patient data in a public place to be stolen. According to the interviewee, this event changed the entire landscape of health data security and led to the encryption of health data in Canada. Evidently, the skits are somewhat trivial for individuals already employed at security companies; however, the examples given here provide insight into the mindset of some organizations in terms of implying that many losses can be avoided by minimizing human error.

Responsibilization

The third prominent theme gathered from the interview data was *responsibilization*. As explored in the literature review, many scholars have dissected the role of responsibility in incidences of cybercrime victimization (see Wall, 2008; Whitson and Haggerty, 2008; Yar, 2013). However, the variety of stakeholders queried for this project provides an interesting perspective on this phenomenon because many participants, specifically those outside of academia, are likely not aware of the literature (for research critical of responsibilization in cybercrime see Banks, 2015; Yar, 2008; Yar, 2013) in condemning the responsibilization of the individual and the neoliberal attitudes that this trend stems from. Further, a benefit of the methods employed in this project, specifically the interviewing techniques informed by Reynolds (2022) and Holstein and Gubrium (as cited in Silverman, 1997), is that the interviewees' attitudes towards responsibilization made apparent throughout the conversation may prompt the adaptation of the questions posed by the interviewer and thus, see the interviewer playing dumb or utilizing the role of the devil's advocate to explore these narratives from different angles. In general, the majority of data gathered for this project pertaining to responsibilization seemed to segregate into two subcategories: the responsibility of the consumer, employee, or citizen, and the responsibility of the larger entity (corporate or state).

For the subtheme of the responsibility of the larger entity, the participants seemed sympathetic to the consumer or citizen's experiences. However, some participants claimed that responsibility should fall to the larger entity (perhaps in an attempt to appear sympathetic) while implying, without explicitly stating, that, in truth, the individual is largely to blame. This finding was most apparent in the discussions of social engineering. It is also worth noting here that the responsibility phenomenon, in reality, is not a dichotomous issue; two participants noted that responsibility, in this case, should be viewed holistically or as a shared burden between the micro and macro structures of society. The first interviewee who expressed this viewpoint was the CISO of a large tech-corporation, participant six. When the theme of responsibility was explored during the interview, the CISO referred to an inside joke in information security stating that:

> “There's a comic you've probably seen. It's a boxing ring, and they said, you know, in this corner, it's, you know, cybercrime, malware, ransomware. And in this corner, we have Dave, the user. What message does that send to Dave? You know the intern, it's always your fault. It's the employee, right? So that's one thing. It's always the user's fault as a narrative. We need to break.”

This example implies that the participant acknowledges the absurdity of placing all of the responsibility for cybersecurity on the individual, in this case, an employee who is presumed to threaten a company by being incautious online. Evidently, the interviewee, as a professional with expertise in cybersecurity, is sympathetic to the user's experience and the difficulty therein. Further, the comic cited in this example may serve as an example of how the victim of cybercrime is perceived in society. As this comic seems to be tailored toward those who are tech-savvy by depicting a *lowly* citizen as the face of human error pitted against a slew of cyberthreats more imposing than their opponent, it may provide insight into the opinions of people employed in IT or the public more generally. The CISO participant also revealed some interesting perspectives about the general responsibility narrative in the corporate world. In speaking about the responsibility of the company in matters of cybersecurity, the interviewee noted that the company has a duty of care to its customers much like in other facets of the corporate world, such as accounting matters. According to participant six, companies abide by an abundance of regulations and training requirements to serve their customers legally and ethically, a notion that does not exactly translate to cybersecurity. Participant six says that “We've got two–three hundred years of generally accepted accounting principles that does not exist in cybersecurity, so you need to figure out how you're going to develop that one step down." The sentiment expressed here seems to be that the company should not absolve themselves of responsibility in cybersecurity since human error accounts for a large percentage of the reasons for victimization. They appear to champion the importance of what they term *cyber literacy* in their company. Evidently, this may be seen as placing the responsibility on individual employees to be educated in these matters, however, their insistence on creating a culture of diligence in their company implies that they recognize the importance of absolving the customer or user of some of the burden. This participant continued to state that:

> "I think as individuals, we're always responsible for our own choices. So rather than… whether that's the consumer or an employee. So, we can't abdicate that sense of responsibility. We, you know, we make choices when we drive a car, you know, to drive it safely… we make a choice to make sure we're properly licensed, that it's maintained and whatnot. So, I think it can't be a zero-sum game where one individual or whatnot has the responsibility, but extending the car metaphor, you know, we have a responsibility or accountability. The person who built that car, built in safely, but we have to, we have to maintain it. So, there's a shared responsibility. Well, we can expect that the government will, you know, maintain the roads, but we have to drive within the laws. So, I think it can't be an all or nothing approach. So, we as individuals can't just say well you know we're responsible or we're not responsible because I downloaded the app and it was in this App Store, therefore, should be saved and we can abdicate that responsibility but, the manufacturer of that app or software has a responsibility

> to the consumer. The government has the responsibility to regulate, you know, whether it's an acceptable use or whatnot of the technology as well."

We can see here that the participant acknowledges the responsibility of the individual while also highlighting the importance of diligence on the part of the company and does not engage in blaming victims for lacking the necessary skills to be completely safe online, a common theme in the cyber trespassing literature (Holt and Bossler, 2014). Participant four, a professor and cybercrime researcher also feels that the responsibility for online safety is a shared one. This participant states that due to the amount of time that people spend online and how much of their interactions are mediated by technology, every sector, whether that be consumers, government, or corporations, "everyone is impacted," and though some corporations and government entities try and promote awareness (sometimes ineffectively) there has to be a holistic commitment to ensuring safety that starts with the education of young people in schools.

As mentioned above, some of the interviewees seemed non-committal to whether cybersecurity responsibility resides in one sector or another. One example of this from the interview data is illustrated by a business analyst for a financial institution. Upon being asked whether cybersecurity was an individual responsibility participant one stated:

> "I think no, I think that like… I think consumers, um, consumers should expect that… companies, providing services, you know, and so you're paying for… you pay for your bank with the service fees and things. Um, but anything, you know, your Spotify and, and Facebook, or things like that. So, I think that I have… I have an expectation, a reasonable expectation, that these companies that I conduct commerce with are going to be… are going to have effective security

> controls in place. So that's… and I think, you know, honestly in our – in our privileged, selfish society, baby boomers and gen X'ers, like me, people kind of expect… they expect the company to look after them, but I think maybe it might be useful if a message got out there that 'hey, we've done everything we can but… and the fact is'… and I think a lot of people are… 'the fact is, is that 95%' or whatever you could find out the specific stat 'something like 95% of breaches are caused by the human engineering factor'"

This excerpt provides an illustration of the non-committal response that does seem to convey a sensible and holistic approach to cybersecurity responsibility while also engaging in a similar sentiment to the boxing ring comic examined above. This participant also provided an anecdote in which they called some of their Facebook friends *cheap* for not paying "the ten bucks a month" to purchase antivirus software. This example is reminiscent of Banks' (2015) notion that corporations and the state work together to create a 'reassurance gap' by maintaining fear surrounding digital crime; this fear then leads to profit through the sale of private security services or antivirus software.

Some participants approached the question of cybersecurity responsibility with more practicality. Specifically, participant 3, a cybercrime researcher and professor, seemed adamant that the larger entities should shoulder most of the responsibility for cybersecurity due to the fact that "if you rely on the end-user or the parents [it can be] too difficult [for them to bear the responsibility of cybersecurity], I think sometimes [it is] too difficult. Right, not everyone has the same awareness, level, or even life experience, or educational background to understand." This participant also provided examples from 'normal' life (non-digital) stating that employees of the Liquor Control Board of Ontario

(LCBO) have a responsibility as a provider to make sure that a customer is of the legal age to purchase alcohol. Similarly, they mentioned payment card industry (PCI) standards implying that from a certain perspective, it is easier to legally obligate compliance from providers and supervisors than it is to hold individuals or users to the same standard. This example provides a segue into another notion that was prevalent across the interview data, that is, the inevitability of victimization and the concept of responsibility while bearing that *fact* in mind. As witnessed in the boxing ring comic, the user seems to face insurmountable odds in the ‘fight’ against cyberthreats; as some interviewees implied, the amount of time spent online significantly increases the likelihood of being victimized. Some participants utilized this notion of the inevitability of victimization to responsibilize the user even further, ironically. Though it would seem that the necessity of interacting with technology in contemporary society would absolve the individual of some of the ‘blame’ in matters of digital crime, some of the participants queried for this project seemed to condemn users for *needing* cybersecurity more than they felt they should. Lavorgna and Ugwudike (2021) speak on the importance of analyzing the implications of technology’s social embeddedness for responsible governance of both knowledge and technology (p. 9).

Similar sentiments to the responsibilzing of the individual were expressed in the fatalistic narrative surrounding threats subtheme. Namely, individuals oversharing aspects of their private life online or being incautious regarding sensitive information on digital platforms was a common notion amongst those participants who seemed to feel that the individual should have more responsibility in matters of digital crime. Employing Brown’s (2006) concept of the technosocial and acknowledging the contemporary zeitgeist that holds that cybercrime victimization is inevitable, it is unfortunate that many experts and stakeholders in cybersecurity expressed views that portray victims as ‘unhelpful’ and incautious (see Cross, Holt, Powell, and Wilson, 2021) throughout their interviews. When asked about cybersecurity responsibility, participant two, a lawyer who primarily works in incident response, stated:

> “One thing I will say, though, probably not the most… probably a bit more controversial and not particularly helpful. I also believe the individual is responsible, you… we give a lot of data off the bat, you can get whatever app and you know, or you have a promotion going on at a store and they're like, ‘yeah, I'll sign up for this,’ and they think it's pretty benign. ‘I'll just give my email address and my name and address. Who cares about that, right?’ Well, you know, things can happen with it, and when that information does get compromised, they're the first ones getting up in line and saying, you know, ‘that's horrible. You guys should have offered me 10 years of credit monitoring because I'm at risk now.’ Well, you… you as… not you individually, but you like… generally, as a consumer, you guys should be thinking about what you're sharing and where you're sharing it.”

Though this participant also admitted that the company can never be fully abdicated of responsibility as the custodian of customer information, their insight into individuals’ responsibility may shed light on the apparent negative stigma around human error in cybersecurity, similar to the ‘privileged and selfish society’ comments made above.

The sentiment expressed by this participant, however, is one that is partially supported in the literature. For example, Toma, Décary-Hétu, and Dupont (2023) find that “customers are insufficiently motivated to protect themselves from crimes that may derive from data theft within an organization. Instead, the burden of security is placed upon the businesses that host their personal information" (p. 1). It seems in the extant literature that corporations counter this user apathy by encouraging small, manageable steps to reduce risk, a phenomenon some participants in this study referred to as cyber hygiene (Whitson and Haggerty, 2008). Participant eight explained cyber hygiene by stating that individuals should not “cross streams,” that is, avoid using professional technology, such as a company phone, for personal purposes. The same participant noted that this was a prominent issue during the COVID-19 pandemic when many people were working remotely. Participant one echoed the prominence of cyber hygiene issues during the pandemic linking this phenomenon with the human engineering strategy that ‘hackers’ take advantage of, such as phishing attempts targeting phones with smaller displays to disguise incorrect email addresses. In both of these instances, the participants were eager to provide strategies for individuals to mitigate their risk of victimization while appearing unable to suggest concrete solutions for larger entities that could keep people safe. This inability may be a product of the notion mentioned above that the technical side of cybersecurity is so well-bolstered that the human engineering element is one of the primary focuses for these stakeholders, or these excerpts may serve as examples of victim-blaming found in the criminology literature.

One interesting trend in the data gathered for this project was another thinly veiled example of paternalism directed toward customers or citizens. With respect to responsibility, many participants felt that individuals should have more skin in the game so-to-speak. This notion pervaded many of the themes and subthemes examined above.

However, most participants who espoused the idea of giving consumers more liability in cybersecurity, did so in conjunction with the opinion that individuals are aloof or apathetic to some of the prominent cyberthreats detailed above. This accountability imperative seems to have few antecedents in the extant literature. Vance et al. (2015), for example, detail a software that increases user accountability in hopes of preventing access-policy violations, defined as an incident in which "insiders access sensitive information contrary to the policies of their organizations (Vance et al., 2015, p. 346). Access-policy violations were implied in the conversation with a cybersecurity vendor mentioned above, in which participant five noted that their company's approach to security is to ensure that people with access are utilizing the software in an appropriate manner. Vance et al. (2015) note that roughly fifty percent of digital breaches are caused by employees, and the user interface proposed by the researchers utilizes accountability theory to apply psychological principles that subliminally encourage users to justify their intentions while accessing sensitive information. In the current study, participants felt that forcing consumers or citizens to face the *reality* of cybercrime could have many benefits for the field in general. Specifically, participant eight implied that companies and federal entities 'coddle' the general public numerous times throughout their interview. To illustrate, the participant mentioned that individuals are incautious in many aspects of their life, which increases the likelihood of victimization while theorizing that:

> "if there was some… you don't want to say feel the pain, but if, if the, if the population, you know, had some personal responsibility in there, you know, bad habits, misuse of data, credit cards, then they might start paying attention."

This participant provided many suggestions as to how the customer or consumer could bear more responsibility in cybersecurity. For example, the participant felt that there were no drawbacks to overusing a credit card because any loss suffered as a result of a digital crime will be reimbursed to the victim with little or no burden of proof placed on the victim. With this in mind, the interviewee suggested that if a consumer has lost fees subscription fees for six months without notifying the proper authorities, then the individual should not be compensated. Similarly, the federal investigator also suggested that any small crime (any loss of fewer than fifty dollars) should be the responsibility of the victim unless there are some “extenuating circumstances.” It should be noted that the participant did not intend to suggest draconian measures only to punish victims of cybercrime; instead, they were trying to suggest strategies to increase consumer awareness and “get people to care” about the possibility of victimization.

Another federal agent, participant seven, shared similar sentiments with the interviewee mentioned above. This participant deemed the apathy of ‘the public’ towards cyberthreats as a “numbing” or “resignation.” They mentioned that because these dangers are so prevalent, individuals are loath to experience fear or worry because of losing “only 50 bucks”. To counter this apathy, the participant shared similar strategies to the federal agent examined above, specifically, the interviewee suggested that there should be a way to incite fear of victimization in the consumer. There appears to be a trend of frustration with the individual or consumer on the part of the federal agents; it appears that these interviewees sincerely feel that the public is not as worried as they should be about certain digital threats and, as a result, are suggesting mitigation strategies that may appear harsh or unnecessary when taken out of context. For example, participant three, a professor and cybercrime researcher also expressed that “what works [in terms of garnering public awareness around cybercrime] is something bad happening in society.” This participant seems to imply that an effective means of generating interest in cybersecurity is, unfortunately, a public display of the harsh realities of cybercrime. Again, this comment serves as another example of these stakeholders' frustrations with the apathy of the general public. There is an attitude of ‘nobody cares until it affects them’ both implicitly and explicitly stated across various interviews. A thread through the responsibility theme apparent in the interview data was the consumer or citizen's role in causing financial losses for the other involved entities (corporations or governments). Marks, Bowling, and Keenan (2017) note that “the language and ethos of commerce have spread throughout the criminal justice system” (p. 705), and this sentiment seems to be mirrored in the responsibility theme, but also, throughout the interview data.

Capitalistic Lens

One prominent theme that emerged during the course of interviews, despite not being specifically queried, was the capitalistic nature of cybersecurity. Much of the extant cybercrime literature does explore the implications of neoliberal and capitalistic attitudes in cybersecurity (see Banks, 2015; Cross, Holt, Powell, and Wilson, 2021; Jewkes and Yar, 2012; Kremer, 2014), however, articles in this vein tend to examine these implications from the standpoint of the victim or the end-user. In other words, critical articles in the ‘cyber-criminology’ field will devote attention to how the computer crime control industry can sell insecurity through the media or other sources of knowledge and the commodification of crime prevention and security (Whitson and Haggerty, 2008). Some interview data gathered for this project explored this commodification. For instance, participant five called many of the threats detailed by media outlets a ‘distraction’ while another, participant two, stated that companies tend to financially profit off of confusion amongst consumers by selling credit monitoring. Though these topics are insightful and useful to the discipline, the contentions appear to be much more insidious than other interviewees in this project spoke to.

The first subtheme that was apparent and particularly relevant to cybercrime threats was the necessity of framing implications in terms of dollars and cents. We saw a juxtaposition with this in the notion of inciting fear into consumers to counter apathy. However, many participants who worked in both the private and public sectors were able to speak to the importance of the language and ethos of commerce highlighted by Marks, Bowling, and Keenan (2017). This is particularly interesting when considering the disconnect between stakeholders examined in the first major theme. Many participants shared anecdotes of issues with securing budgets from the entity they are employed by or familiar with. One of the strategies utilized in this struggle to secure budgets was to substantiate the threats presented with financial losses. For instance, participant two who works as a lawyer and advisor spoke about how Canada’s economy is very sector-based and any incident or breach to one of those sectors can result in years of work and investment lost either through intellectual property theft or financial loss. This same participant stated that with this in mind, explaining to clients how necessary resource and finance investment in cybersecurity is involves conveying that aside from losing customer data or IP:

> “If you’re an e-commerce business and you get hit with a denial-of-service attack and your website is down for a day, two days, three days, whatever. You're

> gonna lose money. That's a bigger threat to you in some ways than a ransomware attack, maybe."

This excerpt provides a tangible example of how professionals manage the disconnect between stakeholders mentioned above.

Participant five, an employee for a cybersecurity vendor, adamantly stated that the biggest issue in cybersecurity that is not directly threat-related is the lack of investment. Specifically, this participant stated that "most companies don't invest as much proportionally in security as they do for the amount of business they're doing". Interestingly, the participant mentioned that this lack of investment and attention toward cybersecurity are solvable problems, whereas an issue such as the disconnect between stakeholders and responsibilization of consumers is more opaque. This participant continued to state that capitalism is the driver of decision-making and the only successful attempts they have witnessed to convince corporate actors to invest more money and resources into cybersecurity is by saying, "you can lose this much if you don't spend this much on security".

Participant one, a business analyst for a financial institution, spoke at length about the trials of securing funding and other capitalistic influences on cybersecurity while echoing the sentiments of the interviewees detailed above. This participant's professional experience provides a unique perspective on the logistical considerations of a large firm with respect to cybersecurity. For example, the interviewee mentioned the concept of value on numerous occasions, specifically in the context of digital assets and security. They stated that every company possesses "digital crown jewels" and since it is "prohibitive to protect everything all of the time," companies must invest in the highest value-delivering controls. The participant also contextualized the claims of some of the other interviewees in stating that cybersecurity can be categorized as “brown dollars” in business, meaning, investments that do not necessarily yield profit. With this in mind, stakeholders must amalgamate many qualitative and quantitative metrics to show the value of investment into cybersecurity for corporate decision-makers. Many participants noted that an inside joke in information security is that if cybersecurity teams are operating efficiently, high-level officials may not hear from the IT department at all, reinforcing the notion that further investment in cybersecurity is unnecessary.

Finally, a federal agent, participant seven, noted that “cybersecurity has always been kind of last on the list of funding priorities with this, right? Advertising, marketing, employee… just general, whatever. Cyber security threats have always been: ‘Well, we don't have enough money in the budget for the good stuff. Let's get the cheaper stuff, right or…the good enough stuff.’” This interviewee implies that though cybercrime is a prominent topic of discussion for larger entities (as evidenced by their earlier comments surrounding the amount of education that their organization provides to their employees), profit maximization perhaps takes precedence over truly bolstering information security. This idea may provide insight into many of the other subthemes explored above, such as the responsibilization of the individual. In fact, Whitson and Haggerty (2008) examine the historic scrutiny placed on the individual in identity theft victimization and instead suggest that criticism is aimed toward companies that are mismanaged and suffer from a lack of funding or indifference. This participant went on to suggest that companies outsource their IT services to cybersecurity vendors instead of hiring internal support. This outsourcing trend was mentioned in other interviews as well as a way to deflect responsibility from the corporation to the vendor. Participant five was critical of this notion as they felt it was another “black box” for a company to check and further absolve themselves from blame in case of a breach. However, it may be that contracting out IT services is a practical measure that can alleviate some of the expertise issues that were examined above (high-level staff making information security decisions without the proper knowledge or experience). However, an interesting theme prevalent in the data follows logically from this excerpt; that is, is investing money in the problem an adequate solution to alleviating disconnect?

Education

The final main theme that became apparent in the interview data was education as a means to alleviate the disconnect amongst cybersecurity stakeholders. This theme translates well to the public scholarship focus of this project, as dissemination is a significant aspect of focus in the public criminology literature. Many of the thought-leaders queried for this project pointed to education and outreach efforts as one of the possible solutions to both the implied apathy of citizens towards these issues as well as the enigmatic nature of the concepts therein. As mentioned above, proactive education was specified as one of the most important factors in addressing the disconnect between cybercrime stakeholders. This means that early outreach is imperative, and many participants in the current study suggested implementing cybersecurity curricula as early as elementary school. Participant four, a professor of information security, currently partners with financial institutions to educate school-aged children but also notes that, in general, businesses and government entities are not doing enough in terms of outreach and awareness on the cybersecurity front. This program was described as follows:

> "So basically, what we do is just, you know, once a month we… we run an information session about passwords, information session about social media, how to be safe with social media. Information session about malware… Information session… you name it… about digital footprint. And then at the end, what we do is… and we run a number of competitions, one of the things is that they have to… they have to prepare a poster about the things they learn in the program. Plus, if they have extra things… how to be kind of safe online and then… so we run competitions. and kids will print these posters and hang them in the hallway of their schools. And we as well we do sometimes… the finale is a summer camp. Where all the, I mean, at the beginning, we brought all the girls, right now, we're bringing some of them for a… for a week. Long summer camp on Cybersecurity at the end of the summer. Yeah."

This participant went on to theorize how this approach could translate to other demographic groups as well. As participant six mentioned, there are significant generational differences inherent in the navigation of the digital world and:

> "we have a lot of work to do in terms of, you know, educating children in school about the dangers of these things as well. But how do we then educate parents? Because I, as a parent, I'm not required to show up for school and sit and listen to a lecture or a classroom. There needs to be mechanisms to educate us [older generations]."

Interestingly, De Kimpe et al. (2022) find that there are diminishing returns in user education insofar as increasing awareness may lead individuals to feel overconfident online. Instead, a more efficient strategy is informing citizens of the danger while also making them aware of the fact that they can be a victim. This finding is reminiscent of the ‘skin in the game’ subtheme explored above. Many participants in this study felt that the public could only be made to take cybersecurity more seriously if they experienced victimization directly or if “something bad” happened in society. Participant three, an academic, even mentioned that other scholars tend to overemphasize the importance of education when discussing cybercrime and posits that education can be helpful, but individuals relating to stories of victimization would be much more effective.

Participant seven, a federal agent, also teaches a cybersecurity course at a local college and champions the utility of these programs through anecdotes. Specifically, this participant, unfortunately, witnesses shock and incomprehension when they introduce some of the prominent cyber threats to their students. Apparently, there is a false sense of security amongst these students as well as the air of resignation or dejection that was touched upon earlier. An interesting contrast is that different participants spoke to the unawareness of companies *and* individuals in the sense that both parties need to be explicitly told that victimization is a very real possibility in hopes of encouraging these stakeholders to take threats seriously. This unawareness again seems to be one of the main barriers to education, according to some of the interviewees queried for this study. For the individual, it seems that many participants are unsure of the most efficient ways to educate because as participant two who is employed as a litigant and consultant mentioned:

> “I have a feeling that government in particular, law enforcement, believe that, ‘Hey, if we simply make a Web page available, it's going to be great.’ Well, it's

> not that simple. That's not true. Actually, there's a lot more that goes into this thing. And I think general public awareness is pretty poor.”

There was a clear distinction apparent in the interview data between awareness efforts directed toward the public and awareness efforts directed toward employees in the context of their profession. For example, participant seven stated that the Department of Defense is currently associated with three proactive educational agencies: the Department of Defense Information Network (DODIN), the Defense Information Systems Agency (DISA), and the United States Cyber Command. These agencies are responsible for ensuring that the information network infrastructure is conducive to efficiency and safety within the Department of Defense. The interviewee admits, however, that this information is not getting through to citizens, which they largely attribute to the apathy described above. The other federal agent queried for this study, participant eight, held similar views regarding cybercrime awareness and education. They stated that educating the public is a key issue in cybercrime in general – “educating the public that they are a target, there is a big threat against them.” Again, this participant states that the public is loath to educate themselves because they face little or no liability in instances of victimization which is a precursor to the ‘skin in the game’ subtheme explored above.

Participant one, the business analyst for a financial institution, detailed the systems in place to educate employees at their company. Namely, they mention that education is a part of cyber-governance and constitutes one of the control outcomes in the aforementioned NIST. They also attested to the effectiveness of phishing tests that are passed throughout the staff at their company. These tests provide statistics on how many employees fell for phishing to the company and allows them to assess whether their staff is adequately trained. Again, this participant notes that they are unaware of any efforts like this from their organization directed at customers or citizens. Another interviewee, participant five, who works for a cybersecurity vendor provided context for this apparent favouring of corporate entities over citizens in cybersecurity education. When asked if academia is antiquated for educating the general public due to the length of time that is required to publish articles as a contrast to the rapidly evolving landscape of cybercrime, the participant responded that “Gartner and Forrester” fill that role. Gartner and Forrester are examples of two technological research and consulting firms that insiders utilize as an authority in what companies' strengths and weaknesses are. The participant mentions Gartner’s ‘magic quadrant’ tool that ranks companies on different axis with respect to their cybersecurity; they also provide resources when companies are hoping to purchase software or other security tools so they can make informed decisions based on their assessment metrics.

It seems that the general sentiment across the interview data regarding education is that corporate entities and government entities do an adequate job of informing and training their employees, but the general public’s education is significantly hindered because “they don’t care enough.” Evidently, this notion is a microcosm of the larger responsibilization and human engineering themes witnessed earlier in the data. How, then, can we bridge public criminology and cybercrime scholarship to contribute to a productive, participatory discourse that emphasizes justice and safety?

Chapter 3. Conclusion

3.1 Discussion and Conclusion

The challenge of creating awareness surrounding the enigmatic concept of cybercrime begins with addressing the disconnect between stakeholders embodied in the first major theme of the findings section as well as the extant literature. Birthriya and Jain (2022) claim that the lack of understanding among the general public is one of the main reasons why phishing victimization is so prevalent. More generally, Holt and Bossler (2014) state that to guide policy development, the perceptions of many different stakeholders and their approach to cybercrime must be analyzed, while Lavorgna and Ugwudike (2021) task academics with examining how technology is framed to the public and state. This and similar research provide testaments to the necessity of the current project. In saying that, exploring the discernments of many stakeholders in cybersecurity or cybercrime has shown that experts identify similar issues to those that are addressed in the public criminology literature. As mentioned above, the intersection between the two disciplines is scarcely documented upon undertaking this study. The original contention guiding this project was that narratives surrounding digital crime were inconsistent, partially due to the marketized nature of both the discourse surrounding cybersecurity (Banks, 2015) as well as the industry more broadly (Collier et al., 2021). In hopes of addressing these inconsistencies and creating an environment conducive to more responsible discourse and effective policy, stakeholders from the various domains highlighted in the introduction and literature review were queried indirectly about their perspectives on the gap between digital criminology and public scholarship.

3.2 Interpretation of Main Findings

As mentioned, five main themes were derived from the interview data: the disconnect between stakeholders, uncertainty regarding threats, responsibilization, the capitalistic lens, and the importance of education. With respect to the disconnect between stakeholders, one of the prominent subthemes was the competition of interest, a notion prevalent in both the public criminology literature as well as the cybercrime literature. Habermas (1964) stated that competition of interest defines the public sphere, and the same could be said in reference to cybersecurity and the industry's corresponding discourse (as cited in Habermas, Lennox, and Lennox, 1974). Many interviewees implied that the interests of actors from different sectors of cybersecurity are counterproductive to the awareness necessary for fostering responsible narratives. One of the remedies for this disconnect suggested in the interview data was public-private partnerships (PPPs). Christensen and Petersen (2017) posit that PPPs have been viewed as a viable solution to problems imposed by cybersecurity's "uncertainty and the diversity of actors affected" (p. 1436). PPPs are geared toward information exchange (Dunn-Cavelty and Suter, 2009). In that sense, PPPs are reminiscent of Powell, Stratton, and Cameron's (2018) claim that "the democratizing effect of digital technologies has enabled state agencies to engage with the public in ways that were unavailable before" (p. 9). A participatory approach to a 'public cyber-criminology' utilizing the framework of PPPs may yield new opportunities for the responsible discourse mentioned above. Currently, the public criminology and cybercrime literature largely discredits the role of bureaucratic structures and the intersection of academia and ecopolitical institutions in creating a responsible discourse. Many scholars feel that public criminologists have failed to influence criminal justice policy meaningfully, often attributing the blame to the academic's inability to engage effectively with external sectors of society (Chancer and McLaughlin, 2007; Rock, 2014; Tittle, 2004). As mentioned above, Carr (2016) states that PPPs can lead to a market-driven approach to cybersecurity, if this is true, PPPs would exacerbate some of the issues present in the findings section regarding the capitalistic tendencies noted by the participants in this study. Perhaps including a certain brand of public scholar in PPPs could empower the general public in this participatory democracy noted by Loader and Sparks (2014) and Powell, Stratton, and Cameron (2018), thus mitigating some of the marketized tendencies.

With respect to the uncertainty regarding threats, many of the implications for these findings are similar to the disconnect between stakeholders, as the former is largely a byproduct of the latter. The main finding of note in this theme was the contrast between stakeholders citing examples of sensational threats or mundane threats. This subtheme succinctly exemplified the lack of common ground with respect to threats, even among experts. It may be easier to identify the *main* threats when examining crime that occurs in the physical world due to more streamlined reporting protocols and more visible victimization. However, even interviewees who were employed in the same or a similar field had different conceptions of what the public should be concerned about. This subtheme should not be viewed as a condemnation of the stakeholders interviewed for being unable to articulate to the public the main cybercrime threats, instead, this finding should serve as a microcosm of some of the broader issues impacting cybersecurity currently, specifically, the disconnect among stakeholders. With respect to the strategies alluded to above, I believe the notion of a more participatory approach to knowledge sharing could evidently lead to increased awareness of threats both for experts and the general public. As mentioned above, Milivojevic and McGovern (2014) have provided an example of non-hierarchical communication aided by public scholarship, generating responsible discourse. However, some academics have been critical of public criminologists and their ability to affect change. The institutional barriers that inhibit the research of criminologists and their subsequent dissemination to the public also contribute to a skepticism surrounding academics that devalues their insight. Further, the competing voices in crime control issues and matters of cybersecurity characterize an ideologically-contested space that criminologists are tasked with confronting in hopes of effectively informing policy and dismantling the uncertainty (Crepault, 2017). The structural coupling of academia with the ecopolitical institutions of society ensures that these competing voices bring similar sanitized 'evidence' to the table in support of their claims. Thus, the sanitized ideas may be perceived as 'common sense,' especially considering the partnership between criminologists and police officers in evidence-based policy. As such, if institutions are adopting these 'refined' ideas of crime control as suggested by traditional public criminologists, the public may fail to see the value of criminologists in the discourse of policing. As social scientists, criminologists who value interpretative ideas of crime may be marginalized in the discourse of crime control due to this skepticism, and positivistic or 'objective' researchers whose policy suggestions may be more punitive will receive the preference of the public and legislators. Again, perhaps a reimagined criminologist may be able to collaborate with the public in a way that circumvents some of the institutional barriers to effective public scholarship noted by

Tonry (2010) by utilizing their knowledge of crime and criminal justice to contextualize or substantiate the claims from other sectors (government, corporation, police, etc.,).

One way in which a reimagined criminologist may contribute to the social justice orientations of public scholarship is through the deconstruction of the concept of ‘criminal’ in the discourse surrounding cybercrime. Much has been written about whistleblowers and the notion of hacktivism in criminology (see George and Leidner, 2019; Lyon, 2014; Smith, Moses, and Chan, 2017). These conceptions of the ‘hacker’ as multifarious are useful for the stakeholders involved in cybercrime to recognize. As mentioned, the media portrayal of the malevolent and omnipotent hacker does little to further public awareness or generate productive discourse (see Mesko and Bernik, 2011; Toma, Décary-Hétu, and Dupont, 2023); thus, subsequent research in the realm of public-cyber criminology must account for the varying conceptions of ‘hackers’ to subvert irresponsible narratives. Neufeld (2023), in an examination of the social construction of technology, notes that contemporary criminological research informed by interpretive ideas such as the social construction of technology allows academics to analyze digital crime reflexively, avoiding the archaic notions of good and bad technologies. Kwok and Koh (2020) use this framework to consider beneficial implementations of deepfake technology (as cited in Neufeld, 2023) as opposed to the often-fatalistic perspective that seems to accompany deepfakes. It is imperative for stakeholders to reconcile fostering awareness of the multitude of risks in cybercrime with the possibility of good-intentioned hackers. These and other interpretive approaches to cybersecurity research could accomplish two goals. The first of which is the demarcation of expertise that is necessary in public-private partnerships. Championing the need for progressive and social justiceoriented opinions in cybersecurity discourse ensures that public criminologists can meaningfully contribute to narrative and policy perhaps more successfully than in the past. Secondly, the public criminologist can provide a voice to actors who may fall into the ethical hacker category, providing a check on narratives that may have otherwise been misconstrued had they been the sole responsibility of corporate or state actors. In other words, a hacker who acts as a counter to oppressive state-corporate practices such as excessive surveillance could be demystified by the public criminologist and thus recognized as integral to the cybercrime ecosystem. The idea of including the hacktivist (and other types of hackers) in stakeholder research will be examined below.

Finally, the main theme of education derived from the interview data provided a rare instance of almost universal agreement among the interviewees. The importance of education in the opinions of the participants yields interesting avenues for the future of intersecting public criminology and cyber criminology. Dissemination is one of the central aspects of public scholarship. During the interviews, as mentioned above, participant five agreed that academia is perhaps antiquated for disseminating cybercrime knowledge. The interviewee mentioned two private companies that “fill that gap”. However, this is another example of marketized ideologies impacting cybersecurity. To even the playing field, both the general public and academics should not be excluded from this discourse (that is not to say that the public or academia is unaffected by market ideologies). However, criminologists have been criticized for both their lack of engagement, as well as their unsuccessful attempts at engagement in the past (Crepault, 2017; Rock, 2014). This critique of criminologists, though warranted, may be explained by academia’s discouragement of engagement with the public (Lumsden and Goode, 2018). As such, the reimagined public criminologist may be required to exist in an environment where engagement is encouraged, and public scholars can separate themselves from academia when mobilizing around social issues and embedding themselves in the general public.

Antonio Gramsci famously stated that everyone is an intellectual; however, not everyone has the social capacity of the intellectual (Saccarelli, 2011). Gramsci dichotomizes the conception of the intellectual into 'organic' and 'traditional' (Olsaretti, 2016). A social class directly generates an organic intellectual, and thus, the intellectual’s interests are synonymous with the caste they originate from (Shear, 2008). The state can use the organic intellectual to forward a hegemonic ideology. On the other end of the spectrum, Gramsci theorized the existence of a traditional intellectual, who, in contrast to the organic intellectual, is independent and autonomous of the state (Saccarelli, 2011). Traditional intellectuals existed before the needs of capitalism, and thus, their contributions to knowledge production were unmediated by the needs of the state. However, with the onset of industrialization and the birth of the organic intellectual, the traditional intellectual became less legitimate and subject to the unconscious biases inherent in believing their insulation from the new politicized environment (Boothman, 2008). Both conceptions of the intellectual shed light on some of the complexities experienced by public criminologists when navigating the highly politicized environment of discourse surrounding crime.

Gramsci's intellectual highlights the significance of common sense in his theorizing (Green, 2018). Specifically, Gramsci's intent in his 'intellectual' conception was to convey the import of non-academics in the role of knowledge generation. Gramsci believed that through communication and social interaction, the public creates a specific understanding of the world, or common sense. Common sense, according to Gramsci, refers to a combination of thoughts, beliefs, and emotions that most of the population internalizes (Green, 2018). This common sense is not stagnant and often reflects the 'folk philosophy' purported by the organic intellectuals on behalf of the ruling class (Olsaretti, 2014). Thus, the intellectual can contribute to the perpetuation or refutation of common sense.

Specifically, Reed (2013) notes that Gramsci's intellectual can contribute to a counter-hegemony by fostering what is known as 'critical awareness.' Critical awareness entails being reflexive over one's role in the public sphere. According to Gramsci, revolutionaries set on countering hegemony must consume knowledge purported by the state with scrutiny and recognize the intricacies of the common sense internalized by the masses (Reed, 2013). The intellectuals who counter hegemony in Gramsci's theorizing are reminiscent of Loader and Spark's (2011) democratic underlabourer whose task "is understood as using one's knowledge as a basis from which to persuade citizens that things can be done otherwise” (p. 127). These two concepts provided by Gramsci and Loader and Sparks constitute the central objective of this study’s intent to combine the tenets of public scholarship and cybersecurity. That is, the themes detailed above provide a framework with which a public criminologist can navigate the spheres surrounding cybercrime.

According to Gramsci (1977), "philosophical systems act on the popular masses as an external political force, as an element of the cohesive force of leading classes, as an element therefore of subordination to an external hegemony" (as cited in Olsaretti, 2016, p. 344). In Gramsci's mind, the philosophers and academics contributed to a hegemonic ideology by ensuring the coherence of messages from the elites and contributing to a harmful common sense among the ruled classes. Interestingly, Gramsci also noted the emotionality inherent in perpetuating a hegemonic ideology, stating that intense emotion becomes internalized by the subaltern classes and represents knowledge or their shared understanding of the world (Boothman, 2008). The emotionality in Gramsci's idea of hegemony is similar to how the professionals in the discourse of cybersecurity today utilize emotions, often through moral panic, to justify increasingly invasive measures of crime control, such as surveillance (Haggerty and Ericson, 2000).

As such, Gramsci's conception of the intellectual may aid in formulating a new public criminologist that can partially address some of the uncertainty that plagues the public's interactions with cybersecurity and alleviate hesitancy to champion PPPs in light of their ability to further marketize discourse and practice. It is important to preface this call to action by stating that there is no simple fix for navigating the politicized environment that characterizes the policing of cybercrime. However, Gramsci's theorizing provides avenues to explore in terms of 'doing public criminology' effectively. As mentioned above, public scholars have participated in a fruitful environment for informing policy in the past, specifically, in the post-war welfare state, and in feminist movements (Reiner, 1988; Nelund, 2014). This call to action elicits Gramsci's idea of the intellectual as dichotomous, the traditional intellectual being independent and autonomous of the ruling class while the organic intellectual's interests are vested in those of a social class (Bezerra et al., 2021). While power dynamics are inherent in becoming a criminological scholar, a public criminologist can also assume the role of the traditional intellectual by stepping out of the academy and mobilizing around current issues, such as the disconnect between cybersecurity stakeholders or proactive education. This new form of public criminologist then combines Gramsci's traditional and organic intellectual to create an independent intellectual who embeds themselves in narrative formulation along with citizens, and the public and private sector (Olsaretti, 2016). Nelund (2014) highlights that a reimagined public criminologist could speak truth to power by drawing attention to social movements formulated by those most afflicted by over-policing and punitive crime control measures in North America, such as Black Lives Matter or the MeToo movement. Similarly, the embedded criminologist utilizes the credibility afforded by the academy and steps outside to support democratic participation in matters of criminal justice discourse reminiscent of Gramsci's traditional intellectual.

As mentioned above, cybercrime, according to the UNODC (2013), has and continues to generate abundant media coverage, public discourse, and scholarly scrutiny. Further, criminological perspectives have proven to be necessary, specifically in defining surrounding terms and understanding how confusion and hysteria may be mitigated by sociological theory. As the UNODC (2013) states, social factors such as poverty and increased global connectivity may directly contribute to increases in cybercrime. Coupling these notions with the established idea that public criminologists have historically been unsuccessful in affecting criminal justice change and generating productive discourse. It is clear that a public criminologist is necessary, though it may require shifts in perception and operation. Thus, the reimagined public criminologist, utilizing the findings from this study, most notably the potential power of PPPs and digital activism in enhancing education, as well as the utility of critical theorizing about concepts such as responsibilization, hacktivism, the technosocial, and the neoliberal market's tendencies and their subsequent effects on cybersecurity practice and discourse, may contribute to empowering the public criminologist and the public sphere. This, in turn, can foster a more participatory approach to narrative generation and academic attention.

3.3 Avenues for Future Research

Barak (2007) states that the next generation of criminologists will have an advantage over their predecessors in that future public criminologists will have a better understanding of technological avenues for research dissemination. For instance, Zhang (2021) finds that contemporary communication mediums such as Tik Tok are uniquely able to disseminate knowledge while shifting the power relations inherent in more traditional forms of state-funded media. Future research must analyze the ability of public criminologists to disseminate knowledge in the non-traditional open forums of the internet. Avenues such as 'Twitch' and 'Discord' allow for community-moderated discussion. However, these mediums also encounter risks of speaking into an echo chamber, as Currie (2007) notes is already a common critique of public criminology thus far. Like Barak's (2007) claim regarding the technological advantage of subsequent generations of criminologists, technological innovation can hopefully produce systemic changes in the nature of ideology formulation more generally. With the influx of communication methods due to technological advances and the internet, public criminologists may have a unique advantage in disseminating knowledge from the sheer number of communication platforms alone.

Another avenue particularly useful for criminology yielded by this project is the implications for stakeholder research. Firstly, as a new graduate student with very few tangible connections to individuals working in cybersecurity, one may assume that gathering an adequate sample would prove overly difficult, especially considering that incentives for participation were not offered to the potential interviewees. However, both the amount and stature of participants attained for this project surprised the researcher and may ease future researchers' hesitancies in attempting to reach a similar population. That is not to say that gathering the sample for this project was devoid of challenge, as will be discussed in the limitations section. Nevertheless, the brand of stakeholder research executed here can serve as a guide for future researchers and hopefully yield more inquiry in a similar vein.

Further, this project also serves as a seemingly rare example of stakeholder-based research in criminology. Though prevalent in business, sustainability, and policy development literature (see Davey et al., 2023; van den Broek, 2019), criminology as a discipline may underutilize this research method. An examination of the reasons for the lack of stakeholder research in criminology is beyond the scope of this project; however, the perceived challenge of gathering subject-matter experts mentioned above may contribute to the reluctance. The approach to stakeholder research implemented here was conducive to addressing the lack of intersection between public and digital criminology, and thus, may inform future projects utilizing the public-cyber criminology advocated for here as a theoretical framework. As witnessed in stakeholder research literature outside of criminology, this method encourages multidisciplinary collaboration and has evident implications for the participatory and democratic approach to public-cyber criminology mentioned above. Future public-cyber criminology research avenues could implement critical or progressive approaches such as McCarthy and Muthuri's (2018) advocacy for the inclusion of 'fringe' stakeholders in business and society research. Evidently owing to critical and feminist academia, this radical strategy involves encompassing more than just the most powerful or visible stakeholders to incorporate the voices of marginalized or less visible populations. Translating fringe stakeholders to public-cyber criminology creates an abundance of possibilities, most notable for the purposes intended in this project would be the inclusion of 'hackers' in similar studies. As noted by McCarthy and Muthuri (2018), relying solely on the most visible sectors of a given population to account for the perspective of harder-to-reach populations may obscure the experiences of the marginalized and delegitimize the possibilities for engagement. As such, future research in public-cyber criminology could benefit significantly from the inclusion of 'hackers', not as a novelty or as a participant in a sample of cybercriminals, but as a legitimate extension of the interested parties in cybersecurity stakeholder research. This collaboration can engender a greater commitment to the social justice roots of public scholarship while also demystifying the notion of 'hacker' amongst the stakeholders involved in cybercrime.

3.4 Limitations

This project may perhaps be critiqued for posing more questions than it answers. However, this criticism should not detract from the merit of the study, which lies in the opportunity to coalesce many different perspectives from the vast diversity of actors impacted by the uncertainty regarding cybercrime. Further, the limited number of experts interviewed does not provide enough basis for making broad generalizations or immediate cross-country comparisons. Gathering thought leaders from a multitude of sectors in various countries proved somewhat challenging, and participant recruitment being reliant on pre-existing connections exacerbated these challenges. The countries included in this study are only representative of the sampling decisions made, and the sample may not be fully representative from an international standpoint. Conducting further research, as previously mentioned, would be effective in addressing the limitations posed by this sample.

REFERENCES

Altheide, D. L. (2009). Moral panic: From sociological concept to public discourse. *Crime, media, culture, 5*(1), 79-99. https://doi.org/10.1177/1741659008102063

Banks, J. (2015). The Heartbleed bug: Insecurity repackaged, rebranded and resold. *Crime, media, culture, 11*(3), 259-279. https://doi.org/10.1177/1741659015592792

Banks, J. (2017). Radical criminology and the techno-security-capitalist complex. In Steinmetz, K., & Nobles, M.R. (Eds.), Technocrime and criminological theory (1st ed.) (pp. 102-115). Routledge. https://doi.org/10.4324/9781315117249

Barak, G. (2007). Doing newsmaking criminology from within the academy. *Theoretical Criminology, 11*(2), 191–207. https://doi.org/10.1177/1362480607075847

Bell, E. (2014). There is an alternative: Challenging the logic of neoliberal penality. *Theoretical Criminology, 18*(4), 489–505. https://doi.org/10.1177/1362480614534880

Bezerra, W. C., Pereira, B. P., & Braga, I. F. (2021). State and civil society in Gramsci: Notes to discuss the institutionalization of social demands in capitalism and the social dimension of occupational therapy. *Cadernos Brasileiros de Terapia Ocupacional, 29*, 1–12. https://doi.org/10.1590/2526-8910.CTOEN2048

Birthriya, S., & Jain, A. K. (2022). A comprehensive survey of phishing email detection and protection techniques. *Information security journal, 31*(4), 411-440. https://doi.org/10.1080/19393555.2021.1959678

Boothman, D. (2008). The sources for Gramsci's concept of hegemony. *Rethinking Marxism*, *20*(2), 201–215. https://doi.org/10.1080/08935690801916942

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative research in psychology, 3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Braun, V., Clarke, V., & Rance, N. (2014). How to use thematic analysis with interview data. In A. Vossler, & N. Moller (Eds.), The counselling & psychotherapy research handbook (pp. 183–197). Sage.

Brown, S. (2006). The criminology of hybrids: Rethinking crime and law in technosocial networks. *Theoretical criminology, 10(*2), 223-244. https://doi.org/10.1177/1362480606063140

Burawoy, M. (2005). For Public Sociology. *American Sociological Review, 70*(1), 4–28. https://doi.org/10.1177/000312240507000102

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

Carrier, N. (2014). On some limits and paradoxes of academic orations on public criminology. *Radical Criminology,* (4), 85-114.

Castells, M. (2008). The new public sphere: global civil society, communication networks, and global governance. *The annals of the American academy of Political and Social Science, 616*(1), 78-93.

Castells, M. (2010). The Rise of The Network Society: The Information Age: Economy, Society and Culture. John Wiley & Sons.

Chancer, L., & McLaughlin, E. (2007). Public criminologies: Diverse perspectives on academia and policy. *Theoretical Criminology, 11*(2), 155-173.

Cherniavskyi, S., Babanina, V., Mykytchyk, O., & Mostepaniuk, L. (2021). Measures to combat cybercrime: analysis of international and Ukrainian experience. *Cuestiones políticas, 39*(69), 115–132. https://doi.org/10.46398/cuestpol.3969.06

Christensen, K. K., & Petersen, K. L. (2017). Public–private partnerships on cyber security: a practice of loyalty. *International Affairs, 93*(6), 1435-1452.

Collier, B., Clayton, R., Hutchings, A., & Thomas, D. (2021). Cybercrime is (often) boring: Infrastructure and alienation in a deviant subculture. *British Journal of Criminology, 61*(5), 1407–1423. https://doi.org/10.1093/bjc/azab026

Conway, G., & Hadlington, L. (2021). How do undergraduate students construct their view of cybercrime? Exploring definitions of cybercrime, perceptions of online risk and victimization. *Policing, 15*(1), 119–129. https://doi.org/10.1093/police/pay098

Crepault, D. (2017). The rise of partisan pedagogy: How stakeholders outside of the academy are answering the call to public criminology. *British journal of criminology, 57*(4), 789-807. https://doi.org/10.1093/bjc/azw034

Cross, C. (2021). Dissent as cybercrime: social media, security, and development in Tanzania. Journal of Eastern African Studies, 15(3), 442–463. https://doi.org/10.1080/17531055.2021.1952797

Cross, C., Holt, T., Powell, A., & Wilson, M. (2021). Responding to cybercrime: Results of a comparison between community members and police personnel. *Trends and issues in crime and criminal justice* (635), 1-20. https://doi.org/10.3316/INFORMIT.123065107596729

Cross, C. (2018). Expectations vs reality: Responding to online fraud across the fraud justice network. *International journal of law, crime, and justice*, 55, 1-12. https://doi.org/10.1016/j.ijlcj.2018.08.001

Currie, E. (2007). Against marginality: Arguments for a public criminology. *Theoretical Criminology*, 11(2), 175–190. https://doi.org/10.1177/1362480607075846

Davey, B., Lindsay, D., Cousins, J., & Glass, B. (2023). “Why didn’t they teach us this?” A qualitative investigation of pharmacist stakeholder perspectives of business management for community pharmacists. *Pharmacy*, *11*(3), 98–119. https://doi.org/10.3390/pharmacy11030098

De Kimpe, L., Walrave, M., Verdegem, P., & Ponnet, K. (2022). What we think we know about cybersecurity: an investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. *Behaviour & Information Technology, 41*(8), 1796–1808. https://doi.org/10.1080/0144929X.2021.1905066

De Paoli, S., Johnstone, J., Coull, N., Ferguson, I., Sinclair, G., Tomkins, P., Brown, M., & Martin, R. (2021). A qualitative exploratory study of the knowledge, forensic, and legal Challenges from the perspective of police cybercrime specialists. *Policing: a journal of policy and practice*, *15*(2), 1429-1445. https://doi.org/10.1093/police/paaa027

Dodge, A. (2016). Digitizing rape culture: Online sexual violence and the power of the digital photograph. *Crime, media, culture*, *12*(1), 65-82. https://doi.org/10.1177/1741659015601173

Dunn Cavelty, M. (2013). From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse. *International studies review*, *15*(1), 105-122. https://doi.org/10.1111/misr.12023

Dunn-Cavelty, M., & Suter, M. (2009). Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection. *International Journal of Critical Infrastructure Protection*, *2*(4), 179–187. https://doi.org/10.1016/j.ijcip.2009.08.006

Electronic Frontier Foundation. (n.d.). About EFF. Retrieved from https://www.eff.org/about

Foucault, M. (1975). Discipline & Punish. *Vintage*. ISBN: 0679752552

Garland, D. (1996). The limits of the sovereign state: Strategies of crime control in contemporary society. *British journal of criminology*, *36*(4), 445–471. https://doi.org/10.1093/oxfordjournals.bjc.a014105

Garland, D., & Sparks, R. (2000). Criminology, social theory, and the challenge of our times. *British journal of criminology, 40*(2), 189-204. https://doi.org/10.1093/bjc/40.2.189

George, J. J., & Leidner, D. E. (2019). From clicktivism to hacktivism: Understanding digital activism. *Information and organization, 29*(3), 100249–100294. https://doi.org/10.1016/j.infoandorg.2019.04.001

Gordon, F., McGovern, A., Thompson, C., & Wood, M. A. (2022). Beyond cybercrime: New perspectives on crime, harm, and digital technologies. *International journal for crime, justice, and social democracy, 11*(1), i-viii. https://doi.org/10.5204/IJCJSD.2215

Green, M. E., (2018). Gramsci's concept of the "simple": Religion, common sense, and the philosophy of praxis. *Rethinking Marxism, 30*(4), 525–545. https://doi.org/10.1080/08935696.2018.1552048

Habermas, J., Lennox, S., & Lennox, F. (1974). The public sphere: An encyclopedia article (1964). *New German Critique, 1*(3), 49–55. https://doi.org/10.2307/487737

Habermas, J. (2005). Legitimation crisis. *Beacon Press*.

Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. *The British journal of sociology*, 51(4), 605-622. https://doi.org/10.1080/00071310020015280

Hall, S., & Winlow, S. (2005). Anti-nirvana: Crime, culture, and instrumentalism in the age of insecurity. *Crime, Media, Culture*, 1(1), 31–48.

Hayward, K. J., & Maas, M. M. (2021). Artificial intelligence and crime: A primer for criminologists. *Crime, media, culture*, *17*(2), 209-233. https://doi.org/10.1177/1741659020917434

Henry, N., & Powell, A. (2016). Sexual violence in the digital age: The scope and limits of criminal law. *Social & legal studies, 25*(4), 397-418. https://doi.org/10.1177/0964663915624273

Herrero, J., Torres, A., Vivas, P., Hidalgo, A., Rodríguez, F. J., & Urueña, A. (2021). Smartphone addiction and cybercrime victimization in the context of lifestyles routine activities and self-control theories: The user's dual vulnerability model of cybercrime victimization. *International Journal of Environmental Research and Public Health*, *18*(7), 3763–. https://doi.org/10.3390/ijerph18073763

Hill, J. B., & Marion, N. E. (2016). Presidential rhetoric on cybercrime: links to terrorism? *Criminal justice studies, 29*(2), 163-177. https://doi.org/10.1080/1478601X.2016.1170279

Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant behavior, 35*(1), 20-40. https://doi.org/10.1080/01639625.2013.822209

Hope, T. (2006). Mass consumption, mass predation - private versus public action? The case of domestic burglary in England and Wales. In Levy (Ed.), *Crime and Insecurity*.

Jane, E. A. (2014). "Your a Ugly, Whorish, Slut": Understanding E-bile. *Feminist media studies*, *14*(4), 531-546. https://doi.org/10.1080/14680777.2012.741073

Jane, E. A. (2015). Flaming? What flaming? The pitfalls and potentials of researching online hostility. *Ethics and information technology*, *17*(1), 65-87. https://doi.org/10.1007/s10676-015-9362-0

Jewkes, Y., & Yar, M. (2012). Policing cybercrime: emerging trends and future challenges. *Handbook of policing*, 608-634.

Joh, E. E. (2017). Feeding the machine: Policing, crime data, & algorithms. *The William and Mary Bill of Rights Journal*, *26*(2), 287-302.

Johansson, T., & Andreasson, J. (2017). The web of loneliness: A netnographic study of narratives of being alone in an online context. *Social sciences (Basel)*, *6*(3), 101. https://doi.org/10.3390/socsci6030101

Johnson, D. G., & Wetmore, J. M. (Eds.). (2021). Technology and society: Building our sociotechnical future. MIT press.

Jordan, T. (2001). Language and libertarianism: the politics of cyberculture and the culture of cyberpolitics. *The sociological review (Keele)*, *49*(1), 1-17. https://doi.org/10.1111/1467-954X.00241

Kellezi, D., Boegelund, C., & Meng, W. (2021). Securing Open Banking with Model-View-Controller Architecture and OWASP. Wireless Communications and Mobile Computing, 2021, 1–13. https://doi.org/10.1155/2021/8028073

Kremer, J. (2014). Policing cybercrime or militarizing cybersecurity? Security mindsets and the regulation of threats from cyberspace. *Information & communications technology law*, *23*(3), 220-237. https://doi.org/10.1080/13600834.2014.970432

Lavorgna, A., & Ugwudike, P. (2021). The datafication revolution in criminal justice: An empirical exploration of frames portraying data-driven technologies for crime prevention and control. *Big data & society*, *8*(2), 205395172110496. https://doi.org/10.1177/20539517211049670

Loader, I., & Sparks, R. (2014). The question of public criminology: Seeking resources of hope for a better politics of crime. *Annales internationales de criminologie, 52*(1-2), 155-177. https://doi.org/10.1017/S0003445200000386

Loader, I. & Sparks, R. (2011). Public criminology? *Routledge*. ISBN: 978-0-415-44550-4

Lumsden, K., & Goode, J. (2018). Public criminology, reflexivity, and the enterprise university: Experiences of research, knowledge transfer work and co-option with police forces. *Theoretical criminology*, *22*(2), 243-257. https://doi.org/10.1177/1362480616689299

Lyon, D. (2014). Surveillance, Snowden, and big data: Capacities, consequences, critique. *Big data & society, 1*(2), 205395171454186. https://doi.org/10.1177/2053951714541861

Marks, A., Bowling, B., & Keenan, C. (2017) 'Automatic Justice? Technology, Crime, and Social Control', in Brownsword, R., Scotford, E., & Yeung, K. (eds), The

Oxford Handbook of Law, Regulation and Technology, Oxford Handbooks. https://doi.org/10.1093/oxfordhb/9780199680832.013.32

McAleese, S. (2019). Doing public criminology with the criminal justice voluntary sector: Methodological reflections and considerations. *The Howard journal of crime and justice*, *58*(3), 366-383.

McCarthy, L., & Muthuri, J. N. (2018). Engaging fringe stakeholders in business and society research: Applying visual participatory research methods. *Business & Society, 57*(1), 131–173. https://doi.org/10.1177/0007650316675610

Mesko, G., & Bernik, I. (2011). Cybercrime: awareness and fear: Slovenian perspectives. *2011 European Intelligence and Security Informatics Conference*, 28–33. https://doi.org/10.1109/EISIC.2011.12

Milivojevic, S., & McGovern, A. (2014). The death of Jill Meagher: crime and punishment on social media. *International Journal for Crime, Justice, and Social Democracy*, *3*(3), 22–39. https://doi.org/10.5204/ijcjsd.v3i3.144

Milivojevic, S., & Radulski, E. M. (2020). The 'future Internet' and crime: towards a criminology of the Internet of Things. *Current issues in criminal justice, 32*(2), 193-207. https://doi.org/10.1080/10345329.2020.1733452

Millman, C.M., Winder, B., & Griffiths, M. D. (2017). UK-based police officers' perceptions of, and role in investigating, cyber-Harassment as a crime. *International Journal of Technoethics, (8)*1, 89-104. DOI: 10.4018/IJT.2017010107

Musiani, F., & Ermoshina, K. (2017). What is a good secure messaging tool? The EFF secure messaging scorecard and the shaping of digital (usable) security. *Westminster papers in communication & culture*, *12*(3), 51–71. https://doi.org/10.16997/wpcc.265

National Institute of Standards and Technology. (n.d.). *Cybersecurity Framework.* https://www.nist.gov/cyberframework

Neufeld, D. (2023). Computer crime motives: Do we have it right? *Sociology Compass*, *17*(4). https://doi.org/10.1111/soc4.13077

Nelund, A. (2014). Troubling publics: A feminist analysis of public criminology. *Radical Criminology*, (4), 67-84.

Notte, R. J., Leukfeldt, R., & Malsch, M. (2021). Double, triple, or quadruple hits?: Exploring the impact of cybercrime on victims in the Netherlands. *International Review of Victimology*, *27*(3), 272–294. https://doi.org/10.1177/02697580211010692

Olsaretti, A. (2014). Beyond class: The many facets of Gramsci's theory of intellectuals. *Journal of Classical Sociology: JCS*, *14*(4), 363–381. https://doi.org/10.1177/1468795X13495125

Olsaretti, A. (2016). Croce, philosophy, and intellectuals: Three aspects of Gramsci's theory of hegemony. *Critical Sociology*, *42*(3), 337–355. https://doi.org/10.1177/0896920514540184

Owen, D. (2021). Cybercrime, cybersecurity, and water utilities. *International journal of water resources development, 37*(6), 1021-1026. https://doi.org/10.1080/07900627.2021.1965965

Payne, K., Maras, K. L., Russell, A. J., Brosnan, M. J., & Mills, R. (2020). Self-reported motivations for engaging or declining to engage in cyber-dependent offending and the role of autistic traits. *Research in Developmental Disabilities, 104*(2020), 103681–103681. https://doi.org/10.1016/j.ridd.2020.103681

Petersilia, J. (2008). Influencing public policy: An embedded criminologist reflects on California prison reform. *Journal of experimental criminology, 4*(4), 335-356.

Piche, J. (2016). Assessing the boundaries of public criminology: on what does count. *Social justice (San Francisco, Calif.), 42*(2), 70-90.

Pogrebna, G., & Skilton, M. (2019). A sneak peek into the motivation of a cybercriminal. In Navigating New Cyber Risks (pp. 31–54). *Springer International Publishing AG*. https://doi.org/10.1007/978-3-030-13527-0_3

Powell, A., Stratton, G., & Cameron, R. (2018). Digital criminology: crime and justice in digital society. *Routledge*.

Preston, K., Halpin, M., & Maguire, F. (2021). The black pill: New technology and the male supremacy of involuntarily celibate men. *Men and masculinities, 24*(5), 823-841. https://doi.org/10.1177/1097184X211017954

Reed, J. P., (2013). Theorist of subaltern subjectivity: Antonio Gramsci, popular beliefs, political passion, and reciprocal learning. *Critical Sociology, 39*(4), 561–591. https://doi.org/10.1177/0896920512437391

Reiner, R. (1988). British criminology and the state. *British journal of criminology, 28*(2), 138-158. https://doi.org/10.1093/oxfordjournals.bjc.a047722

Reynolds, D. (2022). Everyone is victimized or only the naïve? The conflicting discourses surrounding identity theft victimization. *International Review of Victimology, 0*(0). https://doi-org.uproxy.library.dc-uoit.ca/10.1177/02697580221091284

Rock, P. (2014). The public faces of public criminology. *Criminology & criminal justice, 14*(4), 412-433. https://doi.org/10.1177/1748895813509638

Rowe, M. (2013). Just like a TV show: Public criminology and the media coverage of "hunt for Britain's most wanted man. *Crime, Media, Culture, 9*(1), 23–38. https://doi.org/10.1177/1741659012438298

Ruggiero, V. (2012). How public is public criminology? *Crime, media, culture, 8*(2), 151-160. https://doi.org/10.1177/1741659012444432

Saunders, B., Sim, J., Kingstone, T., Baker, S., Waterfield, J., Bartlam, B., Burroughs, H., & Jinks, C. (2017). Saturation in qualitative research: exploring its conceptualization and operationalization. *Quality & Quantity, 52*(4), 1893–1907. https://doi.org/10.1007/s11135-017-0574-8

Saccarelli, E. (2011). The intellectual in question: Antonio Gramsci and the crisis of academia. *Cultural Studies (London, England), 25*(6), 757–782. https://doi.org/10.1080/09502386.2011.567420

Shires, J. (2020). Cyber-noir: Cybersecurity and popular culture. *Contemporary Security Policy, 41*(1), 82–107. https://doi.org/10.1080/13523260.2019.1670006

Silverman, D. (1997). Qualitative research: issues of theory, method, and practice. Sage. (p. 149-168)

Smith, G. J. D., Moses, L. B., & Chan, J. (2017). The challenges of doing criminology in the big data era: Towards a digital and data-driven approach. *British journal of criminology, 57*(2), 259–274. https://doi.org/10.1093/bjc/azw096

Stanko, B. A. (2007). From academia to policy making: Changing police responses to violence against women. *Theoretical Criminology, 11*(2), 209-219.

Stratton, G., Powell, A., & Cameron, R. (2017). Crime and justice in digital society: towards a "digital criminology"? International Journal for Crime, Justice and Social Democracy, 6(2), 17–33. https://doi.org/10.5204/ijcjsd.v6i2.355

Taylor, P. (1999). Hackers: Crime in the digital sublime. Taylor & Francis Group.

Tittle, C. R. (2004). The arrogance of public sociology. Social Forces, 82(4), 1639-1643.

Toma, T., Décary-Hétu, D., & Dupont, B. (2023). The Benefits of a Cyber-Resilience Posture on Negative Public Reaction Following Data Theft. *Journal of Criminology* (2021). https://doi.org/10.1177/26338076231161898

Tonry, M. (2010). “Public criminology” and evidence-based policy. *Criminology & Public Policy*, *9(*4), 783–797. https://doi.org/10.1111/j.1745-9133.2010.00670.x

Turkle, S. (2011). Alone together: Why we expect more from technology and less from each other. Basic Books.

Uggen, C., & Inderbitzin, M. (2010). Public criminologies. *Criminology & public policy*, *9*(4), 725-749.

UNODC. (2013). Comprehensive Study on Cybercrime. Report prepared for the Open-Ended Intergovernmental Expert Group on Cyber crime. New York: United Nations. Retrieved from https://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

Vance, A., Lowry, P. B., & Eggett, D. (2015). Increasing accountability through user-interface design artifacts: A new approach to addressing the problem of access-policy violations. *MIS Quarterly, 39*(2), 345–366. https://doi.org/10.25300/MISQ/2015/39.2.04

van den Broek, K. (2019). Stakeholders’ perceptions of the socio-economic and environmental challenges at Lake Victoria. *Lakes & reservoirs: research and management*, *24*(3), 239–245. https://doi.org/10.1111/lre.12275

Wacquant, L. (2009). The body, the ghetto, and the penal state. *Qualitative sociology*, *32*(1), 101-129.

Wall, D. S. (2008). Cybercrime, media, and insecurity: the shaping of public perceptions of cybercrime. *International review of law, computers & technology, 22*(1-2), 45-63.

Whitson, J. R., & Haggerty, K. D. (2008). Identity theft and the care of the virtual self. *Economy and society, 37*(4), 572-594. https://doi.org/10.1080/03085140802357950

Willson, M. (2010). Technology, networks, and communities. *Information, communication & society, 13*(5), 747-764. https://doi.org/10.1080/13691180903271572

Wood, M. A. (2021). Rethinking how technologies harm. *British journal of criminology, 61*(3), 627-647. https://doi.org/10.1093/bjc/azaa074

Yar, M. (2008). Computer crime control as industry: Virtual insecurity and the market for private policing. In Technologies of InSecurity (pp. 203-218). *Routledge-Cavendish*.

Yar, M. (2013). The policing of Internet sex offences: pluralised governance versus hierarchies of standing. *Policing & society, 23*(4), 482-497. https://doi.org/10.1080/10439463.2013.780226

Zhang, H., Tang, Z., & Jayakar, K. (2018). A socio-technical analysis of China's cybersecurity policy: Towards delivering trusted e-government services. *Telecommunications policy, 42*(5), 409-420. https://doi.org/10.1016/j.telpol.2018.02.004

Zhang, Z. (2021). Infrastructuralization of Tik Tok: transformation, power relationships, and platformization of video entertainment in China. *Media, Culture & Society*, *43*(2), 219–236. https://doi.org/10.1177/0163443720939452